

UNIVERZITET U BEOGRADU

Vanja M. Korać

**DIGITALNA FORENZIKA U FUNKCIJI
ZAŠTITE INFORMACIONOG SISTEMA
BAZIRANOG NA LINUX I WINDOWS
PLATFORMAMA**

- *POSEBAN PRILOG* -

doktorska disertacija

Beograd, 2014.

SADRŽAJ:

4.3.1 WINDOWS OPERATIVNI SISTEMI - SKENIRANJE SERVISA NA RANJIVOSTI U 2011.	10
Tabela 1. Windows OS sa IP adresama 172.23.202.69, 172.23.202.106, 172.23.202.109 (2011. godina)	10
Tabela 2. Windows OS – Pronađeni servisi na IP adresi 172.23.202.109 (2011. godina)	18
Tabela 3. Windows OS – Pronađeni servisi na IP adresi 172.23.202.106 (2011. godina)	19
Tabela 4. Windows OS – Pronađeni servisi na IP adresi 172.23.202.69 (2011. godina)	20
Tabela 5. Windows OS sa IP adresom 172.23.202.107 (2011. godina)	20
Tabela 6. Windows OS – Pronađeni servisi na IP adresi 172.23.202.107 (2011. godina)	24
Tabela 7. Windows OS sa IP adresama 172.23.202.110, 172.23.202.76 (2011. godina)	24
Tabela 8. Windows OS – Pronađeni servisi na IP adresi 172.23.202.110 (2011. godina)	34
Tabela 9. Windows OS – Pronađeni servisi na IP adresi 172.23.202.76 (2011. godina)	34
Tabela 10. Windows OS sa IP adresama 172.23.202.111, 172.23.202.75, 172.23.202.74, 172.23.202.73 (2011. godina)	35
Tabela 11. Windows OS – Pronađeni servisi na IP adresi 172.23.202.111 (2011. godina)	41
Tabela 12. Windows OS – Pronađeni servisi na IP adresi 172.23.202.75 (2011. godina)	41
Tabela 13. Windows OS – Pronađeni servisi na IP adresi 172.23.202.74 (2011. godina)	42
Tabela 14. Windows OS – Pronađeni servisi na IP adresi 172.23.202.73 (2011. godina)	42
Tabela 15. Windows OS sa IP adresom 172.23.202.101 (2011. godina)	43
Tabela 16. Windows OS – Pronađeni servisi na IP adresi 172.23.202.101 (2011. godina)	50
Tabela 17. Windows OS sa IP adresama 172.23.202.112, 172.23.202.72, 172.23.202.71, 172.23.202.70 (2011. godina)	53
Tabela 18. Windows OS – Pronađeni servisi na IP adresi 172.23.202.112 (2011. godina)	57
Tabela 19. Windows OS – Pronađeni servisi na IP adresi 172.23.202.72 (2011. godina)	57
Tabela 20. Windows OS – Pronađeni servisi na IP adresi 172.23.202.71 (2011. godina)	58
Tabela 21. Windows OS – Pronađeni servisi na IP adresi 172.23.202.70 (2011. godina)	58
Tabela 22. Windows OS sa IP adresama 172.23.202.113, 172.23.202.89, 172.23.202.88, 172.23.202.87, 172.23.202.86, 172.23.202.85, 172.23.202.84, 172.23.202.83 (2011. godina)	59
Tabela 23. Windows OS – Pronađeni servisi na IP adresi 172.23.202.113 (2011. godina)	62
Tabela 24. Windows OS – Pronađeni servisi na IP adresi 172.23.202.89 (2011. godina)	63
Tabela 25. Windows OS – Pronađeni servisi na IP adresi 172.23.202.88 (2011. godina)	64
Tabela 26. Windows OS – Pronađeni servisi na IP adresi 172.23.202.87 (2011. godina)	65
Tabela 27. Windows OS – Pronađeni servisi na IP adresi 172.23.202.86 (2011. godina)	66
Tabela 28. Windows OS – Pronađeni servisi na IP adresi 172.23.202.85 (2011. godina)	67
Tabela 29. Windows OS – Pronađeni servisi na IP adresi 172.23.202.84 (2011. godina)	67
Tabela 30. Windows OS – Pronađeni servisi na IP adresi 172.23.202.83 (2011. godina)	68
Tabela 31. Windows OS sa IP adresama 172.23.202.114, 172.23.202.82, 172.23.202.81, 172.23.202.80, 172.23.202.79, 172.23.202.78, 172.23.202.77 (2011. godina)	69
Tabela 32. Windows OS – Pronađeni servisi na IP adresi 172.23.202.114 (2011. godina)	72
Tabela 33. Windows OS – Pronađeni servisi na IP adresi 172.23.202.82 (2011. godina)	72
Tabela 34. Windows OS – Pronađeni servisi na IP adresi 172.23.202.81 (2011. godina)	73
Tabela 35. Windows OS – Pronađeni servisi na IP adresi 172.23.202.80 (2011. godina)	74
Tabela 36. Windows OS – Pronađeni servisi na IP adresi 172.23.202.79 (2011. godina)	75
Tabela 37. Windows OS – Pronađeni servisi na IP adresi 172.23.202.78 (2011. godina)	76
Tabela 38. Windows OS – Pronađeni servisi na IP adresi 172.23.202.77 (2011. godina)	76
Tabela 39. Windows OS sa IP adresama 172.23.202.117, 172.23.202.68 (2011. godina)	77
Tabela 40. Windows OS – Pronađeni servisi na IP adresi 172.23.202.117 (2011. godina)	79
Tabela 41. Windows OS – Pronađeni servisi na IP adresi 172.23.202.68 (2011. godina)	80
Tabela 42. Windows OS sa IP adresama 172.23.202.108 (2011. godina)	81
Tabela 43. Windows OS – Pronađeni servisi na IP adresi 172.23.202.108 (2011. godina)	82
Tabela 44. Windows OS sa IP adresama 172.23.202.105 (2011. godina)	82
Tabela 45. Windows OS – Pronađeni servisi na IP adresi 172.23.202.105 (2011. godina)	90
Tabela 46. Windows OS sa IP adresama 172.23.202.115, 172.23.202.116, 172.23.202.100, 172.23.202.99, 172.23.202.98, 172.23.202.97, 172.23.202.96, 172.23.202.95, 172.23.202.94, 172.23.202.93, 172.23.202.92, 172.23.202.91, 172.23.202.90 (2011. godina)	90
Tabela 47. Windows OS – Pronađeni servisi na IP adresi 172.23.202.115 (2011. godina)	92
Tabela 48. Windows OS – Pronađeni servisi na IP adresi 172.23.202.116 (2011. godina)	93
Tabela 49. Windows OS – Pronađeni servisi na IP adresi 172.23.202.100 (2011. godina)	94
Tabela 50. Windows OS – Pronađeni servisi na IP adresi 172.23.202.99 (2011. godina)	95
Tabela 51. Windows OS – Pronađeni servisi na IP adresi 172.23.202.98 (2011. godina)	96
Tabela 52. Windows OS – Pronađeni servisi na IP adresi 172.23.202.97 (2011. godina)	97
Tabela 53. Windows OS – Pronađeni servisi na IP adresi 172.23.202.96 (2011. godina)	97
Tabela 54. Windows OS – Pronađeni servisi na IP adresi 172.23.202.95 (2011. godina)	98
Tabela 55. Windows OS – Pronađeni servisi na IP adresi 172.23.202.94 (2011. godina)	99

Tabela 56. Windows OS – Pronađeni servisi na IP adresi 172.23.202.93 (2011. godina)	100
Tabela 57. Windows OS – Pronađeni servisi na IP adresi 172.23.202.92 (2011. godina)	101
Tabela 58. Windows OS – Pronađeni servisi na IP adresi 172.23.202.91 (2011. godina)	101
Tabela 59. Windows OS – Pronađeni servisi na IP adresi 172.23.202.90 (2011. godina)	102
Tabela 60. Windows OS sa IP adresama 172.23.202.118 (2011. godina)	103
Tabela 61. Windows OS – Pronađeni servisi na IP adresi 172.23.202.118 (2011. godina)	104
Tabela 62. Windows OS sa IP adresama 172.23.202.103 (2011. godina)	105
Tabela 63. Windows OS – Pronađeni servisi na IP adresi 172.23.202.103 (2011. godina)	106
Tabela 64. Windows OS sa IP adresama 172.23.202.104 (2011. godina)	106
Tabela 65. Windows OS – Pronađeni servisi na IP adresi 172.23.202.104 (2011. godina)	107
Tabela 66. Windows OS sa IP adresama 172.23.202.102 (2011. godina)	108
Tabela 67. Windows OS – Pronađeni servisi na IP adresi 172.23.202.102 (2011. godina)	109
4.3.2 LINUX OPERATIVNI SISTEMI - SKENIRANJE SERVISA NA RANJIVOSTI U 2011.	109
Tabela 68. Linux OS sa IP adresama 172.23.202.124, 172.23.202.220 (2011. godina)	109
Tabela 69. Linux OS – Pronađeni servisi na IP adresi 172.23.202.124 (2011. godina)	129
Tabela 70. Linux OS – Pronađeni servisi na IP adresi 172.23.202.220 (2011. godina)	134
Tabela 71. Linux OS sa IP adresama 172.23.202.126, 172.23.202.225 (2011. godina)	139
Tabela 72. Linux OS – Pronađeni servisi na IP adresi 172.23.202.126 (2011. godina)	165
Tabela 73. Linux OS – Pronađeni servisi na IP adresi 172.23.202.225 (2011. godina)	167
Tabela 74. Linux OS sa IP adresama 172.23.202.193, 172.23.202.194, 172.23.202.226, 172.23.202.227 (2011. godina)	168
Tabela 75. Linux OS – Pronađeni servisi na IP adresi 172.23.202.193 (2011. godina)	192
Tabela 76. Linux OS – Pronađeni servisi na IP adresi 172.23.202.194 (2011. godina)	193
Tabela 77. Linux OS – Pronađeni servisi na IP adresi 172.23.202.226 (2011. godina)	194
Tabela 78. Linux OS – Pronađeni servisi na IP adresi 172.23.202.227 (2011. godina)	196
Tabela 79. Linux OS sa IP adresama 172.23.202.195, 172.23.202.196, 172.23.202.221, 172.23.202.222 (2011. godina)	197
Tabela 80. Linux OS – Pronađeni servisi na IP adresi 172.23.202.195 (2011. godina)	220
Tabela 81. Linux OS – Pronađeni servisi na IP adresi 172.23.202.196 (2011. godina)	221
Tabela 82. Linux OS – Pronađeni servisi na IP adresi 172.23.202.221 (2011. godina)	222
Tabela 83. Linux OS – Pronađeni servisi na IP adresi 172.23.202.222 (2011. godina)	224
Tabela 84. Linux OS sa IP adresama 172.23.202.122, 172.23.202.232, 172.23.202.200, 172.23.202.230, 172.23.202.135, 172.23.202.231 (2011. godina)	225
Tabela 85. Linux OS – Pronađeni servisi na IP adresi 172.23.202.122 (2011. godina)	234
Tabela 86. Linux OS – Pronađeni servisi na IP adresi 172.23.202.232 (2011. godina)	240
Tabela 87. Linux OS – Pronađeni servisi na IP adresi 172.23.202.200 (2011. godina)	245
Tabela 88. Linux OS – Pronađeni servisi na IP adresi 172.23.202.230 (2011. godina)	250
Tabela 89. Linux OS – Pronađeni servisi na IP adresi 172.23.202.135 (2011. godina)	255
Tabela 90. Linux OS – Pronađeni servisi na IP adresi 172.23.202.231 (2011. godina)	261
Tabela 91. Linux OS sa IP adresama 172.23.202.133, 172.23.202.132, 172.23.202.123, 172.23.202.229 (2011. godina)	266
Tabela 92. Linux OS – Pronađeni servisi na IP adresi 172.23.202.133 (2011. godina)	279
Tabela 93. Linux OS – Pronađeni servisi na IP adresi 172.23.202.132 (2011. godina)	284
Tabela 94. Linux OS – Pronađeni servisi na IP adresi 172.23.202.123 (2011. godina)	289
Tabela 95. Linux OS – Pronađeni servisi na IP adresi 172.23.202.229 (2011. godina)	294
Tabela 96. Linux OS sa IP adresama 172.23.202.197 (2011. godina)	300
Tabela 97. Linux OS – Pronađeni servisi na IP adresi 172.23.202.197 (2011. godina)	308
Tabela 98. Linux OS sa IP adresama 172.23.202.199, 172.23.202.224 (2011. godina)	310
Tabela 99. Linux OS – Pronađeni servisi na IP adresi 172.23.202.199 (2011. godina)	317
Tabela 100. Linux OS – Pronađeni servisi na IP adresi 172.23.202.224 (2011. godina)	319
Tabela 101. Linux OS sa IP adresama 172.23.202.198, 172.23.202.223 (2011. godina)	322
Tabela 102. Linux OS – Pronađeni servisi na IP adresi 172.23.202.198 (2011. godina)	327
Tabela 103. Linux OS – Pronađeni servisi na IP adresi 172.23.202.223 (2011. godina)	329
Tabela 104. Linux OS sa IP adresama 172.23.202.131 (2011. godina)	331
Tabela 105. Linux OS – Pronađeni servisi na IP adresi 172.23.202.131 (2011. godina)	335
Tabela 106. Linux OS sa IP adresama 172.23.202.125 (2011. godina)	338
Tabela 107. Linux OS – Pronađeni servisi na IP adresi 172.23.202.125 (2011. godina)	341
4.3.3 WINDOWS OPERATIVNI SISTEMI - SKENIRANJE SERVISA NA RANJIVOSTI U 2013.	342
Tabela 108. Windows OS sa IP adresama 172.23.202.109, 172.23.202.106, 172.23.202.69 (2013. godina)	342
Tabela 109. Windows OS sa IP adresom 172.23.202.107 (2013. godina)	352
Tabela 110. Windows OS sa IP adresama 172.23.202.110, 172.23.202.76 (2013. godina)	355
Tabela 111. Windows OS sa IP adresama 172.23.202.111, 172.23.202.75, 172.23.202.74, 172.23.202.73 (2013. godina)	367
Tabela 112. Windows OS sa IP adresom 172.23.202.101 (2013. godina)	373
Tabela 113. Windows OS sa IP adresama 172.23.202.112, 172.23.202.72, 172.23.202.71, 172.23.202.70 (2013. godina)	381

Tabela 114. Windows OS sa IP adresama 172.23.202.113, 172.23.202.89, 172.23.202.88, 172.23.202.87, 172.23.202.86, 172.23.202.85, 172.23.202.84, 172.23.202.83 (2013. godina)	385
Tabela 115. Windows OS sa IP adresama 172.23.202.114, 172.23.202.82, 172.23.202.81, 172.23.202.80, 172.23.202.79, 172.23.202.78, 172.23.202.77 (2013. godina)	389
Tabela 116. Windows OS sa IP adresama 172.23.202.117, 172.23.202.68 (2013. godina)	391
Tabela 117. Windows OS sa IP adresom 172.23.202.108 (2013. godina)	394
Tabela 118. Windows OS sa IP adresom 172.23.202.105 (2013. godina)	395
Tabela 119. Windows OS sa IP adresama 172.23.202.115, 172.23.202.116, 172.23.202.100, 172.23.202.99, 172.23.202.98, 172.23.202.97, 172.23.202.96, 172.23.202.95, 172.23.202.94, 172.23.202.93, 172.23.202.92, 172.23.202.91, 172.23.202.90 (2013. godina)	404
Tabela 120. Windows OS sa IP adresom 172.23.202.118 (2013. godina)	406
Tabela 121. Windows OS sa IP adresom 172.23.202.103 (2013. godina)	407
Tabela 122. Windows OS sa IP adresom 172.23.202.104 (2013. godina)	408
Tabela 123. Windows OS sa IP adresom 172.23.202.102 (2013. godina)	409
4.3.4 LINUX OPERATIVNI SISTEMI - SKENIRANJE SERVISA NA RANJIVOSTI U 2013	410
Tabela 124. Linux OS sa IP adresama 172.23.202.124, 172.23.202.220 (2013. godina)	410
Tabela 125. Linux OS sa IP adresama 172.23.202.126, 172.23.202.225 (2013. godina)	437
Tabela 126. Linux OS sa IP adresama 172.23.202.193, 172.23.202.227, 172.23.202.194, 172.23.202.226, (2013. godina)	468
Tabela 127. Linux OS sa IP adresama 172.23.202.195, 172.23.202.196, 172.23.202.221, 172.23.202.222, (2013. godina)	496
Tabela 128. Linux OS sa IP adresama 172.23.202.122, 172.23.202.232, 172.23.202.200, 172.23.202.230, 172.23.202.135, 172.23.202.231 (2013. godina)	525
Tabela 129. Linux OS sa IP adresama 172.23.202.133, 172.23.202.132, 172.23.202.123, 172.23.202.229 (2013. godina)	541
Tabela 130. Linux OS sa IP adresom 172.23.202.197 (2013. godina)	560
Tabela 131. Linux OS sa IP adresama 172.23.202.199, 172.23.202.224 (2013. godina)	575
Tabela 132. Linux OS sa IP adresama 172.23.202.198, 172.23.202.223 (2013. godina)	590
Tabela 133. Linux OS sa IP adresom 172.23.202.131 (2013. godina)	602
Tabela 134. Linux OS sa IP adresom 172.23.202.125 (2013. godina)	612

SPISAK TABELA :

Tabela 1. Windows OS sa IP adresama 172.23.202.69, 172.23.202.106, 172.23.202.109 (2011. godina)	10
Tabela 2. Windows OS – Pronađeni servisi na IP adresi 172.23.202.109 (2011. godina).....	18
Tabela 3. Windows OS – Pronađeni servisi na IP adresi 172.23.202.106 (2011. godina).....	19
Tabela 4. Windows OS – Pronađeni servisi na IP adresi 172.23.202.69 (2011. godina).....	20
Tabela 5. Windows OS sa IP adresom 172.23.202.107 (2011. godina).....	20
Tabela 6. Windows OS – Pronađeni servisi na IP adresi 172.23.202.107 (2011. godina).....	24
Tabela 7. Windows OS sa IP adresama 172.23.202.110, 172.23.202.76 (2011. godina)	24
Tabela 8. Windows OS – Pronađeni servisi na IP adresi 172.23.202.110 (2011. godina).....	34
Tabela 9. Windows OS – Pronađeni servisi na IP adresi 172.23.202.76 (2011. godina).....	34
Tabela 10. Windows OS sa IP adresama 172.23.202.111, 172.23.202.75, 172.23.202.74, 172.23.202.73 (2011. godina).....	35
Tabela 11. Windows OS – Pronađeni servisi na IP adresi 172.23.202.111 (2011. godina).....	41
Tabela 12. Windows OS – Pronađeni servisi na IP adresi 172.23.202.75 (2011. godina).....	41
Tabela 13. Windows OS – Pronađeni servisi na IP adresi 172.23.202.74 (2011. godina).....	42
Tabela 14. Windows OS – Pronađeni servisi na IP adresi 172.23.202.73 (2011. godina).....	42
Tabela 15. Windows OS sa IP adresom 172.23.202.101 (2011. godina).....	43
Tabela 16. Windows OS – Pronađeni servisi na IP adresi 172.23.202.101 (2011. godina).....	50
Tabela 17. Windows OS sa IP adresama 172.23.202.112, 172.23.202.72, 172.23.202.71, 172.23.202.70 (2011. godina).....	53
Tabela 18. Windows OS – Pronađeni servisi na IP adresi 172.23.202.112 (2011. godina).....	57
Tabela 19. Windows OS – Pronađeni servisi na IP adresi 172.23.202.72 (2011. godina).....	57
Tabela 20. Windows OS – Pronađeni servisi na IP adresi 172.23.202.71 (2011. godina).....	58
Tabela 21. Windows OS – Pronađeni servisi na IP adresi 172.23.202.70 (2011. godina).....	58
Tabela 22. Windows OS sa IP adresama 172.23.202.113, 172.23.202.89, 172.23.202.88, 172.23.202.87, 172.23.202.86, 172.23.202.85, 172.23.202.84, 172.23.202.83 (2011. godina)	59
Tabela 23. Windows OS – Pronađeni servisi na IP adresi 172.23.202.113 (2011. godina).....	62
Tabela 24. Windows OS – Pronađeni servisi na IP adresi 172.23.202.89 (2011. godina).....	63
Tabela 25. Windows OS – Pronađeni servisi na IP adresi 172.23.202.88 (2011. godina).....	64
Tabela 26. Windows OS – Pronađeni servisi na IP adresi 172.23.202.87 (2011. godina).....	65
Tabela 27. Windows OS – Pronađeni servisi na IP adresi 172.23.202.86 (2011. godina).....	66

Tabela 28. Windows OS – Pronađeni servisi na IP adresi 172.23.202.85 (2011. godina).....	67
Tabela 29. Windows OS – Pronađeni servisi na IP adresi 172.23.202.84 (2011. godina).....	67
Tabela 30. Windows OS – Pronađeni servisi na IP adresi 172.23.202.83 (2011. godina).....	68
Tabela 31. Windows OS sa IP adresama 172.23.202.114, 172.23.202.82, 172.23.202.81, 172.23.202.80, 172.23.202.79, 172.23.202.78, 172.23.202.77 (2011. godina)	69
Tabela 32. Windows OS – Pronađeni servisi na IP adresi 172.23.202.114 (2011. godina).....	72
Tabela 33. Windows OS – Pronađeni servisi na IP adresi 172.23.202.82 (2011. godina).....	72
Tabela 34. Windows OS – Pronađeni servisi na IP adresi 172.23.202.81 (2011. godina).....	73
Tabela 35. Windows OS – Pronađeni servisi na IP adresi 172.23.202.80 (2011. godina).....	74
Tabela 36. Windows OS – Pronađeni servisi na IP adresi 172.23.202.79 (2011. godina).....	75
Tabela 37. Windows OS – Pronađeni servisi na IP adresi 172.23.202.78 (2011. godina).....	76
Tabela 38. Windows OS – Pronađeni servisi na IP adresi 172.23.202.77 (2011. godina).....	76
Tabela 39. Windows OS sa IP adresama 172.23.202.117, 172.23.202.68 (2011. godina)	77
Tabela 40. Windows OS – Pronađeni servisi na IP adresi 172.23.202.117 (2011. godina).....	79
Tabela 41. Windows OS – Pronađeni servisi na IP adresi 172.23.202.68 (2011. godina).....	80
Tabela 42. Windows OS sa IP adresama 172.23.202.108 (2011. godina)	81
Tabela 43. Windows OS – Pronađeni servisi na IP adresi 172.23.202.108 (2011. godina).....	82
Tabela 44. Windows OS sa IP adresama 172.23.202.105 (2011. godina)	82
Tabela 45. Windows OS – Pronađeni servisi na IP adresi 172.23.202.105 (2011. godina).....	90
Tabela 46. Windows OS sa IP adresama 172.23.202.115, 172.23.202.116, 172.23.202.100, 172.23.202.99, 172.23.202.98, 172.23.202.97, 172.23.202.96, 172.23.202.95, 172.23.202.94, 172.23.202.93, 172.23.202.92, 172.23.202.91, 172.23.202.90 (2011. godina)	90
Tabela 47. Windows OS – Pronađeni servisi na IP adresi 172.23.202.115 (2011. godina).....	92
Tabela 48. Windows OS – Pronađeni servisi na IP adresi 172.23.202.116 (2011. godina).....	93
Tabela 49. Windows OS – Pronađeni servisi na IP adresi 172.23.202.100 (2011. godina).....	94
Tabela 50. Windows OS – Pronađeni servisi na IP adresi 172.23.202.99 (2011. godina).....	95
Tabela 51. Windows OS – Pronađeni servisi na IP adresi 172.23.202.98 (2011. godina).....	96
Tabela 52. Windows OS – Pronađeni servisi na IP adresi 172.23.202.97 (2011. godina).....	97
Tabela 53. Windows OS – Pronađeni servisi na IP adresi 172.23.202.96 (2011. godina).....	97
Tabela 54. Windows OS – Pronađeni servisi na IP adresi 172.23.202.95 (2011. godina).....	98
Tabela 55. Windows OS – Pronađeni servisi na IP adresi 172.23.202.94 (2011. godina).....	99
Tabela 56. Windows OS – Pronađeni servisi na IP adresi 172.23.202.93 (2011. godina).....	100

Tabela 57. Windows OS – Pronađeni servisi na IP adresi 172.23.202.92 (2011. godina).....	101
Tabela 58. Windows OS – Pronađeni servisi na IP adresi 172.23.202.91 (2011. godina).....	101
Tabela 59. Windows OS – Pronađeni servisi na IP adresi 172.23.202.90 (2011. godina).....	102
Tabela 60. Windows OS sa IP adresama 172.23.202.118 (2011. godina)	103
Tabela 61. Windows OS – Pronađeni servisi na IP adresi 172.23.202.118 (2011. godina).....	104
Tabela 62. Windows OS sa IP adresama 172.23.202.103 (2011. godina)	105
Tabela 63. Windows OS – Pronađeni servisi na IP adresi 172.23.202.103 (2011. godina).....	106
Tabela 64. Windows OS sa IP adresama 172.23.202.104 (2011. godina)	106
Tabela 65. Windows OS – Pronađeni servisi na IP adresi 172.23.202.104 (2011. godina).....	107
Tabela 66. Windows OS sa IP adresama 172.23.202.102 (2011. godina)	108
Tabela 67. Windows OS – Pronađeni servisi na IP adresi 172.23.202.102 (2011. godina).....	109
Tabela 68. Linux OS sa IP adresama 172.23.202.124, 172.23.202.220 (2011. godina)	109
Tabela 69. Linux OS – Pronađeni servisi na IP adresi 172.23.202.124 (2011. godina)	129
Tabela 70. Linux OS – Pronađeni servisi na IP adresi 172.23.202.220 (2011. godina)	134
Tabela 71. Linux OS sa IP adresama 172.23.202.126, 172.23.202.225 (2011. godina)	139
Tabela 72. Linux OS – Pronađeni servisi na IP adresi 172.23.202.126 (2011. godina)	165
Tabela 73. Linux OS – Pronađeni servisi na IP adresi 172.23.202.225 (2011. godina)	167
Tabela 74. Linux OS sa IP adresama 172.23.202.193, 172.23.202.194, 172.23.202.226, 172.23.202.227 (2011. godina).....	168
Tabela 75. Linux OS – Pronađeni servisi na IP adresi 172.23.202.193 (2011. godina)	192
Tabela 76. Linux OS – Pronađeni servisi na IP adresi 172.23.202.194 (2011. godina)	193
Tabela 77. Linux OS – Pronađeni servisi na IP adresi 172.23.202.226 (2011. godina)	194
Tabela 78. Linux OS – Pronađeni servisi na IP adresi 172.23.202.227 (2011. godina)	196
Tabela 79. Linux OS sa IP adresama 172.23.202.195, 172.23.202.196, 172.23.202.221, 172.23.202.222 (2011. godina).....	197
Tabela 80. Linux OS – Pronađeni servisi na IP adresi 172.23.202.195 (2011. godina)	220
Tabela 81. Linux OS – Pronađeni servisi na IP adresi 172.23.202.196 (2011. godina)	221
Tabela 82. Linux OS – Pronađeni servisi na IP adresi 172.23.202.221 (2011. godina)	222
Tabela 83. Linux OS – Pronađeni servisi na IP adresi 172.23.202.222 (2011. godina)	224
Tabela 84. Linux OS sa IP adresama 172.23.202.122, 172.23.202.232, 172.23.202.200, 172.23.202.230, 172.23.202.135, 172.23.202.231 (2011. godina)	225
Tabela 85. Linux OS – Pronađeni servisi na IP adresi 172.23.202.122 (2011. godina)	234

Tabela 86. Linux OS – Pronađeni servisi na IP adresi 172.23.202.232 (2011. godina)	240
Tabela 87. Linux OS – Pronađeni servisi na IP adresi 172.23.202.200 (2011. godina)	245
Tabela 88. Linux OS – Pronađeni servisi na IP adresi 172.23.202.230 (2011. godina)	250
Tabela 89. Linux OS – Pronađeni servisi na IP adresi 172.23.202.135 (2011. godina)	255
Tabela 90. Linux OS – Pronađeni servisi na IP adresi 172.23.202.231 (2011. godina)	261
Tabela 91. Linux OS sa IP adresama 172.23.202.133, 172.23.202.132, 172.23.202.123, 172.23.202.229 (2011. godina).....	266
Tabela 92. Linux OS – Pronađeni servisi na IP adresi 172.23.202.133 (2011. godina)	279
Tabela 93. Linux OS – Pronađeni servisi na IP adresi 172.23.202.132 (2011. godina)	284
Tabela 94. Linux OS – Pronađeni servisi na IP adresi 172.23.202.123 (2011. godina)	289
Tabela 95. Linux OS – Pronađeni servisi na IP adresi 172.23.202.229 (2011. godina)	294
Tabela 96. Linux OS sa IP adresama 172.23.202.197 (2011. godina).....	300
Tabela 97. Linux OS – Pronađeni servisi na IP adresi 172.23.202.197 (2011. godina)	308
Tabela 98. Linux OS sa IP adresama 172.23.202.199, 172.23.202.224 (2011. godina)	310
Tabela 99. Linux OS – Pronađeni servisi na IP adresi 172.23.202.199 (2011. godina)	317
Tabela 100. Linux OS – Pronađeni servisi na IP adresi 172.23.202.224 (2011. godina)	319
Tabela 101. Linux OS sa IP adresama 172.23.202.198, 172.23.202.223 (2011. godina).....	322
Tabela 102. Linux OS – Pronađeni servisi na IP adresi 172.23.202.198 (2011. godina)	327
Tabela 103. Linux OS – Pronađeni servisi na IP adresi 172.23.202.223 (2011. godina)	329
Tabela 104. Linux OS sa IP adresama 172.23.202.131 (2011. godina).....	331
Tabela 105. Linux OS – Pronađeni servisi na IP adresi 172.23.202.131 (2011. godina)	335
Tabela 106. Linux OS sa IP adresama 172.23.202.125 (2011. godina).....	338
Tabela 107. Linux OS – Pronađeni servisi na IP adresi 172.23.202.125 (2011. godina)	341
Tabela 108. Windows OS sa IP adresama 172.23.202.109, 172.23.202.106, 172.23.202.69 (2013. godina)	342
Tabela 109. Windows OS sa IP adresom 172.23.202.107 (2013. godina).....	352
Tabela 110. Windows OS sa IP adresama 172.23.202.110, 172.23.202.76 (2013. godina)	355
Tabela 111. Windows OS sa IP adresama 172.23.202.111, 172.23.202.75, 172.23.202.74, 172.23.202.73 (2013. godina).....	367
Tabela 112. Windows OS sa IP adresom 172.23.202.101 (2013. godina).....	373
Tabela 113. Windows OS sa IP adresama 172.23.202.112, 172.23.202.72, 172.23.202.71, 172.23.202.70 (2013. godina).....	381

Tabela 114. Windows OS sa IP adresama 172.23.202.113, 172.23.202.89, 172.23.202.88, 172.23.202.87, 172.23.202.86, 172.23.202.85, 172.23.202.84, 172.23.202.83 (2013. godina)	385
Tabela 115. Windows OS sa IP adresama 172.23.202.114, 172.23.202.82, 172.23.202.81, 172.23.202.80, 172.23.202.79, 172.23.202.78, 172.23.202.77 (2013. godina)	389
Tabela 116. Windows OS sa IP adresama 172.23.202.117, 172.23.202.68 (2013. godina)	391
Tabela 117. Windows OS sa IP adresom 172.23.202.108 (2013. godina).....	394
Tabela 118. Windows OS sa IP adresom 172.23.202.105 (2013. godina).....	395
Tabela 119. Windows OS sa IP adresama 172.23.202.115, 172.23.202.116, 172.23.202.100, 172.23.202.99, 172.23.202.98, 172.23.202.97, 172.23.202.96, 172.23.202.95, 172.23.202.94, 172.23.202.93, 172.23.202.92, 172.23.202.91, 172.23.202.90 (2013. godina)	404
Tabela 120. Windows OS sa IP adresom 172.23.202.118 (2013. godina).....	406
Tabela 121. Windows OS sa IP adresom 172.23.202.103 (2013. godina).....	407
Tabela 122. Windows OS sa IP adresom 172.23.202.104 (2013. godina).....	408
Tabela 123. Windows OS sa IP adresom 172.23.202.102 (2013. godina).....	409
Tabela 124. Linux OS sa IP adresama 172.23.202.124, 172.23.202.220 (2013. godina)	410
Tabela 125. Linux OS sa IP adresama 172.23.202.126, 172.23.202.225 (2013. godina)	437
Tabela 126. Linux OS sa IP adresama 172.23.202.193, 172.23.202.227, 172.23.202.194, 172.23.202.226, (2013. godina).....	468
Tabela 127. Linux OS sa IP adresama 172.23.202.195, 172.23.202.196, 172.23.202.221, 172.23.202.222, (2013. godina).....	496
Tabela 128. Linux OS sa IP adresama 172.23.202.122, 172.23.202.232, 172.23.202.200, 172.23.202.230, 172.23.202.135, 172.23.202.231 (2013. godina)	525
Tabela 129. Linux OS sa IP adresama 172.23.202.133, 172.23.202.132, 172.23.202.123, 172.23.202.229 (2013. godina).....	541
Tabela 130. Linux OS sa IP adresom 172.23.202.197 (2013. godina)	560
Tabela 131. Linux OS sa IP adresama 172.23.202.199, 172.23.202.224 (2013. godina)	575
Tabela 132. Linux OS sa IP adresama 172.23.202.198, 172.23.202.223 (2013. godina)	590
Tabela 133. Linux OS sa IP adresom 172.23.202.131 (2013. godina)	602
Tabela 134. Linux OS sa IP adresom 172.23.202.125 (2013. godina)	612

4.3.1 WINDOWS OPERATIVNI SISTEMI - SKENIRANJE SERVISA NA RANJIVOSTI U 2011.

Tabela 1. Windows OS sa IP adresama 172.23.202.69, 172.23.202.106, 172.23.202.109 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.109		OS: Microsoft Windows XP tablet edition SP1 x86, WINXPTabX86sp1			15
IP adresa: 172.23.202.106		OS: Microsoft Windows XP pro sp1 x86, WINXPproSP1x86			15
IP adresa: 172.23.202.69		OS: Microsoft Windows XP pro sp1 x64, WINXPproSP1x64			15
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Microsoft Server Service / CanonicalizePathName() Remote Code Execution Vulnerability (dcerpc-msnetapi-netpathcanonicalize-dos)	Odredene verzije Microsoft Windows-a su ranjive na daljinsko preopterećenje bafera (privremene memorije) koje bi moglo da kompromituje određeni računar. Posebno izrađen paket se može koristiti sa pozivom ka NetPathCanonicalize RPC ruti na servisu servera, pri čemu bi napadač mogao da izvrši kôd pod sistemskim nivoom pristupa.	CVE: CVE-2006-3439 ¹ , MS: MS06-040 ² , MSKB: 921883 ³ , SANS-06: W4 ⁴ , SANS-07: S2 ⁵	Kritičan	Uraditi download a zatim instalirati Microsoft patch za 32-bitnu verziju : WindowXP-KB921883-x86-ENU.EXE ⁶ ili za 64-bitnu verziju Windowsa: WindowsServer2003.WindowsXP-KB921883-v2-x64-ENU.exe ⁷
2.	MS03-039: Buffer Overrun In RPCSS Service Could Allow Code Execution (824146) (windows-hotfix-ms03-039)	Napadač koji je uspešno iskoristio ovu ranjivost bi mogao biti u mogućnosti da pokrene kôd sa privilegijama lokalnog sistema na pogođenom sistemu ili bi mogao da prouzrokuje kvar RPCSS servisa. Napadač bi tada mogao biti u mogućnosti da preduzme bilo kakvu radnju na sistemu, uključujući instaliranje programa, pregledanje, izmene i brisanje podataka ili kreiranje novih naloga sa svim privilegijama. Da bi iskoristio ove ranjivosti, napadač bi mogao da napravi program sa kojim bi poslao	BID: 8458 ⁸ , CVE: CVE-2003-0528 ⁹ , CVE: CVE-2003-0605 ¹⁰ , CVE: CVE-2003-0715 ¹¹ , MSKB: 824146 ¹² , MS: MS03-039 ¹³	Kritičan	Uraditi download a zatim instalirati Microsoft patch za 32-bitnu verziju : WindowsXP-KB824146-x86-ENU.exe (1543456 bytes) ¹⁴ , ili za 64-bitnu verziju Windowsa : WindowsXP-KB824146-ia64-ENU.exe ¹⁵ Uraditi download a zatim instalirati Microsoft patch DirectX9-KB819696-x86-ENU.exe (970312 bytes) ¹⁶

¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-3439>

² <http://technet.microsoft.com/en-us/security/bulletin/ms06-040>

³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;921883>

⁴ <http://www.sans.org/critical-security-controls/#w4>

⁵ <http://www.sans.org/critical-security-controls/#s2>

⁶ download.microsoft.com/download/c/2/b/c2b41862-1113-4e40-a81a-d6971733e361/WindowsXP-KB921883-x86-ENU.exe

⁷ <http://download.microsoft.com/download/0/f/9/0f9eb45e-cb70-40dd-8506-8cdf226731f7/WindowsServer2003.WindowsXP-KB921883-v2-x64-ENU.exe>

⁸ <http://www.securityfocus.com/bid/8458>

⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0528>

¹⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0605>

¹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0715>

¹² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;824146>

¹³ <http://technet.microsoft.com/en-us/security/bulletin/ms03-039>

¹⁴ www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb824146-x86-enu_b957699c7365c462446bd552cd6d203.exe

¹⁵ <http://download.microsoft.com/download/a/c/e/ace7fe00-4bf7-4421-8ccf-2913395500aa/WindowsXP-KB824146-ia64-ENU.exe>

¹⁶ www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/directx9-kb819696-x86-enu_977f8cc86c1e151a0168d1296210913.exe

		malicioznu RPC poruku ranjivom sistemu, ciljajući RPCSS servis.			
3.	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (windows-hotfix-ms08-067)	172.23.202.109:139 172.23.202.109:445 172.23.202.106:139 172.23.202.106:445 172.23.202.69:139 172.23.202.69:445 Ovo ažuriranje bezbednosti rešava ranjivost koja je prijavljena od strane privatnog lica. Ranjivost bi mogla da omogući daljinsko izvršavanje koda ukoliko je napadnuti sistem primio posebno izrađen RPC zahtev. Na sistemima Microsoft Windows 2000, Windows XP, i Windows Server 2003, napadač bi mogao da iskoristi ovu ranjivost bez proveravanja autentičnosti i da pokrene proizvoljan kôd. Moguće je da ova ranjivost može biti upotrebljena za intenziviranje skrivenog korišćenja exploit-a. Praksa je pokazala da upotreba zaštitnog zida može da pomogne u zaštiti mrežnih resursa od napada koji potiču izvan okvira organizacije.	MS: MS08-067 ¹⁷ MSKB: 958644 ¹⁸ CVE: CVE-2008-4250 ¹⁹ SECUNIA: 32326 ²⁰ URL1 ²¹ URL2 ²² URL3 ²³	Kritičan	Uraditi download a zatim instalirati Microsoft patch za 32-bitnu verziju : WindowsXP-KB958644-x86-ENU.exe (648560 bytes) ²⁴ ili za 64-bitnu verziju Windowsa : WindowsServer2003.WindowsXP-KB958644-x64-ENU.exe ²⁵
4.	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (windows-hotfix-ms09-001)	172.23.202.109:139 172.23.202.109:445 172.23.202.106:139 172.23.202.106:445 172.23.202.69:139 172.23.202.69:445 Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti koje su privatno prijavljene a odnose se na protokol Microsoft Server Message Block-a (SMB). Ranjivosti mogu da omoguće daljinsko izvršenje kôda na ugroženim sistemima. Napadač koji je uspešno iskoristion ove ranjivosti može da instalira programe, pregleda, menja ili briše podatke ili otvara nove naloge sa potpunim korisničkim	MS: MS09-001 ²⁶ MSKB: 958687 ²⁷ CVE: CVE-2008-4114 ²⁸ CVE: CVE-2008-4835 ²⁹ CVE: CVE-2008-4834 ³⁰ SECUNIA: 31883 ³¹ URL1 ³² URL2 ³³ URL3 ³⁴	Kritičan	Uraditi download a zatim instalirati Microsoft patch za 32-bitnu verziju : WindowsXP-KB958687-x86-ENU.exe (658288 bytes) ³⁵ ili za 64-bitnu verziju Windowsa : WindowsServer2003.WindowsXP-KB958687-x64-ENU.exe ³⁶

¹⁷ <http://technet.microsoft.com/en-us/security/bulletin/ms08-067>¹⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958644>¹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4250>²⁰ <http://secunia.com/advisories/32326/>²¹ blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx²² <http://blogs.msdn.com/b/sdl/archive/2008/10/22/ms08-067.aspx>²³ <http://blogs.technet.com/b/msrc/archive/2008/10/23/ms08-067-released.aspx>²⁴ http://download.windowsupdate.com/msdownload/update/software/secu/2008/10/windowsxpb958644-x86-enu_5c135a8dae5721849430afe27af255f83e64f62b.exe²⁵ <http://download.microsoft.com/download/5/8/1/5811b6cc-5884-4486-b05d-de69f0e94f67/WindowsServer2003.WindowsXP-KB958644-x64-ENU.exe>²⁶ <http://technet.microsoft.com/en-us/security/bulletin/MS09-001>²⁷ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958687>²⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4114>²⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4835>³⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4834>³¹ <http://secunia.com/advisories/31883/>³² http://www.vallejo.cc/proyectos/vista_SMB_write_DoS.htm³³ <http://www.zerodayinitiative.com/advisories/ZDI-09-001/>³⁴ <http://www.zerodayinitiative.com/advisories/ZDI-09-002/>³⁵ http://download.windowsupdate.com/msdownload/update/software/secu/2008/12/windowsxp-kb958687-x86-enu_a9b85264e9b75e552ae10cd212937b8686a96833.exe³⁶ <http://download.microsoft.com/download/6/6/B/66B29397-A4AB-4586-BEFF-68379C94E99F/WindowsServer2003.WindowsXP-KB958687-x64-ENU.exe>

		pravima. Praksa je pokazala da zaštitni zid i njegove standardne konfiguracije po defaultu mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan okvira organizacije. Za sisteme koji su stalno povezani na Internet preporuka je da imaju što manji broj izloženih portova.			
5.	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-012)	172.23.202.109:139 172.23.202.109:445 172.23.202.106:139 172.23.202.106:445 172.23.202.69:139 172.23.202.69:445 Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti koje su privatno prijavljene u Microsoft Windows-u. Opasnost od ove ranjivosti leži u tome što bi ona omogućila daljinsko izvršavanje kôda ukoliko bi napadač kreirao posebno opremljeni SMB paket i poslao ga ugroženom sistemu. Praksa je pokazala da upotreba zaštitnog zida može da pomogne u zaštiti mrežnih resursa od napada (koji bi pokušali da iskoriste ove ranjivosti), a koji potiču izvan okvira organizacije.	MS: MS10-012 ³⁷ MSKB - 971468 ³⁸ CVE: CVE-2010-0020 ³⁹ CVE: CVE-2010-0021 ⁴⁰ CVE: CVE-2010-0022 ⁴¹ CVE CVE-2010-0231 ⁴² SECUNIA 38510 ⁴³	Kritičan	Uraditi download a zatim instalirati Microsoft patch za 32-bitnu verziju : WindowsXP-KB971468-x86-ENU.exe (664952 bytes) ⁴⁴ ili za 64-bitnu verziju Windowsa : WindowsServer2003.WindowsXP-KB971468-x64-ENU.exe ⁴⁵
6.	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-054)	172.23.202.109:139 172.23.202.109:445 172.23.202.106:139 172.23.202.106:445 172.23.202.69:139 172.23.202.69:445 Opis je isti kao kod ranjivosti MS10-012	CVE: CVE-2010-2550 ⁴⁶ CVE: CVE-2010-2551 ⁴⁷ CVE: CVE-2010-2552 ⁴⁸ MS: MS10-054 ⁴⁹ MSKB 982214 ⁵⁰	Kritičan	Uraditi download a zatim instalirati Microsoft patch za 32-bitnu verziju : windowsxp-kb982214-x86-enu.exe (661368 bytes) ⁵¹ ili za 64-bitnu verziju Windowsa : WindowsServer2003.WindowsXP-KB982214-x64-ENU.exe ⁵²
7.	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution	172.23.202.109:139 172.23.202.109:445 172.23.202.106:139 172.23.202.106:445	CVE: CVE-2011-0661 ⁵³ MS: MS11-020 ⁵⁴ MSKB: 2508429 ⁵⁵	Kritičan	Uraditi download a zatim instalirati Microsoft patch za 32-bitnu verziju : windowsxp-kb2508429-

³⁷ <http://technet.microsoft.com/en-us/security/bulletin/MS10-012>³⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;971468>³⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0020>⁴⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0021>⁴¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0022>⁴² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0231>⁴³ <http://secunia.com/advisories/38510/>⁴⁴ http://download.windowsupdate.com/msdownload/update/software/secu/2010/01/windowsxp-kb971468-x86-enu_68d7899c8b8462219daf40f02c6fb9f362b1ee6b.exe⁴⁵ <http://download.microsoft.com/download/6/0/8/6086ED38-9FC7-476F-BE60-F67E56A335FB/WindowsServer2003.WindowsXP-KB971468-x64-ENU.exe>⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2550>⁴⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2551>⁴⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2552>⁴⁹ <http://technet.microsoft.com/en-us/security/bulletin/MS10-054>⁵⁰ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;982214>⁵¹ http://download.windowsupdate.com/msdownload/update/software/secu/2010/07/windowsxp-kb982214-x86-enu_a24853f682dad3157da4e4a39372951a8ec1e407.exe⁵² <http://download.microsoft.com/download/6/9/3/693AA8A1-BC95-4504-9AD8-3E69D4D2D1B3/WindowsServer2003.WindowsXP-KB982214-x64-ENU.exe>⁵³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661>⁵⁴ <http://technet.microsoft.com/en-us/security/bulletin/ms11-020>⁵⁵ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;2508429>

	(windows-hotfix-ms11-020)	172.23.202.69:139 172.23.202.69:445 Opis je isti kao kod ranjivosti MS10-012			x86-enu.exe (664960 bytes) ⁵⁶ ili za 64-bitnu verziju Windowsa : WindowsServer2003.WindowsXP-KB2508429-x64-ENU.exe ⁵⁷
8.	MS03-026: Buffer Overrun In RPC Interface Could Allow Code Execution (823980) (windows-hotfix-ms03-026)	Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti u Windows Distributed Component Object Model-u (DCOM) preko Remote Procedure Call-a (RPC). Napadač koji bi uspešno iskoristio ovu ranjivost mogao bi da pokrene kôd sa privilegijama lokalnog sistema na napadnutom sistemu. Napadač bi mogao da preduzme bilo kakvu akciju na sistemu, uključujući instaliranje programa, pregledanje, izmenu ili brisanje podataka ili otvaranje novih naloga sa svim privilegijama. Da bi iskoristio ovu ranjivost, napadač bi morao da pošalje posebno formiran zahtev udaljenom računaru ka specifičnim RPC portovima.	CVE: CVE-2003-0352 ⁵⁸ MS: MS03-026 ⁵⁹ BID: 8205 ⁶⁰ MSKB: 823980 ⁶¹	Kritičan	Uraditi download a zatim instalirati Microsoft patch za 32-bitnu verziju : WindowsXP-KB823980-x86-ENU.exe (1291040 bytes) ⁶² ili za 64-bitnu verziju Windowsa : WindowsXP-KB823980-ia64-ENU.exe ⁶³
9.	MS04-011: Security Update for Microsoft Windows (835732) (windows-hotfix-ms04-011)	172.23.202.109:139 172.23.202.109:445 172.23.202.106:139 172.23.202.106:445 172.23.202.69:139 172.23.202.69:445 Ovo ažuriranje rešava nekoliko novootkrivenih ranjivosti. Napadač koji uspešno iskoristi ovu ranjivost bi mogao da preuzme potpunu kontrolu nad napadnutim sistemom, uključujući instaliranje programa, pregledanje, menjanje ili brisanje podataka ili čak otvaranje novih naloga sa svim privilegijama.	BID 10108 ⁶⁴ BID 10113 ⁶⁵ BID 10114 ⁶⁶ BID 10115 ⁶⁷ BID 10117 ⁶⁸ BID 10118 ⁶⁹ BID 10119 ⁷⁰ BID 10120 ⁷¹ BID 10122 ⁷² BID 10124 ⁷³ BID 10125 ⁷⁴ BID 10126 ⁷⁵ CERT-VN 122076 ⁷⁶ CERT-VN 150236 ⁷⁷ CERT-VN 206468 ⁷⁸ CERT-VN 255924 ⁷⁹	Kritičan	Uraditi download a zatim instalirati Microsoft patch za 32-bitnu verziju : WindowsXP-KB835732-x86-ENU.EXE (2710296 bytes) ¹⁵⁹ ili za 64-bitnu verziju Windowsa : WindowsXP-KB835732-IA64-ENU.EXE ¹⁶⁰

⁵⁶http://download.windowsupdate.com/msdownload/update/software/secu/2011/03/windowsxp-kb2508429-x86-enu_e0b40d81f2ecc1bad43439a6bd0a9e2a0ab7dd56.exe

⁵⁷<http://download.microsoft.com/download/8/3/3/833C20D2-59EA-4D23-960F-11270C0C0319/WindowsServer2003.WindowsXP-KB2508429-x64-ENU.exe>

⁵⁸<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0352>

⁵⁹<http://technet.microsoft.com/en-us/security/bulletin/ms03-026>

⁶⁰<http://www.securityfocus.com/bid/8205>

⁶¹<http://support.microsoft.com/default.aspx?scid=kb;EN-US;823980>

⁶²http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb823980-x86-enu_1d296adab6699e66210e5a350236381.exe

⁶³<http://download.microsoft.com/download/a/7/5/a75b3c8f-5df0-451b-b526-cfc7c5c67df5/WindowsXP-KB823980-ia64-ENU.exe>

⁶⁴<http://www.securityfocus.com/bid/10108>

⁶⁵<http://www.securityfocus.com/bid/10113>

⁶⁶<http://www.securityfocus.com/bid/10114>

⁶⁷<http://www.securityfocus.com/bid/10115>

⁶⁸<http://www.securityfocus.com/bid/10117>

⁶⁹<http://www.securityfocus.com/bid/10118>

⁷⁰<http://www.securityfocus.com/bid/10119>

⁷¹<http://www.securityfocus.com/bid/10120>

⁷²<http://www.securityfocus.com/bid/10122>

⁷³<http://www.securityfocus.com/bid/10124>

⁷⁴<http://www.securityfocus.com/bid/10125>

⁷⁵<http://www.securityfocus.com/bid/10126>

⁷⁶<http://www.kb.cert.org/vuls/id/122076>

⁷⁷<http://www.kb.cert.org/vuls/id/150236>

⁷⁸<http://www.kb.cert.org/vuls/id/206468>

⁷⁹<http://www.kb.cert.org/vuls/id/255924>

			CERT-VN 260588 ⁸⁰ CERT-VN 353956 ⁸¹ CERT-VN 471260 ⁸² CERT-VN 526084 ⁸³ CERT-VN 547028 ⁸⁴ CERT-VN 586540 ⁸⁵ CERT-VN 638548 ⁸⁶ CERT-VN 639428 ⁸⁷ CVE CVE-2003-0663 ⁸⁸ CVE CVE-2003-0719 ⁸⁹ CVE CVE-2003-0806 ⁹⁰ CVE CVE-2003-0906 ⁹¹ CVE CVE-2003-0907 ⁹² CVE CVE-2003-0908 ⁹³ CVE CVE-2003-0909 ⁹⁴ CVE CVE-2003-0910 ⁹⁵ CVE CVE-2004-0117 ⁹⁶ CVE CVE-2004-0118 ⁹⁷ CVE CVE-2004-0119 ⁹⁸ CVE CVE-2004-0120 ⁹⁹ CVE CVE-2004-0123 ¹⁰⁰ OVAL OVAL1004 ¹⁰¹ OVAL OVAL1007 ¹⁰² OVAL OVAL1016 ¹⁰³ OVAL OVAL1046 ¹⁰⁴ OVAL OVAL1054 ¹⁰⁵ OVAL OVAL1064 ¹⁰⁶ OVAL OVAL1076 ¹⁰⁷ OVAL OVAL1093 ¹⁰⁸ OVAL OVAL1512 ¹⁰⁹ OVAL OVAL1718 ¹¹⁰ OVAL OVAL1808 ¹¹¹ OVAL OVAL1962 ¹¹² OVAL OVAL1997 ¹¹³		

¹⁵⁹ http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb835732-x86-enu_99fc98fc8e8cbf6720f28028a1f05eb.exe

¹⁶⁰ <http://download.microsoft.com/download/6/b/4/6b4af6c4-62c6-44b2-8d29-9b305636d0b6/WindowsXP-KB835732-IA64-ENU.EXE>

⁸⁰ <http://www.kb.cert.org/vuls/id/260588>

⁸¹ <http://www.kb.cert.org/vuls/id/353956>

⁸² <http://www.kb.cert.org/vuls/id/471260>

⁸³ <http://www.kb.cert.org/vuls/id/526084>

⁸⁴ <http://www.kb.cert.org/vuls/id/547028>

⁸⁵ <http://www.kb.cert.org/vuls/id/586540>

⁸⁶ <http://www.kb.cert.org/vuls/id/638548>

⁸⁷ <http://www.kb.cert.org/vuls/id/639428>

⁸⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0663>

⁸⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0719>

⁹⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0806>

⁹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0906>

⁹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0907>

⁹³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0908>

⁹⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0909>

⁹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0910>

⁹⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0117>

⁹⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0118>

⁹⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0119>

⁹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0120>

¹⁰⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0123>

¹⁰¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1004>

¹⁰² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1007>

¹⁰³ oval.mitre.org/oval/definitions/data/OVAL1016.html

¹⁰⁴ oval.mitre.org/oval/definitions/data/OVAL1046.html

¹⁰⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1054>

¹⁰⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1064>

¹⁰⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1076>

¹⁰⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1093>

¹⁰⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1512>

¹¹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1718>

¹¹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1808>

¹¹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1962>

			OVAL OVAL883 ¹¹⁴ OVAL OVAL885 ¹¹⁵ OVAL OVAL886 ¹¹⁶ OVAL OVAL889 ¹¹⁷ OVAL OVAL890 ¹¹⁸ OVAL OVAL892 ¹¹⁹ OVAL OVAL895 ¹²⁰ OVAL OVAL896 ¹²¹ OVAL OVAL897 ¹²² OVAL OVAL898 ¹²³ OVAL OVAL903 ¹²⁴ OVAL OVAL904 ¹²⁵ OVAL OVAL907 ¹²⁶ OVAL OVAL911 ¹²⁷ OVAL OVAL919 ¹²⁸ OVAL OVAL924 ¹²⁹ OVAL OVAL946 ¹³⁰ OVAL OVAL951 ¹³¹ OVAL OVAL959 ¹³² OVAL OVAL964 ¹³³ URL1 ¹³⁴ URL2 ¹³⁵ URL3 ¹³⁶ URL4 ¹³⁷ URL5 ¹³⁸ URL6 ¹³⁹ URL7 ¹⁴⁰ URL8 ¹⁴¹ XF ssl-message- dos(15712) ¹⁴² XF win-asn1-double- free(15713) ¹⁴³ XF win-h323- bo(15710) ¹⁴⁴ XF win-hcpurl-code- execution(15704) ¹⁴⁵		

- ¹¹³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1997>
- ¹¹⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:883>
- ¹¹⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:885>
- ¹¹⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:886>
- ¹¹⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:889>
- ¹¹⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:890>
- ¹¹⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:892>
- ¹²⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:895>
- ¹²¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:896>
- ¹²² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:897>
- ¹²³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:898>
- ¹²⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:903>
- ¹²⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:904>
- ¹²⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:907>
- ¹²⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:911>
- ¹²⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:919>
- ¹²⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:924>
- ¹³⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:946>
- ¹³¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:951>
- ¹³² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:959>
- ¹³³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:964>
- ¹³⁴ <http://archives.neohapsis.com/archives/vulnwatch/2004-q1/0081.html>
- ¹³⁵ <http://archives.neohapsis.com/archives/vulnwatch/2004-q1/0082.html>
- ¹³⁶ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020065.html>
- ¹³⁷ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020068.html>
- ¹³⁸ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020069.html>
- ¹³⁹ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020070.html>
- ¹⁴⁰ <http://www.securiteam.com/windowsntfocus/5LP0C2ACKU.html>
- ¹⁴¹ <http://www.securityfocus.com/archive/1/361836>
- ¹⁴² <http://xforce.iss.net/xforce/xfdb/15712>
- ¹⁴³ <http://xforce.iss.net/xforce/xfdb/15713>
- ¹⁴⁴ <http://xforce.iss.net/xforce/xfdb/15710>
- ¹⁴⁵ <http://xforce.iss.net/xforce/xfdb/15704>

			XF win-ldt-gain-privileges(15707)¹⁴⁶ XF win-lsass-bo(15699)¹⁴⁷ XF win-spp-bo(15715)¹⁴⁸ XF win-vdm-gain-privileges(15714)¹⁴⁹ XF win-winlogon-bo(15702)¹⁵⁰ XF win2k-lsass-ldap-dos(15700)¹⁵¹ XF win2k-utilitymgr-gain-privileges(15632) MS: MS04-011¹⁵², CVE: CVE-2003-0533¹⁵³ MSKB: 835732¹⁵⁴ OVAL: OVAL1000¹⁵⁵ CERT-VN: 753212¹⁵⁶ CERT-VN: 783748¹⁵⁷ XF: winxp-task-gain-privileges(15678)¹⁵⁸		
10.	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (windows-hotfixms06-035)	Ovo ažuriranje rešava nekoliko otkrivenih i privatno prijavljenih ranjivosti. Preporučuje se da korisnici odmah primene update.	CVE: CVE-2006-1314¹⁶¹ CVE: VE-2006-1315¹⁶² MS: MS06-035¹⁶³ MSKB: 917159¹⁶⁴ SANS-06: W4¹⁶⁵ SANS-07: S2¹⁶⁶ SECUNIA: 21007¹⁶⁷ XF: win-mailslot-bo(26818)¹⁶⁸ XF win-smb-information-disclosure(26820)¹⁶⁹	Kritičan	Uraditi download a zatim instalirati Microsoft patch za 32-bitnu verziju : WindowsXP-KB917159-x86-ENU.exe (725304 bytes) ¹⁷⁰ ili za 64-bitnu verziju Windowsa : WindowsServer2003.WindowsXP-KB917159-x64-ENU.exe ¹⁷¹
11.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.109:139 172.23.202.109:445 172.23.202.106:139 172.23.202.106:445 172.23.202.69:139 172.23.202.69:445	MSKB: 887429¹⁷² URL1¹⁷³	Ozbiljan	Metoda za konfigurisanje SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429 ¹⁷⁴ . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena

¹⁴⁶ <http://xforce.iss.net/xforce/xfdb/15707>¹⁴⁷ <http://xforce.iss.net/xforce/xfdb/15699>¹⁴⁸ <http://xforce.iss.net/xforce/xfdb/15715>¹⁴⁹ <http://xforce.iss.net/xforce/xfdb/15714>¹⁵⁰ <http://xforce.iss.net/xforce/xfdb/15702>¹⁵¹ <http://xforce.iss.net/xforce/xfdb/15700>¹⁵² <http://technet.microsoft.com/en-us/security/bulletin/ms04-011>¹⁵³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0533>¹⁵⁴ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;835732>¹⁵⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1000>¹⁵⁶ <http://www.kb.cert.org/vuls/id/753212>¹⁵⁷ <http://www.kb.cert.org/vuls/id/783748>¹⁵⁸ <http://xforce.iss.net/xforce/xfdb/15678>¹⁶¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1314>¹⁶² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1315>¹⁶³ <http://technet.microsoft.com/en-us/security/bulletin/ms06-035>¹⁶⁴ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;917159>¹⁶⁵ <http://www.sans.org/critical-security-controls/#w4>¹⁶⁶ <http://www.sans.org/critical-security-controls/#s2>¹⁶⁷ <http://secunia.com/advisories/21007/>¹⁶⁸ <http://xforce.iss.net/xforce/xfdb/26818>¹⁶⁹ <http://xforce.iss.net/xforce/xfdb/26820>¹⁷⁰ http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb917159-x86-enu_5ed838e18ceae61a8d94f8c4be2462a8e19212d7.exe¹⁷¹ <http://download.microsoft.com/download/7/e/3/7e3fa65f-f3bc-49be-8b92-9e19f9793933/WindowsServer2003.WindowsXP-KB917159-x64-ENU.exe>¹⁷² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429>¹⁷³ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>¹⁷⁴ <http://support.microsoft.com/kb/887429>

		Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).			prema serveru. Na Samba serveru (na konfiguracionom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing = auto</i> ili da se zahteva SMB potpisivanje: <i>server signing = mandatory</i>
12.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.109:139 172.23.202.109:445 172.23.202.106:139 172.23.202.106:445 172.23.202.69:139 172.23.202.69:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti.
13.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	172.23.202.109:135 172.23.202.106:135 172.23.202.69:135 Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183 ¹⁷⁵ CERT-VN: 415294 ¹⁷⁶ CVE CVE-2004-0230 ¹⁷⁷ MS: MS05-019 ¹⁷⁸ MS: MS06-064 ¹⁷⁹ NETBSD: NetBSD-SA2004-006 ¹⁸⁰ OVAL: OVAL2689 ¹⁸¹ OVAL: OVAL270 ¹⁸² OVAL OVAL3508 ¹⁸³ OVAL OVAL4791 ¹⁸⁴ OVAL OVAL5711 ¹⁸⁵ SECUNIA: 11440 ¹⁸⁶ SECUNIA: 22341 ¹⁸⁷ SGI 20040403-01-A ¹⁸⁸	Ozbiljan	Uraditi download a zatim instalirati Microsoft patch za 32-bitnu verziju : WindowsXP-KB893066-v2-x86-ENU.exe (791280 bytes) ¹⁸⁹ ili za 64-bitnu verziju Windowsa : WindowsXP-KB893066-v2-ia64-ENU.exe ¹⁹⁰
14	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server. Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko poziva udaljenih procedura (RPC). Ovi	BID: 494 ¹⁹¹ CVE: CVE-1999-0519 ¹⁹² MSKB: 143474 ¹⁹³ URL1 ¹⁹⁴	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost.

¹⁷⁵ <http://www.securityfocus.com/bid/10183>¹⁷⁶ <http://www.kb.cert.org/vuls/id/415294>¹⁷⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>¹⁷⁸ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>¹⁷⁹ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>¹⁸⁰ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>¹⁸¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>¹⁸² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>¹⁸³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>¹⁸⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>¹⁸⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>¹⁸⁶ <http://secunia.com/advisories/11440/>¹⁸⁷ <http://secunia.com/advisories/22341/>¹⁸⁸ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>¹⁸⁹ http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb893066-v2-x86-enu_3d2029a4300c0b7943b20c1287c8143087045d52.exe¹⁹⁰ <http://download.microsoft.com/download/0/6/c/06cda61b-b868-4b3d-a07e-3d60501ac2cb/WindowsXP-KB893066-v2-ia64-ENU.exe>¹⁹¹ <http://www.securityfocus.com/bid/494>¹⁹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>¹⁹³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>¹⁹⁴ http://www.hsc.fr/ressources/presentations/null_sessions/

		servisi su i u prošlosti bili skloni ranjivostima.. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinjenije napade.			
15.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	CVE: CVE-1999-0524 ¹⁹⁵ XF: icmp-netmask(306) ¹⁹⁶ XF: icmp-timestamp(322) ¹⁹⁷	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.

Tabela 2. Windows OS – Pronađeni servisi na IP adresi 172.23.202.109 (2011. godina)

Ip adresa	172.23.202.109
SPIDERED WEB SITES	http://172.23.202.109:5000 Sledeće URL adrese su pronađene. One su često uključene u WEB servere po difoltu ili nakon instaliranih dodataka (eng add-ons) : Error (400) exchange default.asp
FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni dedljeni resuers, mount-point: C:\
SERVISI	CIFS ¹⁹⁸ , CIFS Name Service ¹⁹⁹ : advertised-name-1: WINXPTabX86sp1 (Computer Name) advertised-name-2: WINXPTabX86sp1 (File Server Service) advertised-name-3: WORKGROUP (Domain Name) mac-address: 000C293EC90A DCE RPC ²⁰⁰ : interface-uuid: 5A7B91F8-FF00-11D0-A9B2-00C04FB6E6FC interface-version: 1 name: Messenger Service protocol-sequence: ncacn_ip_tcp:172.23.202.109[1025] interface-uuid: 5A7B91F8-FF00-11D0-A9B2-00C04FB6E6FC interface-version: 1

¹⁹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>¹⁹⁶ <http://xforce.iss.net/xforce/xfdb/306>¹⁹⁷ <http://xforce.iss.net/xforce/xfdb/322>¹⁹⁸ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).¹⁹⁹ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.²⁰⁰ DCE/RPC predstavlja implementaciju Remote Procedure Call tehnologije razvijenu od strane Open Group kao deo Distributed Computing Environment. DCE/RPC najčešće se koristi u interakciji sa Windows mrežnim servisima. DCE/RPC na jedan impresivan način poziva procedure iz jedne aplikacije u drugu aplikaciju bez potrebe da se zna na kakvom računaru je ta aplikacija pokrenuta (izvor : <http://www.samba-tng.org/docs/tng-arch/tng-arch05.html>).

	name: Messenger Service protocol-sequence: ncadg_ip_udp:172.23.202.109[1027] NTP: 172.23.202.109 udp 123 UPnP-HTTPU: 172.23.202.109 tcp 5000

Tabela 3. Windows OS – Pronađeni servisi na IP adresi 172.23.202.106 (2011. godina)

Ip adresa	172.23.202.106
SPIDERED WEB SITES	http://172.23.202.106:5000 Sledeće URL adrese su pronađene. One su često uključene u WEB servere po defaultu ili nakon instaliranih dodataka (eng add-ons): Error (400) exchange default.asp
FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - defaultni deljeni resurs, mount-point: C:\
SERVISI	CIFS ²⁰¹ , CIFS Name Service ²⁰² : advertised-name-1: WINXPproSP1x86 (Computer Name) advertised-name-2: WINXPproSP1x86 (File Server Service) advertised-name-3: WORKGROUP (Domain Name) advertised-name-4: WORKGROUP (Browser Service Elections) advertised-name-5: WORKGROUP (Master Browser) DCE RPC ²⁰³ : interface-uuid: 5A7B91F8-FF00-11D0-A9B2-00C04FB6E6FC interface-version: 1 name: Messenger Service protocol-sequence: ncacn_ip_tcp:172.23.202.174[1025] interface-uuid: 5A7B91F8-FF00-11D0-A9B2-00C04FB6E6FC interface-version: 1 name: Messenger Service protocol-sequence: ncadg_ip_udp:172.23.202.174[1026] mac-address: 000C2909EE2D NTP: 172.23.202.106 udp 123 UPnP-HTTPU: 172.23.202.106 tcp 5000

²⁰¹ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

²⁰² Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

²⁰³ DCE/RPC predstavlja implementaciju Remote Procedure Call tehnologije razvijenu od strane Open Group kao deo Distributed Computing Environment. DCE/RPC najčešće se koristi u interakciji sa Windows mrežnim servisima. DCE/RPC na jedan impresivan način poziva procedure iz jedne aplikacije u drugu aplikaciju bez potrebe da se zna na kakvom računaru je ta aplikacija pokrenuta (izvor : <http://www.samba-tng.org/docs/tng-arch/tng-arch05.html>).

Tabela 4. Windows OS – Pronađeni servisi na IP adresi 172.23.202.69 (2011. godina)

Ip adresa	172.23.202.69
SPIDERED WEB SITES	http://172.23.202.69:5000 Sledeće URL adrese su pronađene. One su često uključene u WEB servere po difoltu ili nakon instaliranih dodataka (eng add-ons): Error (400) exchange default.asp
FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni deljeni resurs, mount-point: C:\
SERVISI	CIFS²⁰⁴, CIFS Name Service²⁰⁵ : advertised-name-1: WINXPproSP1x64 (Computer Name) advertised-name-2: WINXPproSP1x64 (File Server Service) advertised-name-3: WORKGROUP (Domain Name) advertised-name-4: WORKGROUP (Browser Service Elections) advertised-name-5: WORKGROUP (Master Browser) mac-address: 222C2909EE2D DCE RPC²⁰⁶: interface-uuid: 7B7B91F8-00FB-11D0-A9B2-00C04FB6E6FA interface-version: 1 name: Messenger Service protocol-sequence: ncacn_ip_tcp:172.23.202.69[1025] interface-uuid: 7B7B91F8-00FB-11D0-A9B2-00C04FB6E6FA interface-version: 1 name: Messenger Service protocol-sequence: ncadg_ip_udp:172.23.202.69[1026] NTP: 172.23.202.69 udp 123 UPnP-HTTPPU: 172.23.202.69 tcp 5000

Tabela 5. Windows OS sa IP adresom 172.23.202.107 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.107		OS: Microsoft Windows XP Pro Sp2 x86, WINXPproSP2x86			11
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti

²⁰⁴ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokl dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

²⁰⁵ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

²⁰⁶ DCE/RPC predstavlja implementaciju Remote Procedure Call tehnologije razvijenu od strane Open Group kao deo Distributed Computing Environment. DCE/RPC najčešće se koristi u interakciji sa Windows mrežnim servisima. DCE/RPC na jedan impresivan način poziva procedure iz jedne aplikacije u drugu aplikaciju bez potrebe da se zna na kakvom računaru je ta aplikacija pokrenuta (izvor : <http://www.samba-tng.org/docs/tng-arch/tng-arch05.html>).

1.	Microsoft Server Service / CanonicalizePathName() Remote Code Execution Vulnerability (dcerpc-msnetapi-netpathcanonicalize-dos)	Određene verzije Microsoft Windows-a su ranjive na daljinsko preopterećenje bafera (privremene memorije) koja bi mogla da kompromituje napadnuti računar. Posebno izrađen paket se može koristiti sa pozivom ka NetPathCanonicalize RPC ruti na sevisu servera, pri čemu bi napadač mogao da izvrši kôd pod sistemskim nivoom pristupa.	CVE: CVE-2006-3439 ²⁰⁷ , MS: MS06-040 ²⁰⁸ , MSKB: 921883 ²⁰⁹ , SANS-06: W4 ²¹⁰ , SANS-07: S2 ²¹¹	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowXP-KB921883-x86-ENU.EXE ²¹²
2.	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (windows-hotfix-ms08-067)	172.23.202.107:139 172.23.202.107:445 Ovo ažuriranje bezbednosti rešava privatno prijavljenu ranjivost. Ova ranjivost bi mogla da omogući izvršenje udaljenog kôda ukoliko bi napadnuti sistem primio posebno kreiran RPC zahtev. Na sistemima Microsoft Windows 2000, Windows XP i Windows Server 2003, napadač bi mogao da iskoristi ovu ranjivost bez autentičnosti da pokrene proizvoljan kôd. Moguće je iskoristiti ovu ranjivost da se kreira eksploatacija. Dosadašnja praksa fajervola i standardne fajervol difolt konfiguracije mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan organizacije.	MS: MS08-067 ²¹³ MSKB: 958644 ²¹⁴ CVE: CVE-2008-4250 ²¹⁵ SECUNIA: 32326 ²¹⁶ URL1 ²¹⁷ URL2 ²¹⁸ URL3 ²¹⁹	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB958644-x86-ENU.exe (648560 bytes) ²²⁰
3.	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (windows-hotfix-ms09-001)	172.23.202.107:139 172.23.202.107:445 Ovo ažuriranje bezbednosti rešava nekoliko privatno prijavljenih ranjivosti, a odnose se na protokol Microsoft Server Message Block-a (SMB). Ove ranjivosti bi mogle da omoguće izvršenje udaljenog kôda na napadnutim sistemima. Napadač koji bi uspešno iskoristio ove ranjivosti mogao bi da instalira programe,	MS: MS09-001 ²²¹ MSKB: 958687 ²²² CVE: CVE-2008-4114 ²²³ CVE: CVE-2008-4835 ²²⁴ CVE: CVE-2008-4834 ²²⁵ SECUNIA: 31883 ²²⁶ URL1 ²²⁷ URL2 ²²⁸ URL3 ²²⁹	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB958687-x86-ENU.exe (658288 bytes) ²³⁰

²⁰⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-3439>²⁰⁸ <http://technet.microsoft.com/en-us/security/bulletin/ms06-040>²⁰⁹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;921883>²¹⁰ <http://www.sans.org/critical-security-controls/#w4>²¹¹ <http://www.sans.org/critical-security-controls/#s2>²¹² download.microsoft.com/download/c/2/b/c2b41862-1113-4e40-a81a-d6971733e361/WindowsXP-KB921883-x86-ENU.exe²¹³ <http://technet.microsoft.com/en-us/security/bulletin/ms08-067>²¹⁴ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958644>²¹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4250>²¹⁶ <http://secunia.com/advisories/32326/>²¹⁷ blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx²¹⁸ <http://blogs.msdn.com/b/sdl/archive/2008/10/22/ms08-067.aspx>²¹⁹ <http://blogs.technet.com/b/msrc/archive/2008/10/23/ms08-067-released.aspx>²²⁰ http://download.windowsupdate.com/msdownload/update/software/secu/2008/10/windowsxpkb958644-x86-enu_5c135a8dae5721849430afe27af255f83e64f62b.exe²²¹ <http://technet.microsoft.com/en-us/security/bulletin/MS09-001>²²² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958687>²²³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4114>²²⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4835>²²⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4834>²²⁶ <http://secunia.com/advisories/31883/>²²⁷ http://www.vallejo.cc/proyectos/vista_SMB_write_DoS.htm²²⁸ <http://www.zerodayinitiative.com/advisories/ZDI-09-001/>²²⁹ <http://www.zerodayinitiative.com/advisories/ZDI-09-002/>²³⁰ http://download.windowsupdate.com/msdownload/update/software/secu/2008/12/windowsxp-kb958687-x86-enu_a9b85264e9b75e552ae10cd212937b8686a96833.exe

		pregleda, menja ili briše podatke ili pak da kreira nove naloge sa punim pravima korisnika. Dosadašnja praksa fajervola i standardne fajervol difolt konfiguracije mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan organizacije. Za sisteme koji su stalno povezani na Internet preporuka je da imaju što manji broj izloženih portova.			
4.	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-012)	172.23.202.107:139 172.23.202.107:445 Ovo ažuriranje bezbednosti rešava nekoliko privatno prijavljenih ranjivosti na Microsoft Windows-u. Opasnost od ove ranjivosti leži u tome što bi ona omogućila daljinsko izvršavanje kôda ukoliko bi napadač kreirao posebno opremljen SMB paket i poslao ga ugroženom sistemu. Dosadašnja praksa fajervola i standardne fajervol difolt konfiguracije mogu da pomognu u zaštiti mrežnih resursa od napada (koji bi pokušali da iskoriste ove ranjivosti), a koji potiču izvan okvira organizacije.	MS: MS10-012 ²³¹ MSKB - 971468 ²³² CVE: CVE-2010-0020 ²³³ CVE: CVE-2010-0021 ²³⁴ CVE: CVE-2010-0022 ²³⁵ CVE CVE-2010-0231 ²³⁶ SECUNIA 38510 ²³⁷	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB971468-x86-ENU.exe (664952 bytes) ²³⁸
5.	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-054)	172.23.202.107:139 172.23.202.107:445 Opis je isti kao kod ranjivosti MS10-012	CVE: CVE-2010-2550 ²³⁹ CVE: CVE-2010-2551 ²⁴⁰ CVE: CVE-2010-2552 ²⁴¹ MS: MS10-054 ²⁴² MSKB 982214 ²⁴³	Kritičan	Uraditi download a zatim instalirati Microsoft patch windowsxp-kb982214-x86-enu.exe (661368 bytes) ²⁴⁴
6.	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms11-020)	172.23.202.107:139 172.23.202.107:445 Opis je isti kao kod ranjivosti MS10-012	CVE: CVE-2011-0661 ²⁴⁵ MS: MS11-020 ²⁴⁶ MSKB: 2508429 ²⁴⁷	Kritičan	Uraditi download a zatim instalirati Microsoft patch windowsxp-kb2508429-x86-enu.exe (664960 bytes) ²⁴⁸
7.	MS06-035: Vulnerability in Server Service Could Allow	Ovo ažuriranje rešava nekoliko otkrivenih i privatno prijavljenih ranjivosti. Preporučuje se da korisnici	CVE: CVE-2006-1314 ²⁴⁹ CVE: VE-2006-1315 ²⁵⁰ MS: MS06-035 ²⁵¹	Kritičan	Uraditi download a zatim instalirati Microsoft patch

²³¹<http://technet.microsoft.com/en-us/security/bulletin/MS10-012>²³²<http://support.microsoft.com/default.aspx?scid=kb;EN-US;971468>²³³<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0020>²³⁴<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0021>²³⁵<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0022>²³⁶<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0231>²³⁷<http://secunia.com/advisories/38510/>²³⁸http://download.windowsupdate.com/msdownload/update/software/secu/2010/01/windowsxp-kb971468-x86-enu_68d7899c8b8462219daf40f02c6fb9f362b1ee6b.exe²³⁹<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2550>²⁴⁰<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2551>²⁴¹<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2552>²⁴²<http://technet.microsoft.com/en-us/security/bulletin/MS10-054>²⁴³<http://support.microsoft.com/default.aspx?scid=kb;EN-US;982214>²⁴⁴http://download.windowsupdate.com/msdownload/update/software/secu/2010/07/windowsxp-kb982214-x86-enu_a24853f682dad3157da4e4a39372951a8ec1e407.exe²⁴⁵<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661>²⁴⁶<http://technet.microsoft.com/en-us/security/bulletin/ms11-020>²⁴⁷<http://support.microsoft.com/default.aspx?scid=kb;EN-US;2508429>²⁴⁸http://download.windowsupdate.com/msdownload/update/software/secu/2011/03/windowsxp-kb2508429-x86-enu_e0b40d81f2ecc1bad43439a6bd0a9e2a0ab7dd56.exe²⁴⁹<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1314>²⁵⁰<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1315>

	Remote Code Execution (917159) (windows-hotfixms06-035)	odmah primene update.	MSKB: 917159 ²⁵² SANS-06: W4 ²⁵³ SANS-07: S2 ²⁵⁴ SECUNIA: 21007 ²⁵⁵ XF: win-mailslot-bo(26818) ²⁵⁶ XF win-smb-information-disclosure(26820) ²⁵⁷		WindowsXP-KB917159-x86-ENU.exe (725304 bytes) ²⁵⁸
8.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.107:139 172.23.202.107:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje omogućava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurirano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB: 887429 ²⁵⁹ URL1 ²⁶⁰	Ozbiljan	Metoda za konfigurisanje SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429 ²⁶¹ . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing = auto</i> ili da se zahteva SMB potpisivanje: <i>server signing = mandatory</i>
9.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.107:139 172.23.202.107:445 Sistem omogućava ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti
10.	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server. Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko poziva udaljenih procedura (RPC). Ovi servisi su i u prošlosti bili skloni ranjivostima. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinjenije napade.	BID: 494 ²⁶² CVE: CVE-1999-0519 ²⁶³ MSKB: 143474 ²⁶⁴ URL1 ²⁶⁵	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost.
11.	ICMP timestamp	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat.	CVE: CVE-1999-0524 ²⁶⁶ XF: icmp-	Umeren	Onemogućavanje ICMP timestamps odgovora vrši

²⁵¹ <http://technet.microsoft.com/en-us/security/bulletin/ms06-035>²⁵² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;917159>²⁵³ <http://www.sans.org/critical-security-controls/#w4>²⁵⁴ <http://www.sans.org/critical-security-controls/#s2>²⁵⁵ <http://secunia.com/advisories/21007/>²⁵⁶ <http://xforce.iss.net/xforce/xfdb/26818>²⁵⁷ <http://xforce.iss.net/xforce/xfdb/26820>²⁵⁸ http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb917159-x86-enu_5ed838e18ceae61a8d94f8c4be2462a8e19212d7.exe²⁵⁹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429>²⁶⁰ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>²⁶¹ <http://support.microsoft.com/kb/887429>²⁶² <http://www.securityfocus.com/bid/494>²⁶³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>²⁶⁴ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>²⁶⁵ http://www.hsc.fr/ressources/presentations/null_sessions/²⁶⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>

response (generic-icmp-timestamp)	Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatišu slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	netmask(306) ²⁶⁷ XF: icmp-timestamp(322) ²⁶⁸	se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost

Tabela 6. Windows OS – Pronađeni servisi na IP adresi 172.23.202.107 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni deljeni resurs, mount-point: C:\
SERVISI	CIFS ²⁶⁹ , CIFS Name Service²⁷⁰ : advertised-name-1: WINXPproSP2x86 (Computer Name) advertised-name-2: WINXPproSP2x86 (File Server Service) advertised-name-3: WORKGROUP (Domain Name) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 000C29AB7A4E NTP: 172.23.202.107 udp 123

Tabela 7. Windows OS sa IP adresama 172.23.202.110, 172.23.202.76 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.110		OS: Microsoft Windows 2000 Advanced server Sp4, WIN2000ADVsp4			18
IP adresa: 172.23.202.76		OS: Windows 2000 server Sp4, Win2000srvsp4			18
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Microsoft Server Service / CanonicalizePathName() Remote Code Execution Vulnerability (dcerpc-msnetapi-netpathcanonicalize-dos)	Određene verzije Microsoft Windows-a su ranjive na daljinsko preopterećenje bafera (privremene memorije) koje bi moglo da kompromituje određeni računar. Posebno izrađen paket se može koristiti sa pozivom ka NetPathCanonicalize RPC ruti na servisu servera, pri čemu bi napadač mogao da izvrši kôd pod sistemskim	CVE CVE-2006-3439 ²⁷¹ MS MS06-040 ²⁷² OVAL OVAL492 ²⁷³ SECUNIA 21388 ²⁷⁴ XF ms-server-service-bo(28002) ²⁷⁵	Kritičan	Uraditi download a zatim instalirati Microsoft patch WinDOWS2000-KB921883-x86-ENU.EXE ²⁷⁶

²⁶⁷ <http://xforce.iss.net/xforce/xfdb/306>²⁶⁸ <http://xforce.iss.net/xforce/xfdb/322>²⁶⁹ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datateka preko Interneta. Proširuje SMB ili Server Message Block protokl dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).²⁷⁰ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.²⁷¹ <http://nvd.nist.gov/?vulnId=CVE-2006-3439>²⁷² <http://technet.microsoft.com/en-us/security/bulletin/ms06-040>²⁷³ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval:def:492>²⁷⁴ <http://secunia.com/advisories/21388/>²⁷⁵ <http://xforce.iss.net/xforce/xfdb/28002>²⁷⁶ download.microsoft.com/download/9/0/b/90b8dbba-09c1-4b27-b0c4-0cc13706823a/Windows2000-KB921883-x86-ENU.EXE

		nivoom pristupa.			
2.	MS03-039: Buffer Overrun In RPCSS Service Could Allow Code Execution (824146) (windows-hotfix-ms03-039)	Napadač koji bi uspešno iskoristio ove ranjivosti mogao bi da pokrene kôd sa privilegijama lokalnog sistema na napadnutom sistemu, ili bi mogao da prouzrokuje isključenje RPCSS servisa. Napadač bi tada bio u mogućnosti da preduzme bilo kakvu akciju na sistemu, uključujući instaliranje programa, pregledanje, menjanje ili brisanje podataka ili otvaranje novih naloga sa svih privilegijama. Da bi iskoristio ove ranjivosti, napadač bi mogao da kreira program koji bi poslao malicioznu RPC poruku ranjivom sistemu, ciljajući na RPCSS servis.	BID: 8458 ²⁷⁷ , CVE: CVE-2003-0528 ²⁷⁸ , CVE: CVE-2003-0605 ²⁷⁹ , CVE: CVE-2003-0715 ²⁸⁰ , MSKB: 824146 ²⁸¹ , MS:MS03-039 ²⁸²	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows2000-KB824146-x86-ENU.exe (938856 bytes) ²⁸³ Uraditi download a zatim instalirati Microsoft patch DirectX9-KB819696-x86-ENU.exe (970312 bytes) ²⁸⁴
3.	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (windows-hotfix-ms08-067)	172.23.202.110:139 172.23.202.110:445 172.23.202.76:139 172.23.202.76:445 Ova bezbednosna ispravka rešava ranjivost koja je prijavljena od strane privatnog lica. Ranjivost bi mogla da omogući daljinsko izvršavanje koda ukoliko je napadnuti sistem primio posebno opremljeni RPC zahtev. Na sistemima Microsoft Windows 2000, Windows XP, i Windows Server 2003, napadač bi mogao da iskoristi ovu ranjivost bez overavanja autentičnosti i da pokrene proizvoljan kôd. Moguće je da ova ranjivost može biti upotrebljena za intenziviranje skrivenog korišćenja. Najbolje prakse zaštitnog zida i standardne konfiguracije zaštitnog zida po difoltu mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan okvira preduzeća.	MS: MS08-067 ²⁸⁵ MSKB: 958644 ²⁸⁶ CVE: CVE-2008-4250 ²⁸⁷ SECUNIA: 32326 ²⁸⁸ URL1 ²⁸⁹ URL2 ²⁹⁰ URL3 ²⁹¹	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows2000-KB958644-x86-ENU.EXE (618024 bytes) ²⁹²
4.	MS09-001: Vulnerabilities in SMB Could Allow Remote	172.23.202.110:139 172.23.202.110:445 172.23.202.76:139 172.23.202.76:445	MS: MS09-001 ²⁹³ MSKB: 958687 ²⁹⁴ CVE: CVE-2008-4114 ²⁹⁵ CVE: CVE-2008-4835 ²⁹⁶	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows2000-KB958687-

²⁷⁷ <http://www.securityfocus.com/bid/8458>²⁷⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0528>²⁷⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0605>²⁸⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0715>²⁸¹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;824146>²⁸² <http://technet.microsoft.com/en-us/security/bulletin/ms03-039>²⁸³ http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windows2000-kb824146-x86-enu_dcf74565af2d26e87ef7cf974f03c30.exe²⁸⁴ http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/directx9-kb819696-x86-enu_977f8cc86c1e151a0168d1296210913.exe²⁸⁵ <http://technet.microsoft.com/en-us/security/bulletin/ms08-067>²⁸⁶ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958644>²⁸⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4250>²⁸⁸ <http://secunia.com/advisories/32326/>²⁸⁹ <http://blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx>²⁹⁰ <http://blogs.msdn.com/b/sdl/archive/2008/10/22/ms08-067.aspx>²⁹¹ <http://blogs.technet.com/b/msrc/archive/2008/10/23/ms08-067-released.aspx>²⁹² http://download.windowsupdate.com/msdownload/update/software/secu/2008/10/windows2000-kb958644-x86-enu_32416827ab7de148e5e7998e6e1f4c3b16fa4719.exe²⁹³ <http://technet.microsoft.com/en-us/security/bulletin/MS09-001>²⁹⁴ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958687>²⁹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4114>²⁹⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4835>

	Code Execution (windows-hotfix-ms09-001)	Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti koje su privatno prijavljene, a odnose se na protokol Microsoft Server Message Block-a (SMB). Ranjivosti mogu da omoguće daljinsko izvršenje koda na ugroženim sistemima. Napadač koji je uspešno iskoristio ove ranjivosti može da instalira programe, pregleda, menja ili briše podatke ili otvara nove naloge sa potpunim korisničkim pravima. Najbolje prakse zaštitnog zida i standardne konfiguracije zaštitnog zida po defaultu mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan okvira preduzeća. Za sisteme koji su stalno povezani na Internet preporuka je da imaju što manji broj izloženih portova.	CVE: CVE-2008-4834 ²⁹⁷ SECUNIA: 31883 ²⁹⁸ URL1 ²⁹⁹ URL2 ³⁰⁰ URL3 ³⁰¹		x86-ENU.EXE (617512 bytes) ³⁰²
5.	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-012)	172.23.202.110:139 172.23.202.110:445 172.23.202.76:139 172.23.202.76:445 Ovo ažuriranje bezbednosti rešava nekoliko privatno prijavljenih ranjivosti u Microsoft Windows-u. Opasnost od ove ranjivosti leži u tome što bi ona omogućila daljinsko izvršavanje koda ukoliko bi napadač kreirao posebno opremljen SMB paket i poslao ga ugroženom sistemu. Dosadašnja praksa fajervola i standardne fajervol default konfiguracije mogu da pomognu u zaštiti mrežnih resursa od napada (koji bi pokušali da iskoriste ove ranjivosti), a koji potiču izvan okvira organizacije.	MS: MS10-012 ³⁰³ MSKB - 971468 ³⁰⁴ CVE: CVE-2010-0020 ³⁰⁵ CVE: CVE-2010-0021 ³⁰⁶ CVE: CVE-2010-0022 ³⁰⁷ CVE CVE-2010-0231 ³⁰⁸ SECUNIA 38510 ³⁰⁹	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows2000-KB971468-x86-ENU.EXE (621304 bytes) ³¹⁰
6.	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-054)	172.23.202.110:139 172.23.202.110:445 172.23.202.76:139 172.23.202.76:445 Opis je isti kao kod ranjivosti MS10-012	CVE: CVE-2010-2550 ³¹¹ CVE: CVE-2010-2551 ³¹² CVE: CVE-2010-2552 ³¹³ MS: MS10-054 ³¹⁴ MSKB 982214 ³¹⁵	Kritičan	Blokirati portove 139 i 445 na spoljnom fajervolu. Treba imati u vidu da će ova ranjivost takođe uticati na sisteme Windows 2000, a usled zastarevanja Windows 2000; ne postoji

²⁹⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4834>²⁹⁸ <http://secunia.com/advisories/31883/>²⁹⁹ http://www.vallejo.cc/proyectos/vista_SMB_write_DoS.htm³⁰⁰ <http://www.zerodayinitiative.com/advisories/ZDI-09-001/>³⁰¹ <http://www.zerodayinitiative.com/advisories/ZDI-09-002/>³⁰² http://download.windowsupdate.com/msdownload/update/software/secu/2008/12/windows2000-kb958687-x86-enu_f0ce8f2df0b10e58fb8c5ee278153eae03ad4ac6.exe³⁰³ <http://technet.microsoft.com/en-us/security/bulletin/MS10-012>³⁰⁴ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;971468>³⁰⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0020>³⁰⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0021>³⁰⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0022>³⁰⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0231>³⁰⁹ <http://secunia.com/advisories/38510/>³¹⁰ http://download.windowsupdate.com/msdownload/update/software/secu/2010/01/windows2000-kb971468-x86-enu_d951943f14a5e6e52fbbbed11ae55882c685795c.exe³¹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2550>³¹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2551>³¹³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2552>³¹⁴ <http://technet.microsoft.com/en-us/security/bulletin/MS10-054>³¹⁵ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;982214>

					odgovarajuća zakrpa koja bi omogućila ublažavanje ove ranjivosti.
7.	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms11-020)	172.23.202.110:139 172.23.202.110:445 172.23.202.76:139 172.23.202.76:445 Opis je isti kao kod ranjivosti MS10-012	CVE: CVE-2011-0661 ³¹⁶ MS: MS11-020 ³¹⁷ MSKB: 2508429 ³¹⁸	Kritičan	Blokirati portove 139 i 445 na spoljnom fajervolu. Treba imati u vidu da će ova ranjivost takode uticati na sisteme Windows 2000, a usled zastarevanja Windows 2000; ne postoji odgovarajuća zakrpa koja bi omogućila ublažavanje ove ranjivosti.
8.	Anonymous users can obtain the Windows password policy (cifs-nt-0002)	Korišćenjem CIFS NULL sesije, anonimni korisnik može da dobije uvid u polisu šifri. Polisa šifri sadrži osetljive informacije o najmanjoj mogućoj dužini lozinke, zaključavanje šifre, vremensko trajanje zaključanosti šifre itd.	SANS-01 W5 ³¹⁹ CVE CVE-2000-1200 ³²⁰ MSKB 143474 ³²¹ XF nt-lsa-domain-sid(4015) ³²² MSKB 823659 ³²³ MSKB 246261 ³²⁴ MSKB 129457 ³²⁵ SANS-02 W5 ³²⁶ BID 959 ³²⁷ SANS-04 W3 ³²⁸ SANS-03 W5 ³²⁹ BID 87 ³³⁰	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost.
9.	MS03-026: Buffer Overrun In RPC Interface Could Allow Code Execution (823980) (windows-hotfix-ms03-026)	Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti u Windows Distributed Component Object Model (DCOM) Remote Procedure Call (RPC). Napadač koji uspešno iskoristi ovu ranjivost, bio bi u mogućnosti da pokrene kôd sa privilegijama lokalnog sistema na napadnutom sistemu. Napadač bi bio u mogućnosti da preduzme bilo kakvu akciju na sistemu, uključujući instaliranje programa, pregledanje, menjanje ili brisanje podataka, ili pak kreiranje novih naloga sa svim privilegijama. Da bi iskoristio ovu ranjivost, napadač bi morao da pošalje posebno kreiran zahtev udaljenom kompjuteru na specifične RPC portove.	CVE: CVE-2003-0352 ³³¹ MS: MS03-026 ³³² BID: 8205 ³³³ MSKB: 823980 ³³⁴	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows2000-KB823980-x86-ENU.exe ³³⁵

³¹⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661>³¹⁷ <http://technet.microsoft.com/en-us/security/bulletin/ms11-020>³¹⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;2508429>³¹⁹ <http://www.sans.org/critical-security-controls/#w5>³²⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2000-1200>³²¹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>³²² <http://xforce.iss.net/xforce/xfdb/4015>³²³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;823659>³²⁴ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;246261>³²⁵ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;129457>³²⁶ <http://www.sans.org/critical-security-controls/#w5>³²⁷ <http://www.securityfocus.com/bid/959>³²⁸ <http://www.sans.org/critical-security-controls/#w3>³²⁹ <http://www.sans.org/critical-security-controls/#w5>³³⁰ <http://www.securityfocus.com/bid/87>³³¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0352>³³² <http://technet.microsoft.com/en-us/security/bulletin/ms03-026>³³³ <http://www.securityfocus.com/bid/8205>³³⁴ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;823980>³³⁵ download.microsoft.com/download/0/1/f/01fdd40f-efc5-433d-8ad2-b4b9d42049d5/windows2000-kb823980-x86-enu.exe

10.	MS04-011: Security Update for Microsoft Windows (835732) (windows-hotfix-ms04-011)	172.23.202.110:139 172.23.202.110:445 172.23.202.76:139 172.23.202.76:445 Ovo ažuriranje rešava nekoliko novootkrivenih ranjivosti. Napadač koji uspešno iskoristi ovu ranjivost bi mogao da preuzme potpunu kontrolu nad napadnutim sistemom, uključujući instaliranje programa, pregledanje, menjanje ili brisanje podataka ili čak otvaranje novih naloga sa svim privilegijama.	BID 10108³³⁶ BID 10113³³⁷ BID 10114³³⁸ BID 10115³³⁹ BID 10117³⁴⁰ BID 10118³⁴¹ BID 10119³⁴² BID 10120³⁴³ BID 10122³⁴⁴ BID 10124³⁴⁵ BID 10125³⁴⁶ BID 10126³⁴⁷ CERT-VN 122076³⁴⁸ CERT-VN 150236³⁴⁹ CERT-VN 206468³⁵⁰ CERT-VN 255924³⁵¹ CERT-VN 260588³⁵² CERT-VN 353956³⁵³ CERT-VN 471260³⁵⁴ CERT-VN 526084³⁵⁵ CERT-VN 547028³⁵⁶ CERT-VN 586540³⁵⁷ CERT-VN 638548³⁵⁸ CERT-VN 639428³⁵⁹ CVE CVE-2003-0663³⁶⁰ CVE CVE-2003-0719³⁶¹ CVE CVE-2003-0806³⁶² CVE CVE-2003-0906³⁶³ CVE CVE-2003-0907³⁶⁴ CVE CVE-2003-0908³⁶⁵ CVE CVE-2003-0909³⁶⁶ CVE CVE-2003-0910³⁶⁷ CVE CVE-2004-0117³⁶⁸ CVE CVE-2004-0118³⁶⁹ CVE CVE-2004-0119³⁷⁰	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows2000-KB835732-x86-ENU ⁴³¹

³³⁶ <http://www.securityfocus.com/bid/10108>³³⁷ <http://www.securityfocus.com/bid/10113>³³⁸ <http://www.securityfocus.com/bid/10114>³³⁹ <http://www.securityfocus.com/bid/10115>³⁴⁰ <http://www.securityfocus.com/bid/10117>³⁴¹ <http://www.securityfocus.com/bid/10118>³⁴² <http://www.securityfocus.com/bid/10119>³⁴³ <http://www.securityfocus.com/bid/10120>³⁴⁴ <http://www.securityfocus.com/bid/10122>³⁴⁵ <http://www.securityfocus.com/bid/10124>³⁴⁶ <http://www.securityfocus.com/bid/10125>³⁴⁷ <http://www.securityfocus.com/bid/10126>³⁴⁸ <http://www.kb.cert.org/vuls/id/122076>³⁴⁹ <http://www.kb.cert.org/vuls/id/150236>³⁵⁰ <http://www.kb.cert.org/vuls/id/206468>³⁵¹ <http://www.kb.cert.org/vuls/id/255924>³⁵² <http://www.kb.cert.org/vuls/id/260588>³⁵³ <http://www.kb.cert.org/vuls/id/353956>³⁵⁴ <http://www.kb.cert.org/vuls/id/471260>³⁵⁵ <http://www.kb.cert.org/vuls/id/526084>³⁵⁶ <http://www.kb.cert.org/vuls/id/547028>³⁵⁷ <http://www.kb.cert.org/vuls/id/586540>³⁵⁸ <http://www.kb.cert.org/vuls/id/638548>³⁵⁹ <http://www.kb.cert.org/vuls/id/639428>³⁶⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0663>³⁶¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0719>³⁶² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0806>³⁶³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0906>³⁶⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0907>³⁶⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0908>³⁶⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0909>³⁶⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0910>³⁶⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0117>³⁶⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0118>³⁷⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0119>

			CVE CVE-2004-0120³⁷¹ CVE CVE-2004-0123³⁷² OVAL OVAL1004³⁷³ OVAL OVAL1007³⁷⁴ OVAL OVAL1016³⁷⁵ OVAL OVAL1046³⁷⁶ OVAL OVAL1054³⁷⁷ OVAL OVAL1064³⁷⁸ OVAL OVAL1076³⁷⁹ OVAL OVAL1093³⁸⁰ OVAL OVAL1512³⁸¹ OVAL OVAL1718³⁸² OVAL OVAL1808³⁸³ OVAL OVAL1962³⁸⁴ OVAL OVAL1997³⁸⁵ OVAL OVAL883³⁸⁶ OVAL OVAL885³⁸⁷ OVAL OVAL886³⁸⁸ OVAL OVAL889³⁸⁹ OVAL OVAL890³⁹⁰ OVAL OVAL892³⁹¹ OVAL OVAL895³⁹² OVAL OVAL896³⁹³ OVAL OVAL897³⁹⁴ OVAL OVAL898³⁹⁵ OVAL OVAL903³⁹⁶ OVAL OVAL904³⁹⁷ OVAL OVAL907³⁹⁸ OVAL OVAL911³⁹⁹ OVAL OVAL919⁴⁰⁰ OVAL OVAL924⁴⁰¹ OVAL OVAL946⁴⁰² OVAL OVAL951⁴⁰³ OVAL OVAL959⁴⁰⁴ OVAL OVAL964⁴⁰⁵		

⁴³¹ download.microsoft.com/download/F/A/A/FAA796AA-399D-437A-9284-C3536E9F2E6E/Windows2000-KB835732-x86-ENU.EXE
³⁷¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0120>
³⁷² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0123>
³⁷³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1004>
³⁷⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1007>
³⁷⁵ oval.mitre.org/oval/definitions/data/OVAL1016.html
³⁷⁶ oval.mitre.org/oval/definitions/data/OVAL1046.html
³⁷⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1054>
³⁷⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1064>
³⁷⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1076>
³⁸⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1093>
³⁸¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1512>
³⁸² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1718>
³⁸³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1808>
³⁸⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1962>
³⁸⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1997>
³⁸⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:883>
³⁸⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:885>
³⁸⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:886>
³⁸⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:889>
³⁹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:890>
³⁹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:892>
³⁹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:895>
³⁹³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:896>
³⁹⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:897>
³⁹⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:898>
³⁹⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:903>
³⁹⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:904>
³⁹⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:907>
³⁹⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:911>
⁴⁰⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:919>
⁴⁰¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:924>
⁴⁰² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:946>
⁴⁰³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:951>
⁴⁰⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:959>

			URL1⁴⁰⁶ URL2⁴⁰⁷ URL3⁴⁰⁸ URL4⁴⁰⁹ URL5⁴¹⁰ URL6⁴¹¹ URL7⁴¹² URL8⁴¹³ XF ssl-message-dos(15712)⁴¹⁴ XF win-asn1-double-free(15713)⁴¹⁵ XF win-h323-bo(15710)⁴¹⁶ XF win-hcpurl-code-execution(15704)⁴¹⁷ XF win-ldt-gain-privileges(15707)⁴¹⁸ XF win-lsass-bo(15699)⁴¹⁹ XF win-spp-bo(15715)⁴²⁰ XF win-vdm-gain-privileges(15714)⁴²¹ XF win-winlogon-bo(15702)⁴²² XF win2k-lsass-ldap-dos(15700)⁴²³ XF win2k-utilitymgr-gain-privileges(15632) MS: MS04-011⁴²⁴ , CVE: CVE-2003-0533⁴²⁵ MSKB: 835732⁴²⁶ OVAL: OVAL1000⁴²⁷ CERT-VN: 753212⁴²⁸ CERT-VN: 783748⁴²⁹ XF: winxp-task-gain-privileges(15678)⁴³⁰		
11.	MS05-051: Vulnerabilities in	Ovo ažuriranje rešava nekoliko novootkrivenih ranjivosti. Napadač	BID 15056⁴³² BID 15057⁴³³	Kritičan	Uraditi download a zatim instalirati Microsoft patch

⁴⁰⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:964>

⁴⁰⁶ <http://archives.neohapsis.com/archives/vulnwatch/2004-q1/0081.html>

⁴⁰⁷ <http://archives.neohapsis.com/archives/vulnwatch/2004-q1/0082.html>

⁴⁰⁸ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020065.html>

⁴⁰⁹ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020068.html>

⁴¹⁰ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020069.html>

⁴¹¹ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020070.html>

⁴¹² <http://www.securiteam.com/windowsntfocus/5LP0C2ACKU.html>

⁴¹³ <http://www.securityfocus.com/archive/1/361836>

⁴¹⁴ <http://xforce.iss.net/xforce/xfdb/15712>

⁴¹⁵ <http://xforce.iss.net/xforce/xfdb/15713>

⁴¹⁶ <http://xforce.iss.net/xforce/xfdb/15710>

⁴¹⁷ <http://xforce.iss.net/xforce/xfdb/15704>

⁴¹⁸ <http://xforce.iss.net/xforce/xfdb/15707>

⁴¹⁹ <http://xforce.iss.net/xforce/xfdb/15699>

⁴²⁰ <http://xforce.iss.net/xforce/xfdb/15715>

⁴²¹ <http://xforce.iss.net/xforce/xfdb/15714>

⁴²² <http://xforce.iss.net/xforce/xfdb/15702>

⁴²³ <http://xforce.iss.net/xforce/xfdb/15700>

⁴²⁴ <http://technet.microsoft.com/en-us/security/bulletin/ms04-011>

⁴²⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0533>

⁴²⁶ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;835732>

⁴²⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1000>

⁴²⁸ <http://www.kb.cert.org/vuls/id/753212>

⁴²⁹ <http://www.kb.cert.org/vuls/id/783748>

⁴³⁰ <http://xforce.iss.net/xforce/xfdb/15678>

⁴³² <http://www.securityfocus.com/bid/15056>

⁴³³ <http://www.securityfocus.com/bid/15057>

MSDTC and COM+ Could Allow Remote Code Execution (902400) (windowshotfix-ms05-051)	koji uspešno iskoristi ovu ranjivost bi mogao da preuzme potpunu kontrolu nad napadnutim sistemom, uključujući instaliranje programa, pregledanje, menjanje ili brisanje podataka ili čak otvaranje novih naloga sa svim privilegijama.	BID 15058 ⁴³⁴ BID 15059 ⁴³⁵ CERT-VN 180868 ⁴³⁶ CERT-VN 950516 ⁴³⁷ CVE CVE-2005-1978 ⁴³⁸ CVE CVE-2005-1979 ⁴³⁹ CVE CVE-2005-1980 ⁴⁴⁰ CVE CVE-2005-2119 ⁴⁴¹ MS MS05-051 ⁴⁴² MSKB 902400 ⁴⁴³ OVAL OVAL1071 ⁴⁴⁴ OVAL OVAL1134 ⁴⁴⁵ OVAL OVAL1136 ⁴⁴⁶ OVAL OVAL1182 ⁴⁴⁷ OVAL OVAL1203 ⁴⁴⁸ OVAL OVAL1253 ⁴⁴⁹ OVAL OVAL1261 ⁴⁵⁰ OVAL OVAL1269 ⁴⁵¹ OVAL OVAL1283 ⁴⁵² OVAL OVAL1325 ⁴⁵³ OVAL OVAL1338 ⁴⁵⁴ OVAL OVAL1413 ⁴⁵⁵ OVAL OVAL1452 ⁴⁵⁶ OVAL OVAL1466 ⁴⁵⁷ OVAL OVAL1499 ⁴⁵⁸ OVAL OVAL1513 ⁴⁵⁹ OVAL OVAL1550 ⁴⁶⁰ OVAL OVAL551 ⁴⁶¹ OVAL OVAL576 ⁴⁶² OVAL OVAL686 ⁴⁶³ OVAL OVAL816 ⁴⁶⁴ SECTRACK 1015037 ⁴⁶⁵ SECUNIA 17161 ⁴⁶⁶ SECUNIA 17172 ⁴⁶⁷ SECUNIA 17223 ⁴⁶⁸	Windows2000-KB902400-x86-ENU.EXE (5417976 bytes) ⁴⁷¹

⁴³⁴ <http://www.securityfocus.com/bid/15058>⁴³⁵ <http://www.securityfocus.com/bid/15059>⁴³⁶ <http://www.kb.cert.org/vuls/id/180868>⁴³⁷ <http://www.kb.cert.org/vuls/id/950516>⁴³⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-1978>⁴³⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-1979>⁴⁴⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-1980>⁴⁴¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2119>⁴⁴² <http://technet.microsoft.com/en-us/security/bulletin/ms05-051>⁴⁴³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;902400>⁴⁴⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1071>⁴⁴⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1134>⁴⁴⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1136>⁴⁴⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1182>⁴⁴⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1203>⁴⁴⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1253>⁴⁵⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1261>⁴⁵¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1269>⁴⁵² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1283>⁴⁵³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1325>⁴⁵⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1338>⁴⁵⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1413>⁴⁵⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1452>⁴⁵⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1466>⁴⁵⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1499>⁴⁵⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1513>⁴⁶⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1550>⁴⁶¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:551>⁴⁶² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:576>⁴⁶³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:686>⁴⁶⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:816>⁴⁶⁵ <http://securitytracker.com/id?1015037>⁴⁶⁶ <http://secunia.com/advisories/17161/>⁴⁶⁷ <http://secunia.com/advisories/17172/>⁴⁶⁸ <http://secunia.com/advisories/17223/>

			SECUNIA 17509 ⁴⁶⁹ URL1 ⁴⁷⁰		
12.	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (windows-hotfixms06-035)	Ovo ažuriranje rešava nekoliko otkrivenih i privatno prijavljenih ranjivosti. Preporučuje se da korisnici odmah primene update.	CVE: CVE-2006-1314 ⁴⁷² CVE: VE-2006-1315 ⁴⁷³ MS: MS06-035 ⁴⁷⁴ MSKB: 917159 ⁴⁷⁵ SANS-06: W4 ⁴⁷⁶ SANS-07: S2 ⁴⁷⁷ SECUNIA: 21007 ⁴⁷⁸ XF: win-mailslot-bo(26818) ⁴⁷⁹ XF win-smb-information-disclosure(26820) ⁴⁸⁰	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows2000-KB917159-x86-ENU.EXE (614888 bytes) ⁴⁸¹
13.	CIFS Account Password Never Expires (cifs-acct-password-never-expires)	CIFS nalog ne zahteva vremensko ograničenje šifre. Ovo je rizik za bezbednost. Ako šifra nije vremenski ograničena, to omogućava zlonamernom napadaču da izvrši napad sa ciljem otkrivanja korisničke šifre. Ukoliko rok trajanja šifre nikada ne ističe, napad se može sprovoditi tokom dužeg perioda, što povećava mogućnost da šifra bude otkrivena.		Ozbiljan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 pod primerom Opšte ranjivosti
14.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.110:139 172.23.202.110:445 172.23.202.76:139 172.23.202.76:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje omogućava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB: 887429 ⁴⁸² URL1 ⁴⁸³	Ozbiljan	Metoda za konfigurisanje SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429. Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing</i> = <i>auto</i> ili da se zahteva SMB potpisivanje: <i>server signing</i> = <i>mandatory</i> .
15.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.110:139 172.23.202.110:445 172.23.202.76:139 172.23.202.76:445 Sistem omogućava ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti
16.	TCP Sequence Number	172.23.202.110:135: 172.23.202.76:135	BID: 10183 ⁴⁸⁴ CERT-VN: 415294 ⁴⁸⁵	Ozbiljan	Uraditi download a zatim

⁴⁷¹ www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windows2000-kb902400-x86-enu_f6eabdb255f52661f789b6fb94bbc8dea6822213.exe

⁴⁶⁹ <http://secunia.com/advisories/17509/>

⁴⁷⁰ <https://downloads.avaya.com/elmodocs2/security/ASA-2005-214.pdf>

⁴⁷² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1314>

⁴⁷³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1315>

⁴⁷⁴ <http://technet.microsoft.com/en-us/security/bulletin/ms06-035>

⁴⁷⁵ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;917159>

⁴⁷⁶ <http://www.sans.org/critical-security-controls/#w4>

⁴⁷⁷ <http://www.sans.org/critical-security-controls/#s2>

⁴⁷⁸ <http://secunia.com/advisories/21007/>

⁴⁷⁹ <http://xforce.iss.net/xforce/xfdb/26818>

⁴⁸⁰ <http://xforce.iss.net/xforce/xfdb/26820>

⁴⁸¹ www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windows2000-kb917159-x86-enu_e685b01f66b72125ed2c97afd2813ce309b9a7f5.exe

⁴⁸² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429>

⁴⁸³ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>

⁴⁸⁴ <http://www.securityfocus.com/bid/10183>

	Approximation Vulnerability (tcp-seq-num-approximation)	Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hедера i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	CVE CVE-2004-0230 ⁴⁸⁶ MS: MS05-019 ⁴⁸⁷ MS: MS06-064 ⁴⁸⁸ NETBSD: NetBSD-SA2004-006 ⁴⁸⁹ OVAL: OVAL2689 ⁴⁹⁰ OVAL: OVAL270 ⁴⁹¹ OVAL OVAL3508 ⁴⁹² OVAL OVAL4791 ⁴⁹³ OVAL OVAL5711 ⁴⁹⁴ SECUNIA: 11440 ⁴⁹⁵ SECUNIA: 22341 ⁴⁹⁶ SGI 20040403-01-A ⁴⁹⁷		instalirati Microsoft patch Windows2000-KB893066-v2-x86-ENU.EXE (756728 bytes) ⁴⁹⁸
17.	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server. Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko poziva udaljenih procedura (RPC). Ovi servisi su i u prošlosti bili skloni ranjivostima.. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinjenije napade.	BID: 494 ⁴⁹⁹ CVE: CVE-1999-0519 ⁵⁰⁰ MSKB: 143474 ⁵⁰¹ URL1 ⁵⁰²	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost
18.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-ov zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatišu slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	CVE: CVE-1999-0524 ⁵⁰³ XF: icmp-netmask(306) ⁵⁰⁴ XF: icmp-timestamp(322) ⁵⁰⁵	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost

⁴⁸⁵ <http://www.kb.cert.org/vuls/id/415294>⁴⁸⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁴⁸⁷ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁴⁸⁸ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁴⁸⁹ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁴⁹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>⁴⁹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>⁴⁹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>⁴⁹³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>⁴⁹⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>⁴⁹⁵ <http://secunia.com/advisories/11440/>⁴⁹⁶ <http://secunia.com/advisories/22341/>⁴⁹⁷ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>⁴⁹⁸ www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windows2000-kb893066-v2-x86-enu_a5b95ec14e70e531e784ea83e633d24a0ea83795.exe⁴⁹⁹ <http://www.securityfocus.com/bid/494>⁵⁰⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>⁵⁰¹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>⁵⁰² http://www.hsc.fr/ressources/presentations/null_sessions/⁵⁰³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁵⁰⁴ <http://xforce.iss.net/xforce/xfdb/306>⁵⁰⁵ <http://xforce.iss.net/xforce/xfdb/322>

Tabela 8. Windows OS – Pronađeni servisi na IP adresi 172.23.202.110 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni deljeni resurs, mount-point: C:\
SERVISI	CIFS ⁵⁰⁶ , CIFS Name Service ⁵⁰⁷ : advertised-name-1: WIN2000ADVsp4 (Computer Name) advertised-name-2: WIN2000ADVsp4 (File Server Service) advertised-name-3: WORKGROUP (Domain Name) advertised-name-4: WORKGROUP (Browser Service Elections) advertised-name-5: WIN2000ADVsp4 (Logged-on User) mac-address: 000C299B0E64 DCE RPC interface-uuid: 906B0CE0-C70B-1067-B317-00DD010662DA interface-version: 1 name: 906B0CE0-C70B-1067-B317-00DD010662DA object-interface-uuid: F88B382B-574E-4719-B3F8-8562B08A9801 protocol-sequence: ncacn_ip_tcp:172.23.202.110[1025] interface-uuid: 378E52B0-C0A9-11CF-822D-00AA0051E40F interface-version: 1 name: 378E52B0-C0A9-11CF-822D-00AA0051E40F protocol-sequence: ncacn_ip_tcp:172.23.202.110[1026] interface-uuid: 5A7B91F8-FF00-11D0-A9B2-00C04FB6E6FC interface-version: 1 name: Messenger Service protocol-sequence: ncadg_ip_udp:172.23.202.110[1028] NTP: 172.23.202.110 udp 123
Korisnička imena i grupe	Administrator, type User (Built-in account), user-id: 500 Administrators, type Group, group-id: 544 Backup Operators, type Group, group-id: 551 Guest, type User (Built-in account), user-id: 501 None, type Group, group-id: 513 Power Users Group group-id: 547 Replicator Group group-id: 552 TsInternetUser, type User (nalog za Terminal Services),user-id: 1000 Users, type Group, group-id: 545

Tabela 9. Windows OS – Pronađeni servisi na IP adresi 172.23.202.76 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni deljeni resurs, mount-point: C:\
SERVISI	CIFS ⁵⁰⁸ , CIFS Name Service ⁵⁰⁹ :

⁵⁰⁶ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datateka preko Interneta. Proširuje SMB ili Server Message Block protokoli dizajniran od strane IBM-a. CIFS obezbedjuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

⁵⁰⁷ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

⁵⁰⁸ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datateka preko Interneta. Proširuje SMB ili Server Message Block protokoli dizajniran od strane IBM-a. CIFS obezbedjuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

	advertised-name-1: Win2000srvsp4 (Computer Name) advertised-name-2: Win2000srvsp4 (File Server Service) advertised-name-3: WORKGROUP (Domain Name) advertised-name-4: WORKGROUP (Browser Service Elections) advertised-name-5: Win2000srvsp4 (Logged-on User) mac-address: 000C299A0E58 DCE RPC interface-uuid: 816A0CE0-C70B-1068-B318-00DD010662DB interface-version: 1 name: 816A0CE0-C70B-1068-B318-00DD010662DB object-interface-uuid: B88B382B-574E-4719-A3F8-8562B08A9801 protocol-sequence: ncacn_ip_tcp:172.23.202.76[1025] interface-uuid: 568E52B0-B0A9-11CF-822B-00AA0051E32A interface-version: 1 name: 568E52B0-B0A9-11CF-822B-00AA0051E32A protocol-sequence: ncacn_ip_tcp:172.23.202.76[1026] interface-uuid: 6B7B91F8-FF11-12B0-A9B2-00C04FB6E5BA interface-version: 1 name: Messenger Service protocol-sequence: ncadg_ip_udp:172.23.202.76[1028] NTP: 172.23.202.76 udp 123
Korisnička imena i grupe	Administrator, type User (Built-in account), user-id: 500 Administrators, type Group, group-id: 544 Backup Operators, type Group, group-id: 551 Guest, type User (Built-in account), user-id: 501 None, type Group, group-id: 513 Power Users Group group-id: 547 Replicator Group group-id: 552 TsInternetUser, type User (nalog za Terminal Services),user-id: 1000 Users, type Group, group-id: 545

Tabela 10. Windows OS sa IP adresama 172.23.202.111, 172.23.202.75, 172.23.202.74, 172.23.202.73 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.111		OS: Microsoft Windows 2003 Enterprise server x64 SP1, WIN2003ENX64sp1			14
IP adresa: 172.23.202.75		OS: Windows server 2003 Enterprise x86 SP1, WIN2003ENX86sp1			14
IP adresa: 172.23.202.74		OS: Windows server 2003 Standard x86 SP1, WIN2003StX86sp1			14
IP adresa: 172.23.202.73		OS: Windows server 2003 Standard x64 SP1, WIN2003StX64sp1			14
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Microsoft Server Service / CanonicalizePathName() Remote Code	Određene verzije Microsoft Windows-a su ranjive na daljinsko preopterećenje bafera (privremene memorije) koje bi moglo da	BID 19409 CERT TA06-220A CERT-VN 650769 CVE CVE-2006-3439	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003.Wind

⁵⁰⁹ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	Execution Vulnerability (dcerpc-msnetapi-netpathcanonicalize-dos)	kompromituje određeni računar. Posebno opremljen paket se može koristiti sa pozivom ka NetPathCanonicalize RPC ruti na servisu servera, pri čemu bi napadač mogao da izvrši kod pod sistemskim nivoom pristupa.	MS MS06-040 OVAL OVAL492 SECUNIA 21388 XF ms-server-service-bo(28002)		owsXP-KB921883-v2-x64.ENU.EXE ⁵¹⁰ , a za 32-bitnu verziju : WindowsServer2003-KB921883-v2-x86-ENU.exe ⁵¹¹
2.	MS03-039: Buffer Overrun In RPCSS Service Could Allow Code Execution (824146) (windows-hotfix-ms03-039)	Napadač koji je uspešno iskoristio ove ranjivosti bi mogao biti u mogućnosti da pokrene kôd sa privilegijama lokalnog sistema na pogođenom sistemu ili bi mogao da prouzrokuje kvar RPCSS servisa. Napadač bi tada mogao biti u mogućnosti da preduzme bilo kakvu radnju na sistemu, uključujući instaliranje programa, pregledavanje, menjanje i brisanje podataka ili stvaranje novih naloga sa svim privilegijama. Da bi iskoristio ove ranjivosti, napadač bi morao da napravi program sa kojim bi poslao malicioznu RPC poruku ranjivom sistemu, ciljajući na RPCSS servis.	BID: 8458 ⁵¹² , CVE: CVE-2003-0528 ⁵¹³ , CVE: CVE-2003-0605 ⁵¹⁴ , CVE: CVE-2003-0715 ⁵¹⁵ , MSKB: 824146 ⁵¹⁶ , MS: MS03-039 ⁵¹⁷	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003-KB824146-ia64-ENU.exe ⁵¹⁸ , a za 32-bitnu verziju WindowsXP-KB824146-x86-ENU.exe ⁵¹⁹ Uraditi download a zatim instalirati Microsoft patch WindowsServer2003-KB819696-ia64-ENU.exe ⁵²⁰ , a za 32-bitnu verziju WindowsServer2003-KB819696-x86-ENU.exe ⁵²¹
3.	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (windows-hotfix-ms08-067)	172.23.202.111:139 172.23.202.111:445 172.23.202.75:139 172.23.202.75:445 172.23.202.74:139 172.23.202.74:445 172.23.202.73:139 172.23.202.73:445 Ova bezbednosna ispravka rešava ranjivost koja je prijavljena od strane privatnog lica. Ranjivost bi mogla da omogućiti daljinsko izvršavanje koda ukoliko je napadnuti sistem primio posebno opremljeni RPC zahtev. Na sistemima Microsoft Windows 2000, Windows XP, i Windows Server	MS: MS08-067 ⁵²² MSKB: 958644 ⁵²³ CVE: CVE-2008-4250 ⁵²⁴ SECUNIA: 32326 ⁵²⁵ URL1 ⁵²⁶ URL2 ⁵²⁷ URL3 ⁵²⁸	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003.WindowsXP-KB958644-x64-ENU.exe (1288568 bytes) ⁵²⁹ , a za 32-bitnu verziju WindowsServer2003-KB958644-x86-ENU.exe ⁵³⁰

⁵¹⁰ <http://download.microsoft.com/download/3/9/e/39ee55a0-f350-4a1c-ab0f-a3525c072593/WindowsServer2003.WindowsXP-KB921883-v2-x64-ENU.exe>

⁵¹¹ <http://download.microsoft.com/download/6/e/e/6ee2a18d-b3a7-457a-af39-fb687fd6aa91/WindowsServer2003-KB921883-v2-x86-ENU.exe>

⁵¹² <http://www.securityfocus.com/bid/8458>

⁵¹³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0528>

⁵¹⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0605>

⁵¹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0715>

⁵¹⁶ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;824146>

⁵¹⁷ <http://technet.microsoft.com/en-us/security/bulletin/ms03-039>

⁵¹⁸ <http://www.microsoft.com/en-us/download/confirmation.aspx?id=13195>

⁵¹⁹ <http://download.microsoft.com/download/c/d/d/cdd7ac92-e4cc-4b1e-bc2f-7a61b46b23bf/WindowsXP-KB824146-x86-ENU.exe>

⁵²⁰ <http://www.microsoft.com/en-us/download/confirmation.aspx?id=627>

⁵²¹ <http://download.microsoft.com/download/5/e/6/5e6f9e28-b684-4788-8b1a-013eb62a41ba/WindowsServer2003-KB819696-x86-ENU.exe>

⁵²² <http://technet.microsoft.com/en-us/security/bulletin/ms08-067>

⁵²³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958644>

⁵²⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4250>

⁵²⁵ <http://secunia.com/advisories/32326/>

⁵²⁶ blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx

⁵²⁷ <http://blogs.msdn.com/b/sdl/archive/2008/10/22/ms08-067.aspx>

⁵²⁸ <http://blogs.technet.com/b/msrc/archive/2008/10/23/ms08-067-released.aspx>

⁵²⁹ download.windowsupdate.com/msdownload/update/software/secu/2008/10/windowsserver2003.windowsexp-kb958644-x64-enu_75717882c206870bdba8e8e606c588853fb8e34c.exe

⁵³⁰ <http://download.microsoft.com/download/e/e/3/ee322649-7f38-4553-a26b-a2ac40a0b205/WindowsServer2003-KB958644-x86-ENU.exe>

		2003, napadač bi mogao da iskoristi ovu ranjivost bez overavanja autentičnosti i da pokrene proizvoljan kôd. Moguće je da ova ranjivost može biti upotrebljena za intenziviranje skrivenog korišćenja. Najbolje prakse zaštitnog zida i standardne konfiguracije zaštitnog zida po difoltu mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan okvira preduzeća.			
4.	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (windows-hotfix-ms09-001)	172.23.202.111:139 172.23.202.111:445 172.23.202.75:139 172.23.202.75:445 172.23.202.74:139 172.23.202.74:445 172.23.202.73:139 172.23.202.73:445 Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti koje su privatno prijavljene, a odnose se na Microsoft Server Message Block (SMB). Ranjivosti mogu da omoguće daljinsko izvršenje koda na ugroženim sistemima. Napadač koji je uspešno iskoristion ove ranjivosti može da instalira programe, pregleda, menja ili briše podatke ili otvara nove naloge sa potpunim korisničkim pravima. Najbolje prakse zaštitnog zida i standardne konfiguracije zaštitnog zida po difoltu mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan okvira preduzeća. Za sisteme koji su stalno povezani na Internet preporuka je da imaju što manji broj izloženih portova.	MS: MS09-001 ⁵³¹ MSKB: 958687 ⁵³² CVE: CVE-2008-4114 ⁵³³ CVE: CVE-2008-4835 ⁵³⁴ CVE: CVE-2008-4834 ⁵³⁵ SECUNIA: 31883 ⁵³⁶ URL1 ⁵³⁷ URL2 ⁵³⁸ URL3 ⁵³⁹	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003-KB958687-ia64-ENU.exe (1691512 bytes) ⁵⁴⁰ , a za 32-bitnu verziju WindowsServer2003-KB958687-x86-ENU.exe ⁵⁴¹
5.	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-012)	172.23.202.111:139 172.23.202.111:445 172.23.202.75:139 172.23.202.75:445 172.23.202.74:139 172.23.202.74:445 172.23.202.73:139	MS: MS10-012 ⁵⁴² MSKB - 971468 ⁵⁴³ CVE: CVE-2010-0020 ⁵⁴⁴ CVE: CVE-2010-0021 ⁵⁴⁵ CVE: CVE-2010-0022 ⁵⁴⁶ CVE CVE-2010-0231 ⁵⁴⁷ SECUNIA 38510 ⁵⁴⁸	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003.WindowsXP-KB971468-x64-ENU.exe (1026944 bytes) ⁵⁴⁹ , a za 32-bitnu

⁵³¹ <http://technet.microsoft.com/en-us/security/bulletin/MS09-001>⁵³² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958687>⁵³³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4114>⁵³⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4835>⁵³⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4834>⁵³⁶ <http://secunia.com/advisories/31883/>⁵³⁷ http://www.vallejo.cc/proyectos/vista_SMB_write_DoS.htm⁵³⁸ <http://www.zerodayinitiative.com/advisories/ZDI-09-001/>⁵³⁹ <http://www.zerodayinitiative.com/advisories/ZDI-09-002/>⁵⁴⁰ download.windowsupdate.com/msdownload/update/software/secu/2008/12/windowsserver2003-kb958687-ia64-enu_a4d695fccfc7fc0071240d49035fbc9e6fbb16df.exe⁵⁴¹ <http://download.microsoft.com/download/6/9/8/698F11AA-15C7-4BAF-818D-2BCC1704F202/WindowsServer2003-KB958687-x86-ENU.exe>⁵⁴² <http://technet.microsoft.com/en-us/security/bulletin/MS10-012>⁵⁴³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;971468>⁵⁴⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0020>⁵⁴⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0021>⁵⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0022>⁵⁴⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0231>

	012)	172.23.202.73:445 Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti koje su privatno prijavljene u Microsoft Windows-u. Opasnost od ove ranjivosti leži u tome što bi ona omogućila daljinsko izvršavanje kôda ukoliko bi napadač kreirao posebno opremljen SMB paket i poslao ga ugroženom sistemu. Najbolje prakse zaštitnog zida i standardne konfiguracije zaštitnog zida po difoltu mogu da pomognu u zaštiti mrežnih resursa od napada (koji bi pokušali da iskoriste ove ranjivosti), a koji potiču izvan okvira organizacije.			verziju WindowsServer2003-KB971468-x86-ENU.exe ⁵⁵⁰
6.	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-054)	172.23.202.111:139 172.23.202.111:445 172.23.202.75:139 172.23.202.75:445 172.23.202.74:139 172.23.202.74:445 172.23.202.73:139 172.23.202.73:445 Opis je isti kao kod ranjivosti MS10-012	CVE: CVE-2010-2550 ⁵⁵¹ CVE: CVE-2010-2551 ⁵⁵² CVE: CVE-2010-2552 ⁵⁵³ MS: MS10-054 ⁵⁵⁴ MSKB 982214 ⁵⁵⁵	Kritičan	Uraditi download a zatim instalirati Microsoft patch windowsserver2003.windowssxp-kb982214-x64-enu.exe (1027968 bytes) ⁵⁵⁶ , a za 32-bitnu verziju WindowsServer2003-KB982214-x86-ENU.exe ⁵⁵⁷
7.	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms11-020)	172.23.202.111:139 172.23.202.111:445 172.23.202.75:139 172.23.202.75:445 172.23.202.74:139 172.23.202.74:445 172.23.202.73:139 172.23.202.73:445 Opis je isti kao kod ranjivosti MS10-012	CVE CVE-2011-0661 ⁵⁵⁸ MS: MS11-020 ⁵⁵⁹ MSKB: 2508429 ⁵⁶⁰	Kritičan	Uraditi download a zatim instalirati Microsoft patch windowsserver2003.windowssxp-kb2508429-x64-enu.exe (1044864 bytes) ⁵⁶¹ , a za 32-bitnu verziju WindowsServer2003-KB2508429-x86-ENU.exe ⁵⁶²
8.	MS03-026: Buffer Overrun In RPC Interface Could Allow Code Execution (823980) (windows-	Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti u Windows Distributed Component Object Model-u (DCOM) preko Remote Procedure Call-a (RPC). Napadač	CVE: CVE-2003-0352 ⁵⁶³ MS: MS03-026 ⁵⁶⁴ BID: 8205 ⁵⁶⁵ MSKB: 823980 ⁵⁶⁶	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003-KB823980-ia64-

⁵⁴⁸ <http://secunia.com/advisories/38510/>⁵⁴⁹ download.windowsupdate.com/msdownload/update/software/secu/2010/01/windowsserver2003.windowssxp-kb971468-x64-enu_8ea00e574a923da8a3aa9205a07780ed0a8741fa.exe⁵⁵⁰ <http://download.microsoft.com/download/F/5/B/F5BCEB3A-58B9-4FFE-8698-D0F74F02CAE2/WindowsServer2003-KB971468-x86-ENU.exe>⁵⁵¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2550>⁵⁵² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2551>⁵⁵³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2552>⁵⁵⁴ <http://technet.microsoft.com/en-us/security/bulletin/MS10-054>⁵⁵⁵ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;982214>⁵⁵⁶ download.windowsupdate.com/msdownload/update/software/secu/2010/07/windowsserver2003.windowssxp-kb982214-x64-enu_3780ab4068c4715ca93c4d5e4d9d4dbf9bbb6bc3.exe⁵⁵⁷ <http://download.microsoft.com/download/E/F/9/EF903A71-690C-4D73-A871-63E5932FD5E3/WindowsServer2003-KB982214-x86-ENU.exe>⁵⁵⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661>⁵⁵⁹ <http://technet.microsoft.com/en-us/security/bulletin/ms11-020>⁵⁶⁰ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;2508429>⁵⁶¹ download.windowsupdate.com/msdownload/update/software/secu/2011/03/windowsserver2003.windowssxp-kb2508429-x64-enu_a1ab44f33a891a3fdff7273ad240f35d5af7ce99.exe⁵⁶² <http://download.microsoft.com/download/E/D/7/ED71C471-3229-4120-B9E3-F6B03D7D3714/WindowsServer2003-KB2508429-x86-ENU.exe>⁵⁶³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0352>⁵⁶⁴ <http://technet.microsoft.com/en-us/security/bulletin/ms03-026>⁵⁶⁵ <http://www.securityfocus.com/bid/8205>⁵⁶⁶ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;823980>

	hotfix-ms03-026)	koji bi uspešno iskoristio ovu ranjivost mogao bi da pokrene kôd sa privilegijama lokalnog sistema na napadnutom sistemu. Napadač bi mogao da preduzme bilo kakvu akciju na sistemu, uključujući instaliranje programa, pregledanje, izmenu ili brisanje podataka ili otvaranje novih naloga sa svim privilegijama. Da bi iskoristio ovu ranjivost, napadač bi morao da pošalje posebno formiran zahtev udaljenom računaru ka specifičnim RPC portovima.			ENU.exe ⁵⁶⁷ , a za 32-bitnu verziju WindowsServer2003-KB823980-x86-ENU.exe ⁵⁶⁸
9.	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (windows-hotfixms06-035)	Ovo ažuriranje rešava nekoliko otkrivenih i privatno prijavljenih ranjivosti. Preporučuje se da korisnici odmah primene update.	BID 18863 ⁵⁶⁹ CVE: CVE-2006-1314 ⁵⁷⁰ CVE: VE-2006-1315 ⁵⁷¹ MS: MS06-035 ⁵⁷² MSKB: 917159 ⁵⁷³ SANS-06: W4 ⁵⁷⁴ SANS-07: S2 ⁵⁷⁵ SECUNIA: 21007 ⁵⁷⁶ XF: win-mailslot-bo(26818) ⁵⁷⁷ XF win-smb-information-disclosure(26820) ⁵⁷⁸ URL1 ⁵⁷⁹	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003.WindowsXP-KB917159-x64-ENU.exe (1033528 bytes) ⁵⁸⁰ , a za 32-bitnu verziju WindowsServer2003-KB917159-x86-ENU.exe ⁵⁸¹
10.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.111:139 172.23.202.111:445 172.23.202.75:139 172.23.202.75:445 172.23.202.74:139 172.23.202.74:445 172.23.202.73:139 172.23.202.73:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB: 887429 ⁵⁸² URL1 ⁵⁸³	Ozbiljan	Metoda za konfiguracije SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429. Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing</i> = <i>auto</i> ili da se zahteva SMB potpisivanje: <i>server signing</i> = <i>mandatory</i> .
11.	SMB signing not	172.23.202.111:139 172.23.202.111:445	Isto kao kod „SMB	Ozbiljan	Isto kao kod „SMB signing

⁵⁶⁷ <http://www.microsoft.com/en-us/download/confirmation.aspx?id=186>⁵⁶⁸ <http://download.microsoft.com/download/8/f/2/8f21131d-9df3-4530-802a-2780629390b9/WindowsServer2003-KB823980-x86-ENU.exe>⁵⁶⁹ <http://www.securityfocus.com/bid/18863>⁵⁷⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1314>⁵⁷¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1315>⁵⁷² <http://technet.microsoft.com/en-us/security/bulletin/ms06-035>⁵⁷³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;917159>⁵⁷⁴ <http://www.sans.org/critical-security-controls/#w4>⁵⁷⁵ <http://www.sans.org/critical-security-controls/#s2>⁵⁷⁶ <http://secunia.com/advisories/21007/>⁵⁷⁷ <http://xforce.iss.net/xforce/xfdb/26818>⁵⁷⁸ <http://xforce.iss.net/xforce/xfdb/26820>⁵⁷⁹ <http://technet.microsoft.com/en-us/security/bulletin/MS06-035>⁵⁸⁰ www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsserver2003.windowsexp-kb917159-x64-enu_93a5cfec377221668b923e88a741ce1cadcb76c1.exe⁵⁸¹ <http://download.microsoft.com/download/e/f/e/efef9f44-94fd-4659-8b95-db20ca3378d9/WindowsServer2003-KB917159-x86-ENU.exe>⁵⁸² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429>⁵⁸³ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>

	required (cifs-smb-signing-not-required)	172.23.202.75:139 172.23.202.75:445 172.23.202.74:139 172.23.202.74:445 172.23.202.73:139 172.23.202.73:445 Sistem omogućava ali ne zahteva SMB potpisivanje.	signing disabled (cifs-smb-signing-disabled) ⁵⁸⁴ ranjivosti		disabled (cifs-smb-signing-disabled) ⁵⁸⁴ ranjivosti
12.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	172.23.202.111:135 172.23.202.75:135 172.23.202.74:135 172.23.202.73:135 Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183 ⁵⁸⁴ CERT TA04-111A ⁵⁸⁵ CERT-VN: 415294 ⁵⁸⁶ CVE CVE-2004-0230 ⁵⁸⁷ MS: MS05-019 ⁵⁸⁸ MS: MS06-064 ⁵⁸⁹ NETBSD: NetBSD-SA2004-006 ⁵⁹⁰ OSVDB 4030 ⁵⁹¹ OVAL: OVAL2689 ⁵⁹² OVAL: OVAL270 ⁵⁹³ OVAL OVAL3508 ⁵⁹⁴ OVAL OVAL4791 ⁵⁹⁵ OVAL OVAL5711 ⁵⁹⁶ SECUNIA: 11440 ⁵⁹⁷ SECUNIA: 22341 ⁵⁹⁸ SECUNIA 11458 ⁵⁹⁹ SGI 20040403-01-A ⁶⁰⁰ XF tcp-rst-dos(15886) ⁶⁰¹ URL1 ⁶⁰²	Ozbiljan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003.WindowsXP-KB922819-x64-ENU.exe (898360 bytes) ⁶⁰³ , a za 32-bitnu verziju WindowsServer2003-KB922819-x86-ENU.exe ⁶⁰⁴
13.	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server. Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko poziva udaljenih procedura (RPC). Ovi servisi su i u prošlosti bili skloni	BID: 494 ⁶⁰⁵ CVE: CVE-1999-0519 ⁶⁰⁶ MSKB: 143474 ⁶⁰⁷ URL1 ⁶⁰⁸	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost

⁵⁸⁴ <http://www.securityfocus.com/bid/10183>⁵⁸⁵ <http://www.us-cert.gov/ncas/alerts/ta04-111a>⁵⁸⁶ <http://www.kb.cert.org/vuls/id/415294>⁵⁸⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁵⁸⁸ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁵⁸⁹ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁵⁹⁰ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁵⁹¹ <http://www.osvdb.org/4030>⁵⁹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>⁵⁹³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>⁵⁹⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>⁵⁹⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>⁵⁹⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>⁵⁹⁷ <http://secunia.com/advisories/11440/>⁵⁹⁸ <http://secunia.com/advisories/22341/>⁵⁹⁹ <http://secunia.com/advisories/11458/>⁶⁰⁰ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>⁶⁰¹ <http://xforce.iss.net/xforce/xfdb/15886>⁶⁰² <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁶⁰³ www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsserver2003.windowsexp-kb922819-x64-enu_4c34629b0664f2d2cd78c0276e4bd6b5e72ede61.exe⁶⁰⁴ <http://download.microsoft.com/download/a/d/2/ad2acd40-3ae7-49d3-88fe-064a71ccc61a/WindowsServer2003-KB922819-x86-ENU.exe>⁶⁰⁵ <http://www.securityfocus.com/bid/494>⁶⁰⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>⁶⁰⁷ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>⁶⁰⁸ http://www.hsc.fr/ressources/presentations/null_sessions/

		ranjivosti.. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinjenije napade.			
14.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	OSVDB 95 ⁶⁰⁹ CVE: CVE-1999-0524 ⁶¹⁰ XF: icmp-netmask(306) ⁶¹¹ XF: icmp-timestamp(322) ⁶¹²	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost

Tabela 11. Windows OS – Pronađeni servisi na IP adresi 172.23.202.111 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni deljeni resurs, mount-point: C:\
SERVISI	CIFS ⁶¹³ , CIFS Name Service ⁶¹⁴ : advertised-name-1: WIN2003ENX64sp1 (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: WIN2003ENX64sp1 (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 000C295DCFC7 DCE RPC interface-uuid: 12345778-1234-ABCD-EF00-0123456789AC interface-version: 1 name: 12345778-1234-ABCD-EF00-0123456789AC protocol-sequence: ncacn_ip_tcp:172.23.202.111[1025] interface-uuid: 0A74EF1C-41A4-4E06-83AE-DC74FB1CDD53 interface-version: 1 name: 0A74EF1C-41A4-4E06-83AE-DC74FB1CDD53 protocol-sequence: ncacn_ip_tcp:172.23.202.111[1026]

Tabela 12. Windows OS – Pronađeni servisi na IP adresi 172.23.202.75 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni deljeni resurs, mount-point: C:\

⁶⁰⁹ <http://www.osvdb.org/95>⁶¹⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁶¹¹ <http://xforce.iss.net/xforce/xfdb/306>⁶¹² <http://xforce.iss.net/xforce/xfdb/322>⁶¹³ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).⁶¹⁴ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

SERVISI	CIFS⁶¹⁵, CIFS Name Service⁶¹⁶ : advertised-name-1: WIN2003ENX64sp1 (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: WIN2003ENX64sp1 (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 000C296ABCC7 DCE RPC interface-uuid: 12345778-2222-DCBA-BF00-5123466786AB interface-version: 1 name: 12345778-2222-DCBA-BF00-5123466786AB protocol-sequence: ncacn_ip_tcp:172.23.202.75[1025] interface-uuid: 0A74EF1C-41A4-4E06-83AE-DC74FB1CDD53 interface-version: 1 name: 0A74EF1C-41A4-4E06-83AE-DC74FB1CDD53 protocol-sequence: ncacn_ip_tcp:172.23.202.75[1026]

Tabela 13. Windows OS – Pronađeni servisi na IP adresi 172.23.202.74 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni deljeni resurs, mount-point: C:\
SERVISI	CIFS⁶¹⁷, CIFS Name Service⁶¹⁸ : advertised-name-1: WIN2003ENX64sp1 (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: WIN2003ENX64sp1 (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 001H395DABC6 DCE RPC interface-uuid: 22222778-1234-ABCD-EF00-0123336789FF interface-version: 1 name: 22222778-1234-ABCD-EF00-0123336789FF protocol-sequence: ncacn_ip_tcp:172.23.202.74[1025] interface-uuid: 0A88EF2B-52A4-4E07-85AE-DC74FB1CAA53 interface-version: 1 name: 0A88EF2B-52A4-4E07-85AEDC74FB1CAA53 protocol-sequence: ncacn_ip_tcp:172.23.202.74[1026]

Tabela 14. Windows OS – Pronađeni servisi na IP adresi 172.23.202.73 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin)

⁶¹⁵ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

⁶¹⁶ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

⁶¹⁷ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

⁶¹⁸ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

SERVISI	C\$ - difoltni deljeni resurs, mount-point: C:\ CIFS⁶¹⁹, CIFS Name Service⁶²⁰ : advertised-name-1: WIN2003ENX64sp1 (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: WIN2003ENX64sp1 (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 020C295DCFC7 DCE RPC interface-uuid: 88885778-1234-ABCD-EF00-4444458889AC interface-version: 1 name: 88885778-1234-ABCD-EF00-4444458889AC protocol-sequence: ncacn_ip_tcp:172.23.202.73[1025] interface-uuid: 1A77EF1D-42A4-4B06-89AE-DC74FB1CDD56 interface-version: 1 name: 1A77EF1D-42A4-4B06-89AEDC74FB1CDD56 protocol-sequence: ncacn_ip_tcp:172.23.202.73[1026]

Tabela 15. Windows OS sa IP adresom 172.23.202.101 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.101		OS: Microsoft Windows NT 4 Enterprise Sp6, NT4entsp6			21
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	MS03-039: Buffer Overrun In RPCSS Service Could Allow Code Execution (824146) (windows-hotfix-ms03-039)	Napadač koji bi uspešno iskoristio ove ranjivosti mogao bi da pokrene kôd sa privilegijama lokalnog sistema na napadnutom sistemu, ili bi mogao da prouzrokuje isključenje RPCSS servisa. Napadač bi tada bio u mogućnosti da preduzme bilo kakvu akciju na sistemu, uključujući instaliranje programa, pregledanje, menjanje ili brisanje podataka ili otvaranje novih naloga sa svih privilegijama. Da bi iskoristio ove ranjivosti, napadač bi morao da napravi program sa kojim bi poslao malicioznu RPC poruku ranjivom sistemu, ciljajući na RPCSS servis.	BID: 8458 ⁶²¹ , CVE: CVE-2003-0528 ⁶²² , CVE: CVE-2003-0605 ⁶²³ , CVE: CVE-2003-0715 ⁶²⁴ , MSKB: 824146 ⁶²⁵ , MS:MS03-039 ⁶²⁶	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsNT4Workstation-KB824146-x86-ENU.EXE ⁶²⁷

⁶¹⁹ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

⁶²⁰ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

⁶²¹ <http://www.securityfocus.com/bid/8458>

⁶²² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0528>

⁶²³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0605>

⁶²⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0715>

⁶²⁵ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;824146>

⁶²⁶ <http://technet.microsoft.com/en-us/security/bulletin/ms03-039>

⁶²⁷ download.microsoft.com/download/3/0/c/30cff3cd-414d-4754-b9db-276de8161eef/windowsnt4workstation-kb824146-x86-enu.exe

2.	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (windows-hotfix-ms09-001)	172.23.202.101:139 172.23.202.101:445 Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti koje su privatno prijavljene, a odnose se na protokol Microsoft Server Message Block-a (SMB). Ove ranjivosti bi mogle da omoguće izvršenje udaljenog kôda na napadnutim sistemima. Napadač koji bi uspešno iskoristio ove ranjivosti mogao bi da instalira programe, pregleda, menja ili briše podatke ili pak da kreira nove naloge sa punim pravima korisnika. Dosadašnja praksa fajervola i standardne fajervol difolt konfiguracije mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan organizacije. Za sisteme koji su stalno povezani na Internet preporuka je da imaju što manji broj izloženih portova.	MS: MS09-001 ⁶²⁸ MSKB: 958687 ⁶²⁹ CVE: CVE-2008-4114 ⁶³⁰ CVE: CVE-2008-4835 ⁶³¹ CVE: CVE-2008-4834 ⁶³² SECUNIA: 31883 ⁶³³ URL1 ⁶³⁴ URL2 ⁶³⁵ URL3 ⁶³⁶	Kritičan	Nema adekvatne zakrpe zbog prestanka podrške. Rešenje ažuriranje Operativnog sistema.
3.	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-012)	172.23.202.101:139 172.23.202.101:445 Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti koje su privatno prijavljene u Microsoft Windows-u. Opasnost od ove ranjivosti leži u tome što bi ona omogućila daljinsko izvršavanje kôda ukoliko bi napadač kreirao posebno opremljen SMB paket i poslao ga ugroženom sistemu. Praksa je pokazala da upotreba zaštitnog zida može da pomogne u zaštiti mrežnih resursa od napada (koji bi pokušali da iskoriste ove ranjivosti), a koji potiču izvan okvira organizacije.	MS: MS10-012 ⁶³⁷ MSKB - 971468 ⁶³⁸ CVE: CVE-2010-0020 ⁶³⁹ CVE: CVE-2010-0021 ⁶⁴⁰ CVE: CVE-2010-0022 ⁶⁴¹ CVE CVE-2010-0231 ⁶⁴² SECUNIA 38510 ⁶⁴³	Kritičan	Blokirati portove 139 i 445 na spoljnom fajervolu. Treba imati u vidu da će ova ranjivost takođe uticati na sisteme Windows 2000, a usled zastarevanja Windows 2000; ne postoji odgovarajuća zakrpa koja bi omogućila ublažavanje ove ranjivosti.
4.	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-054)	172.23.202.101:139 172.23.202.101:445 Opis je isti kao kod ranjivosti MS10-012	CVE: CVE-2010-2550 ⁶⁴⁴ CVE: CVE-2010-2551 ⁶⁴⁵ CVE: CVE-2010-2552 ⁶⁴⁶ MS: MS10-054 ⁶⁴⁷ MSKB 982214 ⁶⁴⁸	Kritičan	Blokirati portove 139 i 445 na spoljnom fajervolu. Treba imati u vidu da će ova ranjivost takođe uticati na sisteme Windows 2000, a usled zastarevanja Windows 2000; ne postoji

⁶²⁸ <http://technet.microsoft.com/en-us/security/bulletin/MS09-001>⁶²⁹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958687>⁶³⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4114>⁶³¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4835>⁶³² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4834>⁶³³ <http://secunia.com/advisories/31883/>⁶³⁴ http://www.vallejo.cc/proyectos/vista_SMB_write_DoS.htm⁶³⁵ <http://www.zerodayinitiative.com/advisories/ZDI-09-001/>⁶³⁶ <http://www.zerodayinitiative.com/advisories/ZDI-09-002/>⁶³⁷ <http://technet.microsoft.com/en-us/security/bulletin/MS10-012>⁶³⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;971468>⁶³⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0020>⁶⁴⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0021>⁶⁴¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0022>⁶⁴² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0231>⁶⁴³ <http://secunia.com/advisories/38510/>⁶⁴⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2550>⁶⁴⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2551>⁶⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2552>⁶⁴⁷ <http://technet.microsoft.com/en-us/security/bulletin/MS10-054>⁶⁴⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;982214>

					odgovarajuća zakrpa koja bi omogućila ublažavanje ove ranjivosti.
5.	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms11-020)	172.23.202.101:139 172.23.202.101:445 Opis je isti kao kod ranjivosti MS10-012	CVE CVE-2011-0661 ⁶⁴⁹ MS: MS11-020 ⁶⁵⁰ MSKB: 2508429 ⁶⁵¹	Kritičan	Blokirati portove 139 i 445 na spoljnom fajervolu. Treba imati u vidu da će ova ranjivost takode uticati na sisteme Windows 2000, a usled zastarevanja Windows 2000; ne postoji odgovarajuća zakrpa koja bi omogućila ublažavanje ove ranjivosti.
6.	Anonymous users can obtain the Windows password policy (cifs-nt-0002)	Korišćenjem CIFS NULL sesije, anonimni korisnik može da dobije uvid u polisu šifri. Polisa šifri sadrži osetljive informacije o najmanjoj mogućoj dužini lozinke, zaključavanje šifre, vremensko trajanje zaključanosti šifre itd.	SANS-01 W5 ⁶⁵² CVE CVE-2000-1200 ⁶⁵³ MSKB 143474 ⁶⁵⁴ XF nt-lsa-domain-sid(4015) ⁶⁵⁵ MSKB 823659 ⁶⁵⁶ MSKB 246261 ⁶⁵⁷ MSKB 129457 ⁶⁵⁸ SANS-02 W5 ⁶⁵⁹ BID 959 ⁶⁶⁰ SANS-04 W3 ⁶⁶¹ SANS-03 W5 ⁶⁶² BID 87 ⁶⁶³		Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost
7.	MS03-026: Buffer Overrun In RPC Interface Could Allow Code Execution (823980) (windows-hotfix-ms03-026)	Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti u Windows Distributed Component Object Model-u (DCOM) preko Remote Procedure Call-a (RPC). Napadač koji bi uspešno iskoristio ovu ranjivost mogao bi da pokrene kôd sa privilegijama lokalnog sistema na napadnutom sistemu. Napadač bi mogao da preduzme bilo kakvu akciju na sistemu, uključujući instaliranje programa, pregledanje, izmenu ili brisanje podataka ili otvaranje novih naloga sa svim privilegijama. Da bi iskoristio ovu ranjivost, napadač bi morao da pošalje posebno formiran zahtev udaljenom računaru na specifične RPC portove.	CVE: CVE-2003-0352 ⁶⁶⁴ MS: MS03-026 ⁶⁶⁵ BID: 8205 ⁶⁶⁶ MSKB: 823980 ⁶⁶⁷	Kritičan	Uraditi download a zatim instalirati Microsoft patch Q823980i.EXE ⁶⁶⁸ Napomena: Posle instaliranja ove zakrpe obavezno je restart sistema.

⁶⁴⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661>⁶⁵⁰ <http://technet.microsoft.com/en-us/security/bulletin/ms11-020>⁶⁵¹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;2508429>⁶⁵² <http://www.sans.org/critical-security-controls/#w5>⁶⁵³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2000-1200>⁶⁵⁴ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>⁶⁵⁵ <http://xforce.iss.net/xforce/xfdb/4015>⁶⁵⁶ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;823659>⁶⁵⁷ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;246261>⁶⁵⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;129457>⁶⁵⁹ <http://www.sans.org/critical-security-controls/#w5>⁶⁶⁰ <http://www.securityfocus.com/bid/959>⁶⁶¹ <http://www.sans.org/critical-security-controls/#w3>⁶⁶² <http://www.sans.org/critical-security-controls/#w5>⁶⁶³ <http://www.securityfocus.com/bid/87>⁶⁶⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0352>⁶⁶⁵ <http://technet.microsoft.com/en-us/security/bulletin/ms03-026>⁶⁶⁶ <http://www.securityfocus.com/bid/8205>⁶⁶⁷ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;823980>⁶⁶⁸ download.microsoft.com/download/6/5/1/651c3333-4892-431f-ae93-bf8718d29e1a/q823980i.exe

8.	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (windows- hotfixms06- 035)	Ovo ažuriranje rešava nekoliko otkrivenih i privatno prijavljenih ranjivosti. Preporučuje se da korisnici odmah primene update.	CVE: CVE-2006-1314 ⁶⁶⁹ CVE: VE-2006-1315 ⁶⁷⁰ MS: MS06-035 ⁶⁷¹ MSKB: 917159 ⁶⁷² SANS-06: W4 ⁶⁷³ SANS-07: S2 ⁶⁷⁴ SECUNIA: 21007 ⁶⁷⁵ XF: win-mailslot- bo(26818) ⁶⁷⁶ XF win-smb-information- disclosure(26820) ⁶⁷⁷	Kritičan	Nema adekvatne zakrpe zbog prestanka podrške za ovaj OS. Rešenje: ažurirati sistem novijom verzijom operativnog sistema.
9.	CIFS Account Password Never Expires (cifs-acct- password-never- expires)	CIFS nalog ne zahteva vremensko ograničenje šifre. Ovo je rizik za bezbednost. Ako šifra nije vremenski ograničena, to omogućava zlonamernom napadaču da izvrši napad sa ciljem otkrivanja korisničke šifre. Ukoliko rok trajanja šifre nikada ne ističe, napad se može sprovoditi tokom dužeg perioda, što povećava mogućnost da šifra bude otkrivena.		Ozbiljan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 pod primerom Opšte ranjivosti
10.	SMB signing disabled (cifs-smb-signing- disabled)	172.23.202.101:139 172.23.202.101:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje omogućava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB: 887429 ⁶⁷⁸ URL1 ⁶⁷⁹	Ozbiljan	Metoda za konfiguracije SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429 ⁶⁸⁰ . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing</i> = <i>auto</i> ili da se zahteva SMB potpisivanje: <i>server</i> <i>signing</i> = <i>mandatory</i> .
11.	Microsoft IIS 3.0 newdsn.exe File Creation Vulnerability (http-iis-0017)	172.23.202.101:80 Microsoft IIS 3.0 se instalira po difoltu zajedno sa programom newdsn.exe u direktorijumu wwwroot/scripts/tools/. Pokretanje ovog programa sa odgovarajućim prosleđenim URL-om može omogućiti daljisko kreiranje fajlova. Tako kreiran fajl je Microsoft Access Database formata, ali može imati bilo kakvu ekstenziju, uključujući i .html.	BID 1818 ⁶⁸¹ CVE CVE-1999-0191 ⁶⁸² SANS-03 W1 ⁶⁸³ XF http-cgi- newdsn(1530) ⁶⁸⁴	Ozbiljan	Ukloniti sve semplovane programe sa servera. Takođe iz direktorijuma wwwroot/scripts/tools ukloniti fajl newdsn.exe
12.	SMB signing not	172.23.202.101:139	Isto kao kod „SMB	Ozbiljan	Isto kao kod „SMB signing

⁶⁶⁹<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1314>⁶⁷⁰<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1315>⁶⁷¹<http://technet.microsoft.com/en-us/security/bulletin/ms06-035>⁶⁷²<http://support.microsoft.com/default.aspx?scid=kb;EN-US;917159>⁶⁷³<http://www.sans.org/critical-security-controls/#w4>⁶⁷⁴<http://www.sans.org/critical-security-controls/#s2>⁶⁷⁵<http://secunia.com/advisories/21007/>⁶⁷⁶<http://xforce.iss.net/xforce/xfdb/26818>⁶⁷⁷<http://xforce.iss.net/xforce/xfdb/26820>⁶⁷⁸<http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429>⁶⁷⁹<http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>⁶⁸⁰<http://support.microsoft.com/kb/887429>⁶⁸¹<http://www.securityfocus.com/bid/1818>⁶⁸²<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0191>⁶⁸³<http://www.sans.org/critical-security-controls/#w1>⁶⁸⁴<http://xforce.iss.net/xforce/xfdb/1530>

	required (cifs-smb-signing-not-required)	172.23.202.101:445 Sistem omogućava ali ne zahteva SMB potpisivanje.	signing disabled (cifs-smb-signing-disabled)“ ranjivosti		disabled (cifs-smb-signing-disabled)“ ranjivosti
13.	Weak LAN Manager hashing permitted (cifs-generic-0005)	Ovaj sistem omogućava udaljenim korisnicima da se autentifikuju kroz LAN Manager (LM) heš mehanizam za otkrivanje lozinke. LM heš vrednost se lako može kreirati presretanjem korisničke komunikacije na mreži. Microsoft je obezbedio metod autentifikacije pod imenom NTLMv2 koji uvek treba koristiti umesto LM. NTLMv2 je dostupan na Windows NT 4.0 SP4 i na kasnijim verzijama (uključujući Windows 2000, Windows XP i Windows 2003).	SANS-02 W6 ⁶⁸⁵ URL1 ⁶⁸⁶ SANS-03 W3 ⁶⁸⁷ SANS-04 W5 ⁶⁸⁸ SANS-01 W6 ⁶⁸⁹	Ozbiljan	Ažurirati metod autorizacije korišćenjem registra. Treba imati u vidu da će ažuriranje metode autorizacije na NTLMv2 ukinuti kompatibilnost sa sistemima Windows 95/98/ME i starijim sistemima, pre -NT4 SP4. Pokrenuti editovanje registra (regedit.exe ili regedt32.exe) i potražiti do sledeće stavke: „HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa“ a zatim postaviti sledeću vrednost: -Naziv vrednosti: LMCompatibilityLevel -tip podataka: REG_DWORD -Podaci: treba koristiti najmanje nivo 3, ali se preporučuje nivo 5. Dodatno uraditi registarska podešavanja prema Microsoft uputstvu Q147706 ⁶⁹⁰
14.	FTP access with ftp account (ftp-generic-0001)	172.23.202.101:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisnikovim ID-jem (identifikacijom) "ftp" i šifrom "ftp". Dosadašnja praksa je pokazala da je najbolje ukloniti difoltnu naloge, ukoliko je to moguće. Za naloge koje sistem zahteva treba izmeniti difoltnu šifru.	CVE CVE-1999-0497 ⁶⁹¹	Ozbiljan	Ukloniti ili onemogućiti nalog, ukoliko to nije kritično za funkcionisanje sistema. U suprotnom, lozinku treba promeniti u onu koja nije po difoltu.
15.	FTP access with anonymous account (ftp-generic-0002)	172.23.202.101:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisnikovim ID-jem (identifikacijom) "anonymous" i lozinkom "ftp@". Dosadašnja praksa je pokazala da je najbolje ukloniti difoltnu naloge, ukoliko je to moguće. Za naloge koje sistem zahteva treba izmeniti difoltnu šifru.	CVE CVE-1999-0497 ⁶⁹²	Ozbiljan	Ukloniti ili onemogućiti nalog, ukoliko to nije kritično za funkcionisanje sistema. U suprotnom, lozinku treba promeniti u onu koja nije po difoltu.
16.	FTP server does not support AUTH command (ftp-generic-0007)	FTP klijenti po difoltu šalju FTP server-u poverljive podatke (korisnički ID i šifra) u vidu čitkog teksta. Ova okolnost dozvoljava zlonamernim korisnicima da presreću poverljive podatke ukoliko prisluškuju vezu.		Ozbiljan	Ažurirati/preći na FTP server koji podržava AUTH komandu.

⁶⁸⁵ <http://www.sans.org/critical-security-controls/#w6>⁶⁸⁶ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;147706>⁶⁸⁷ <http://www.sans.org/critical-security-controls/#w3>⁶⁸⁸ <http://www.sans.org/critical-security-controls/#w5>⁶⁸⁹ <http://www.sans.org/critical-security-controls/#w6>⁶⁹⁰ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;147706>⁶⁹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>⁶⁹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>

		Noviji FTP serveri podržavaju AUTH komandu, koja omogućava dodatne opcije autentifikacije, kao što su TLS, Kerberos, GSSAPI itd. Ona se može koristiti za sprečavanje prisluškivanja na FTP vezama.			
17.	NT IIS4 Remote Web-Based Administration Vulnerability (http-iis-0018)	172.23.202.101:80 Administriranje za IIS 4.0 je po defaultu ograničen na lokalnu mrežnu loopback adresu, 127.0.0.1. U slučajevima kada je IIS 4.0 instaliran kao nadogradnja IIS 2.0 ili 3.0, a prethodna verzija ISAPI DLL (ISM.DLL) je ostala u direktorijumu /scripts/iisadmin. Napadač može da pozove DLL preko sledeće sintakse: http://www.server.com/scripts/iisadmin/ism.dll?http/dir Ovaj URL traži od korisnika korisničko ime/lozinku da bi pristupio administrativnoj konzoli. Iako omogućen pristup ne dozvoljava korisnicima da vrši izmene na IIS serveru, može im dozvoliti da prikupi osetljive informacije o mrežnom serveru i njegovoj konfiguraciji.	BID 189 ⁶⁹³ CVE CVE-1999-1538 ⁶⁹⁴ URL1 695	Ozbiljan	Izbrisati ISM.DLL iz direktorijuma /scripts/iisadmin.
18.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	172.23.202.101:135: Ovo ažuriranje rešava nekoliko novootkrivenih ranjivosti. Napadač koji uspešno iskoristi ovu ranjivost bi mogao da preuzme potpunu kontrolu nad napadnutim sistemom, uključujući instaliranje programa, pregledanje, menjanje ili brisanje podataka ili čak otvaranje novih naloga sa svim privilegijama. Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183 ⁶⁹⁶ CERT-VN: 415294 ⁶⁹⁷ CVE CVE-2004-0230 ⁶⁹⁸ MS: MS05-019 ⁶⁹⁹ MS: MS06-064 ⁷⁰⁰ NETBSD: NetBSD-SA2004-006 ⁷⁰¹ OVAL: OVAL2689 ⁷⁰² OVAL: OVAL270 ⁷⁰³ OVAL OVAL3508 ⁷⁰⁴ OVAL OVAL4791 ⁷⁰⁵ OVAL OVAL5711 ⁷⁰⁶ SECUNIA: 11440 ⁷⁰⁷ SECUNIA: 22341 ⁷⁰⁸ SGI 20040403-01-A ⁷⁰⁹	Ozbiljan	Nema adekvatne zakrpe zbog prestanka podrške za ovaj OS. Rešenje : ažurirati sistem novijom verzijom operativnog sistema.
19.	FTP server uses predictable port numbers for PASV	FTP server koristi sekvencijalne brojeve za portove za PASV FTP veze. FTP server je koristio portove 1030, 1031, 1032, 1033, 1034, što je	CVE CVE-1999-0351 ⁷¹⁰ URL1 711 BID 5461⁷¹² CERT-VN 2558⁷¹³	Ozbiljan	Ažurirati verziju FTP servera i Operativnog sistema koji dodeljuje otvorene brojeve portova po

⁶⁹³ <http://www.securityfocus.com/bid/189>⁶⁹⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-1538>⁶⁹⁵ <http://www.securityfocus.com/bid/189>⁶⁹⁶ <http://www.securityfocus.com/bid/10183>⁶⁹⁷ <http://www.kb.cert.org/vuls/id/415294>⁶⁹⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁶⁹⁹ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁷⁰⁰ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁷⁰¹ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁷⁰² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>⁷⁰³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>⁷⁰⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>⁷⁰⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>⁷⁰⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>⁷⁰⁷ <http://secunia.com/advisories/11440/>⁷⁰⁸ <http://secunia.com/advisories/22341/>⁷⁰⁹ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>⁷¹⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0351>⁷¹¹ http://www.cert.org/tech_tips/ftp_port_attacks.html⁷¹² <http://www.securityfocus.com/bid/5461>

	connections (ftp-pasv-predictable-ports)	predvidiv redosled. Ovo bi moglo olakšati napadaču da presretne ili prisvoji autorizovane FTP veze sa serverom i pristupi ili ukrade fajlove na FTP serveru. Ovo je uglavnom poznato kao napad "Pizza Thief"-a. FTP serveri bi trebalo da koriste pseudoslučajne brojeve za portove za PASV veze da bi otežali napadaču da prisvaja sesije. Važno je imati u vidu da na mnogim platformama brojeve portova bira operativni sistem, a ne FTP server. To ovu ranjivost čini još opasnijom, jer bi napadač mogao da iskoristi FTP serverov PASV mehanizam da predvidi brojeve portova za ostale (ne-FTP) servise.	XF openunix-unixware-pasv-hijacking(9253) ⁷¹⁴ BID 4895 ⁷¹⁵ MSKB 260934 ⁷¹⁶		naizmeničnom redosledu, a ne po redu. Uzeti u obzir da ažuriranje FTP servera bez ažuriranja operativnog sistema možda ne da željeni rezultat. Za IIS FTP servere na Windows 2000, ažuriranje na Windows 2000 Service Pack 1 će dati rezultat. Za više informacija pogledati Microsoft Knowledge Base Article Q260934 ⁷¹⁷ . Za wu-ftpd servere ažurirati na verziju wu-ftpd version 2.5.0 ili novije.
20.	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server . Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko RPC funkcionalnih poziva. Ovi servisi su i u prošlosti bili skloni ranjivostima. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinejnije napade.	BID: 494 ⁷¹⁸ CVE: CVE-1999-0519 ⁷¹⁹ MSKB: 143474 ⁷²⁰ URL1 ⁷²¹	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost
21.	Database Open Access (database-open-access)	172.23.202.101:70 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posredovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7. ⁷²²	URL1 ⁷²³	Umeren	Konfigurisati server baze podataka tako da dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.

⁷¹³ <http://www.kb.cert.org/vuls/id/2558>⁷¹⁴ <http://xforce.iss.net/xforce/xfdb/9253>⁷¹⁵ <http://www.securityfocus.com/bid/4895>⁷¹⁶ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;260934>⁷¹⁷ <http://smallbusiness.support.microsoft.com/en-au/kb/260934>⁷¹⁸ <http://www.securityfocus.com/bid/494>⁷¹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>⁷²⁰ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>⁷²¹ http://www.hsc.fr/ressources/presentations/null_sessions/⁷²² https://www.pcisecuritystandards.org/pdfs/pci_dss_sa_q_navigating_dss.pdf⁷²³ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf

Tabela 16. Windows OS – Pronađeni servisi na IP adresi 172.23.202.101 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni deljeni resurs, mount-point: C:\
SERVISI	CIFS⁷²⁴, CIFS Name Service⁷²⁵ : advertised-name-1: NT4ent6 (Computer Name) advertised-name-10: __MSBROWSE__ (Master Browser) advertised-name-2: INet~Services (IIS) advertised-name-3: IS~ NT4ent6 (IIS) advertised-name-4: NT4ent6 (File Server Service) advertised-name-5: WORKGROUP (Domain Name) advertised-name-6: NT4ent6 (Logged-on User) advertised-name-7: WORKGROUP (Browser Service Elections) advertised-name-8: ADMINISTRATOR (Logged-on User) advertised-name-9: WORKGROUP (Master Browser) mac-address: 000C29018E21 DCE RPC interface-uuid: 82AD4280-036B-11CF-972C-00AA006887B0 interface-version: 2 name: 82AD4280-036B-11CF-972C-00AA006887B0 protocol-sequence: ncacn_ip_tcp:172.23.202.101[1028] FTP: 172.23.202.101 tcp 21 HTTP: 172.23.202.101 tcp 80 GOPHER⁷²⁶ : 172.23.202.101 tcp 70
Korisnička imena i grupe	Administrator, type User (Built-in account), user-id: 500 Administrators, type Group, group-id: 544 Backup Operators, type Group, group-id: 551 Guest, type User (Built-in account), user-id: 501 Guest, type Group (Built-in account), group-id: 546 IUSR_ NT4ent6, type User (Internet Server Anonymous Access) , user-id: 1000 None, type Group, group-id: 513 Power Users Group group-id: 547 Replicator Group group-id: 552 TsInternetUser, type User (nalog za Terminal Services),user-id: 1000 Users, type Group, group-id: 545
Spidered sites	http://172.23.202.101:80 Common Default URLs The following URLs were guessed. They are often included with default web server or web server add-on installations. Access Error (403) scripts Successful (200) Samples Guessed URLs The following URLs were guessed using various tricks based on the

⁷²⁴ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

⁷²⁵ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

⁷²⁶ The Gopher servis obezbeđuje sistem za povraćaj dokumenata distribuiranih preko mreže. Ovaj servis omogućava korisnicima da pretražuju (brauzuju) i vraćaju informacije, moguće čak i sa različitih hostova, koji su predstavljeni kao da potiču sa istog izvora. Korisniku Gopher server se ova informacija pojavljuje kao set menija. Ovi meniji mogu bilo da vode do nekog specifičnog sadržaja (npr. tekstualni fajl, binarni podaci, slike itd) ili do još specifičnijeg seta pod-menija. Struktura i namena Gopher-a je vrlo slična mnogo popularnijem World Wide Web-u i često se navodi kao prethodnik Web-u. A Gopher server sadrži informacije i prikazuje te informacije Gopher-ovim klijentima na zahtev. Gopher serveri takođe mogu da obezbede prolaz ka drugim serverima (npr. Telnet, FTP), drugim sistemima za povraćaj informacija (WWW, whois) ili drugim gopher serverima (Gopherspace).

	discovered web site content. <i>Access Error (403)</i> samples dbsamp gbook htmlsamp images ?P=+ADw-script+AD4-alert(42)+ADwscript+ AD4- script+AD4- script+AD4- isapi scripts scripts %3f.jsp .svn entries ADw-script AD4-alert(42) ADwscript AD4- CVS Entries Root DEADJOE Trace.axd WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc iisadmin %23adojavas.inc%23 %23adovbs.inc%23 %3f.jsp %3f.jsp%00 %3f.jsp%5C .svn entries ADw-script AD4-alert(42) ADwscript AD4- CVS Entries Root DEADJOE Trace.axd WS_FTP.LOG Web.sitemap adojavas.inc adojavas.inc.bak adojavas.inc.old adojavas.inc.tmp adojavas.inc~ adovbs.inc adovbs.inc.bak adovbs.inc.old adovbs.inc.tmp adovbs.inc~ web.config samples tools web.config <i>Error (400)</i> %3f.jsp %3f.jsp%00 %3f.jsp%5C iisadmin %3f.jsp %3f.jsp%00 %3f.jsp%5C htmldocs

	%3f.jsp %3f.jsp%00 %3f.jsp%5C samples %3f.jsp IMAGES h_samp.map images %3f.jsp %3f.jsp%00 %3f.jsp%5C <i>Successful (200)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-script+AD4-script+AD4-default.htm iisadmin htmldocs default.htm samples dbsamp dbsamp.htm htmlsamp htmlsamp.htm isapi isapi.htm sampsite sampsite.htm Linked URLs The following URLs were found as links in the content of other web pages. <i>Error (400)</i> scripts samples favlist.dll <i>Requires Authentication (401)</i> scripts iisadmin ism.dll?http serv <i>Successful (200)</i> iisadmin default.htm htmldocs 00_iis.htm 01_iis.htm 02_iis.htm 03_iis.htm 04_iis.htm 05_iis.htm 06_iis.htm 07_iis.htm 08_iis.htm 09_iis.htm 10_iis.htm 11_iis.htm aa_iis.htm befr_iis.htm iisdocs.HTM inetdocs.htm ix_iis.htm zz_iis.htm samples IMAGES db_mh.map h_samp.map

	html_mh.map mh_data.map mh_html.map mh_prog.map mh_sampl.map p_mh.map dbsamp dbsamp1.htm default.htm disclaim.htm gbook query.htm register.htm htmlsamp styles.htm styles2.htm tables.htm isapi drop.htm sampsite catalog.htm default.htm process.htm results.htm taste.htm ctguestb.idc query.idc register.idc sample.idc sample2.idc sample3.idc viewbook.idc volresp.dll scripts

Tabela 17. Windows OS sa IP adresama 172.23.202.112, 172.23.202.72, 172.23.202.71, 172.23.202.70 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.112		OS: Microsoft Windows 2003 Enterprise server x86 SP2, WIN2003ENSP2x86			9
IP adresa: 172.23.202.72		OS: Windows Server 2003 Enterprise x64 SP2, WIN2003ENSP2x64			9
IP adresa: 172.23.202.71		OS: Windows server 2003 Standard x86 SP2, WIN2003StX86sp2			9
IP adresa: 172.23.202.70		OS: Windows server 2003 Standard x64 SP2, WIN2003StX64sp2			9
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (windows-hotfix-ms08-	172.23.202.112:139 172.23.202.112:445 172.23.202.72:139 172.23.202.72:445 172.23.202.71:139 172.23.202.71:445 172.23.202.70:139	MS: MS08-067 ⁷²⁷ MSKB: 958644 ⁷²⁸ CVE: CVE-2008-4250 ⁷²⁹ SECUNIA: 32326 ⁷³⁰ URL1 ⁷³¹ URL2 ⁷³² URL3 ⁷³³	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003-KB958644-x86-ENU.exe (702840 bytes) ⁷³⁴ , a za 64-bitnu verziju

⁷²⁷ <http://technet.microsoft.com/en-us/security/bulletin/ms08-067>

⁷²⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958644>

⁷²⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4250>

⁷³⁰ <http://secunia.com/advisories/32326/>

⁷³¹ blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx

⁷³² <http://blogs.msdn.com/b/sdl/archive/2008/10/22/ms08-067.aspx>

	067)	172.23.202.70:445 Ova bezbednosna ispravka rešava ranjivost koja je prijavljena od strane privatnog lica. Ranjivost bi mogla da omogući daljinsko izvršavanje koda ukoliko je napadnuti sistem primio posebno opremljeni RPC zahtev. Na sistemima Microsoft Windows 2000, Windows XP, i Windows Server 2003, napadač bi mogao da iskoristi ovu ranjivost bez overavanja autentičnosti i da pokrene proizvoljan kôd. Moguće je da ova ranjivost može biti upotrebljena za intenziviranje skrivenog korišćenja. Najbolje prakse zaštitnog zida i standardne konfiguracije zaštitnog zida po difoltu mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan okvira preduzeća.			WindowsServer2003.WindowsXP-KB958644-x64-ENU.exe ⁷³⁵
2.	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (windows-hotfix-ms09-001)	172.23.202.112:139 172.23.202.112:445 172.23.202.72:139 172.23.202.72:445 172.23.202.71:139 172.23.202.71:445 172.23.202.70:139 172.23.202.70:445 Ovo ažuriranje bezbednosti rešava nekoliko privatno prijavljenih ranjivosti, a odnosi se na protokol Microsoft Server Message Block-a (SMB). Ove ranjivosti bi mogle da omoguće izvršenje udaljenog kôda na napadnutim sistemima. Napadač koji bi uspešno iskoristio ove ranjivosti mogao bi da instalira programe, pregleda, menja ili briše podatke ili pak da kreira nove naloge sa punim pravima korisnika. Dosadašnja praksa fajervola i standardne fajervol difolt konfiguracije mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan organizacije. Za sisteme koji su stalno povezani na Internet preporuka je da imaju što manji broj izloženih portova.	MS: MS09-001 ⁷³⁶ MSKB: 958687 ⁷³⁷ CVE: CVE-2008-4114 ⁷³⁸ CVE: CVE-2008-4835 ⁷³⁹ CVE: CVE-2008-4834 ⁷⁴⁰ SECUNIA: 31883 ⁷⁴¹ URL1 ⁷⁴² URL2 ⁷⁴³ URL3 ⁷⁴⁴	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003-KB958687-x86-ENU.exe (736632 bytes) ⁷⁴⁵ , a za 64-bitnu verziju WindowsServer2003.WindowsXP-KB958687-x64-ENU.exe ⁷⁴⁶

⁷³³ <http://blogs.technet.com/b/msrc/archive/2008/10/23/ms08-067-released.aspx>⁷³⁴ download.windowsupdate.com/msdownload/update/software/secu/2008/10/windowsserver2003-kb958644-x86-enu_af4987620549ae4174e45ec5aa872f4a352f34c1.exe⁷³⁵ <http://download.microsoft.com/download/f/7/6/f761e8ee-caad-4528-aa47-ed5d744be523/WindowsServer2003.WindowsXP-KB958644-x64-ENU.exe>⁷³⁶ <http://technet.microsoft.com/en-us/security/bulletin/MS09-001>⁷³⁷ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958687>⁷³⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4114>⁷³⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4835>⁷⁴⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4834>⁷⁴¹ <http://secunia.com/advisories/31883/>⁷⁴² http://www.vallejo.cc/proyectos/vista_SMB_write_DoS.htm⁷⁴³ <http://www.zerodayinitiative.com/advisories/ZDI-09-001/>⁷⁴⁴ <http://www.zerodayinitiative.com/advisories/ZDI-09-002/>⁷⁴⁵ download.windowsupdate.com/msdownload/update/software/secu/2008/12/windowsserver2003-kb958687-x86-enu_7769ec8bf8869acd01fb8f9f63d79c23afbad5c6.exe⁷⁴⁶ <http://download.microsoft.com/download/3/4/D/34D5EF31-2729-4050-AB12-EE90C31E1461/WindowsServer2003.WindowsXP-KB958687-x64-ENU.exe>

3.	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-012)	172.23.202.112:139 172.23.202.112:445 172.23.202.72:139 172.23.202.72:445 172.23.202.71:139 172.23.202.71:445 172.23.202.70:139 172.23.202.70:445 Ovo ažuriranje bezbednosti rešava nekoliko privatno prijavljenih ranjivosti na Microsoft Windows-u. Opasnost od ove ranjivosti leži u tome što bi ona omogućila daljinsko izvršavanje kôda ukoliko bi napadač kreirao posebno opremljen SMB paket i poslao ga ugroženom sistemu. Dosadašnja praksa fajervola i standardne fajervol difolt konfiguracije mogu da pomognu u zaštiti mrežnih resursa od napada (koji bi pokušali da iskoriste ove ranjivosti), a koji potiču izvan okvira organizacije.	MS: MS10-012 ⁷⁴⁷ MSKB - 971468 ⁷⁴⁸ CVE: CVE-2010-0020 ⁷⁴⁹ CVE: CVE-2010-0021 ⁷⁵⁰ CVE: CVE-2010-0022 ⁷⁵¹ CVE CVE-2010-0231 ⁷⁵² SECUNIA 38510 ⁷⁵³	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003-KB971468-x86-ENU.exe (681856 bytes) ⁷⁵⁴ , a za 64-bitnu verziju WindowsServer2003.WindowsXP-KB971468-x64-ENU.exe ⁷⁵⁵
4.	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-054)	172.23.202.112:139 172.23.202.112:445 172.23.202.72:139 172.23.202.72:445 172.23.202.71:139 172.23.202.71:445 172.23.202.70:139 172.23.202.70:445 Opis je isti kao kod ranjivosti MS10-012	CVE: CVE-2010-2550 ⁷⁵⁶ CVE: CVE-2010-2551 ⁷⁵⁷ CVE: CVE-2010-2552 ⁷⁵⁸ MS: MS10-054 ⁷⁵⁹ MSKB 982214 ⁷⁶⁰	Kritičan	Uraditi download a zatim instalirati Microsoft patch windowsserver2003-kb982214-x86-enu.exe (682880 bytes) ⁷⁶¹ , a za 64-bitnu verziju WindowsServer2003.WindowsXP-KB982214-x64-ENU.exe ⁷⁶²
5.	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms11-020)	172.23.202.112:139 172.23.202.112:445 172.23.202.72:139 172.23.202.72:445 172.23.202.71:139 172.23.202.71:445 172.23.202.70:139 172.23.202.70:445 Opis je isti kao kod ranjivosti MS10-	CVE CVE-2011-0661 ⁷⁶³ MS: MS11-020 ⁷⁶⁴ MSKB: 2508429 ⁷⁶⁵	Kritičan	Uraditi download a zatim instalirati Microsoft patch windowsserver2003-kb2508429-x86-enu.exe (693120 bytes) ⁷⁶⁶ , a za 64-bitnu verziju WindowsServer2003.Wind

⁷⁴⁷ <http://technet.microsoft.com/en-us/security/bulletin/MS10-012>⁷⁴⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;971468>⁷⁴⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0020>⁷⁵⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0021>⁷⁵¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0022>⁷⁵² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0231>⁷⁵³ <http://secunia.com/advisories/38510/>⁷⁵⁴ download.windowsupdate.com/msdownload/update/software/secu/2010/01/windowsserver2003-kb971468-x86-enu_b6dcb60d113c4affd98b5bae0dfd1f5a785ae64d.exe⁷⁵⁵ <http://download.microsoft.com/download/1/4/3/1438049D-7D9B-4694-860E-3E99BF9839A5/WindowsServer2003.WindowsXP-KB971468-x64-ENU.exe>⁷⁵⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2550>⁷⁵⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2551>⁷⁵⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2552>⁷⁵⁹ <http://technet.microsoft.com/en-us/security/bulletin/MS10-054>⁷⁶⁰ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;982214>⁷⁶¹ download.windowsupdate.com/msdownload/update/software/secu/2010/07/windowsserver2003-kb982214-x86-enu_40e37ace02116c2baf27c14c7e3d1883887707e6.exe⁷⁶² <http://download.microsoft.com/download/1/E/2/1E2C6AD3-11CC-448F-BF23-42A32252CCDF/WindowsServer2003.WindowsXP-KB982214-x64-ENU.exe>⁷⁶³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661>⁷⁶⁴ <http://technet.microsoft.com/en-us/security/bulletin/ms11-020>⁷⁶⁵ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;2508429>⁷⁶⁶ download.windowsupdate.com/msdownload/update/software/secu/2011/03/windowsserver2003-kb2508429-x86-enu_1d4ff4ef7163f06d580e7fbc94cc222bafd0733f.exe

		012			owsXP-KB2508429-x64-ENU.exe ⁷⁶⁷
6.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.112:139 172.23.202.112:445 172.23.202.72:139 172.23.202.72:445 172.23.202.71:139 172.23.202.71:445 172.23.202.70:139 172.23.202.70:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje omogućava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB: 887429 ⁷⁶⁸ URL1 ⁷⁶⁹	Ozbiljan	Metoda za konfiguracije SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429. ⁷⁷⁰ Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing</i> = <i>auto</i> ili da se zahteva SMB potpisivanje: <i>server signing</i> = <i>mandatory</i> .
7.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.112:139 172.23.202.112:445 172.23.202.72:139 172.23.202.72:445 172.23.202.71:139 172.23.202.71:445 172.23.202.70:139 172.23.202.70:445 Sistem omogućava ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti
8.	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server. Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko RPC funkcionalnih poziva. Ovi servisi su i u prošlosti bili skloni ranjivostima. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinejnije napade.	BID: 494 ⁷⁷¹ CVE: CVE-1999-0519 ⁷⁷² MSKB: 143474 ⁷⁷³ URL1 ⁷⁷⁴	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost
9.	ICMP timestamp response (generic-icmp-)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat.	OSVDB 95 ⁷⁷⁵ CVE: CVE-1999-0524 ⁷⁷⁶	Umeren	Onemogućavanje ICMP timestamps odgovora vrši

⁷⁶⁷ <http://download.microsoft.com/download/8/3/3/833C20D2-59EA-4D23-960F-11270C0C0319/WindowsServer2003.WindowsXP-KB2508429-x64-ENU.exe>

⁷⁶⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429>

⁷⁶⁹ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>

⁷⁷⁰ <http://support.microsoft.com/kb/887429>

⁷⁷¹ <http://www.securityfocus.com/bid/494>

⁷⁷² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>

⁷⁷³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>

⁷⁷⁴ http://www.hsc.fr/ressources/presentations/null_sessions/

⁷⁷⁵ <http://www.osvdb.org/95>

⁷⁷⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>

timestamp)	Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	XF: netmask(306) ⁷⁷⁷ XF: timestamp(322) ⁷⁷⁸	icmp- icmp-	se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.

Tabela 18. Windows OS – Pronađeni servisi na IP adresi 172.23.202.112 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni deljeni resurs, mount-point: C:\
SERVISI	CIFS ⁷⁷⁹ , CIFS Name Service ⁷⁸⁰ : advertised-name-1: WIN2003ENSP2x86 (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: WIN2003ENSP2x86 (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 000C29D694EB DCE RPC interface-uuid: 99945778-1234-ABCD-EF00-0123456789AC interface-version: 1 name: 99945778-1234-ABCD-EF00-0123456789AC protocol-sequence: ncacn_ip_tcp:172.23.202.112[1025]

Tabela 19. Windows OS – Pronađeni servisi na IP adresi 172.23.202.72 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni deljeni resurs, mount-point: C:\
SERVISI	CIFS ⁷⁸¹ , CIFS Name Service ⁷⁸² : advertised-name-1: WIN2003ENSP2x64 (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: WIN2003ENSP2x64 (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 444C29D664EA DCE RPC

⁷⁷⁷ <http://xforce.iss.net/xforce/xfdb/306>⁷⁷⁸ <http://xforce.iss.net/xforce/xfdb/322>⁷⁷⁹ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).⁷⁸⁰ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.⁷⁸¹ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).⁷⁸² Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	interface-uuid: 55555778-1234-ABCD-EF00-777756789AC interface-version: 1 name: 55555778-1234-ABCD-EF00-777756789AC protocol-sequence: ncacn_ip_tcp:172.23.202.72[1025]

Tabela 20. Windows OS – Pronađeni servisi na IP adresi 172.23.202.71 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni deljeni resurs, mount-point: C:\
SERVISI	CIFS⁷⁸³ , CIFS Name Service⁷⁸⁴ : advertised-name-1: WIN2003StX86sp2 (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: WIN2003StX86sp2 (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 123C29D555AB DCE RPC interface-uuid: 23455778-2222-DDDD-EF00-0123456789AB interface-version: 1 name: 12345778-2222-DDDD-EF00-0123456789AB protocol-sequence: ncacn_ip_tcp:172.23.202.71[1025]
Korisnička imena i grupe	

Tabela 21. Windows OS – Pronađeni servisi na IP adresi 172.23.202.70 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni deljeni resurs, mount-point: C:\
SERVISI	CIFS⁷⁸⁵ , CIFS Name Service⁷⁸⁶ : advertised-name-1: WIN2003StX64sp2 (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: WIN2003StX64sp2 (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 000B89D999CB DCE RPC interface-uuid: 88888878-5555-AACD-EF00-0123456789AD interface-version: 1 name: 88888878-5555-AACD-EF00-0123456789AD

⁷⁸³ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

⁷⁸⁴ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

⁷⁸⁵ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

⁷⁸⁶ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	protocol-sequence: ncacn_ip_tcp:172.23.202.70[1025]
Korisnička imena i grupe	

Tabela 22. Windows OS sa IP adresama 172.23.202.113, 172.23.202.89, 172.23.202.88, 172.23.202.87, 172.23.202.86, 172.23.202.85, 172.23.202.84, 172.23.202.83 (2011. godina)

OS: Microsoft Windows Vista ultimate x86		IP ADRESA : 172.23.202.190		Datum: .2011	
Datum: 20.08.2011		Operativni sistem i ime računara		Broj ranjivosti	
IP adresa: 172.23.202.113		OS: : Windows Vista ultimate x86, VISTAx86ULT		8	
IP adresa: 172.23.202.89		OS: Windows Vista Home Basic x86, VISTAx86HoBa		8	
IP adresa: 172.23.202.88		OS: Windows Vista Home Basic x64, VISTAx64HoBa		8	
IP adresa: 172.23.202.87		OS: Windows Vista Home Premium x86, VISTAx86HoPre		8	
IP adresa: 172.23.202.86		OS: Windows Vista Home Premium x64, VISTAx64HoPre		8	
IP adresa: 172.23.202.85		OS: Windows Vista Business x86, VISTAx86Bsn		8	
IP adresa: 172.23.202.84		OS: Windows Vista Business x64, VISTAx64Bsn		8	
IP adresa: 172.23.202.83		OS: Windows Vista Ultimate x64, VISTAx64ULT		8	
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (windows-hotfix-ms09-001)	172.23.202.113:139 172.23.202.113:445 172.23.202.89:139 172.23.202.89:445 172.23.202.88:139 172.23.202.88:445 172.23.202.87:139 172.23.202.87:445 172.23.202.86:139 172.23.202.86:445 172.23.202.85:139 172.23.202.85:445 172.23.202.84:139 172.23.202.84:445 172.23.202.83:139 172.23.202.83:445 Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti koje su privatno prijavljene, a odnose se na protokol	MS: MS09-001 ⁷⁸⁷ MSKB: 958687 ⁷⁸⁸ CVE: CVE-2008-4114 ⁷⁸⁹ CVE: CVE-2008-4835 ⁷⁹⁰ CVE: CVE-2008-4834 ⁷⁹¹ SECUNIA: 31883 ⁷⁹² URL1 ⁷⁹³ URL2 ⁷⁹⁴ URL3 ⁷⁹⁵	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows6.0-KB958687- x86.cab (216319 bytes) ⁷⁹⁶ , ili za 64-bitnu verziju Windows6.0-KB958687- x64.msu ⁷⁹⁷

⁷⁸⁷ <http://technet.microsoft.com/en-us/security/bulletin/MS09-001>

⁷⁸⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958687>

⁷⁸⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4114>

⁷⁹⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4835>

⁷⁹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4834>

⁷⁹² <http://secunia.com/advisories/31883/>

⁷⁹³ http://www.vallejo.cc/proyectos/vista_SMB_write_DoS.htm

⁷⁹⁴ <http://www.zerodayinitiative.com/advisories/ZDI-09-001/>

⁷⁹⁵ <http://www.zerodayinitiative.com/advisories/ZDI-09-002/>

⁷⁹⁶ download.windowsupdate.com/msdownload/update/software/secu/2008/12/windows6.0-kb958687-x86_48df8df9513e517d7db0a4a75ed2b260c5b7acbf.cab

⁷⁹⁷ <http://download.microsoft.com/download/7/5/9/759DF890-E7DB-471C-B52A-E03712BBD616/Windows6.0-KB958687-x64.msu>

		Microsoft Server Message Block-a (SMB). Ranjivosti mogu da omoguće daljinsko izvršenje kôda na ugroženim sistemima. Napadač koji je uspešno iskoristio ove ranjivosti može da instalira programe, pregleda, menja ili briše podatke ili otvara nove naloge sa potpunim korisničkim pravima. Najbolje prakse zaštitnog zida i standardne konfiguracije zaštitnog zida po difoltu mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan okvira preduzeća. Za sisteme koji su stalno povezani na Internet preporuka je da imaju što manji broj izloženih portova.			
2.	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-012)	172.23.202.113:139 172.23.202.113:445 172.23.202.89:139 172.23.202.89:445 172.23.202.88:139 172.23.202.88:445 172.23.202.87:139 172.23.202.87:445 172.23.202.86:139 172.23.202.86:445 172.23.202.85:139 172.23.202.85:445 172.23.202.84:139 172.23.202.84:445 172.23.202.83:139 172.23.202.83:445 Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti koje su privatno prijavljene u Microsoft Windows-u. Opasnost od ove ranjivosti leži u tome što bi ona omogućila daljinsko izvršavanje kôda ukoliko bi napadač kreirao posebno opremljen SMB paket i poslao ga ugroženom sistemu. Praksa je pokazala da upotreba zaštitnog zida može da pomogne u zaštiti mrežnih resursa od napada (koji bi pokušali da iskoriste ove ranjivosti), a koji potiču izvan okvira organizacije.	MS: MS10-012 ⁷⁹⁸ MSKB - 971468 ⁷⁹⁹ CVE: CVE-2010-0020 ⁸⁰⁰ CVE: CVE-2010-0021 ⁸⁰¹ CVE: CVE-2010-0022 ⁸⁰² CVE CVE-2010-0231 ⁸⁰³ SECUNIA 38510 ⁸⁰⁴	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows6.0-KB971468-x86.cab (319207 bytes) ⁸⁰⁵ , ili za 64-bitnu verziju Windows6.0-KB971468-x64.msu ⁸⁰⁶
3.	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution	172.23.202.113:139 172.23.202.113:445 172.23.202.89:139 172.23.202.89:445 172.23.202.88:139	CVE: CVE-2010-2550 ⁸⁰⁷ CVE: CVE-2010-2551 ⁸⁰⁸ CVE: CVE-2010-2552 ⁸⁰⁹ MS: MS10-054 ⁸¹⁰ MSKB 982214 ⁸¹¹	Kritičan	Uraditi download a zatim instalirati Microsoft patch windows6.0-kb982214-x86.cab (325694 bytes) ⁸¹² ,

⁷⁹⁸ <http://technet.microsoft.com/en-us/security/bulletin/MS10-012>⁷⁹⁹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;971468>⁸⁰⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0020>⁸⁰¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0021>⁸⁰² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0022>⁸⁰³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0231>⁸⁰⁴ <http://secunia.com/advisories/38510/>⁸⁰⁵ [download.windowsupdate.com/msdownload/update/software/secu/2010/01/windows6.0-kb971468-](http://download.windowsupdate.com/msdownload/update/software/secu/2010/01/windows6.0-kb971468-x86_673ca9ff1fae6a26038f2e8764d07033c451de06.cab)⁸⁰⁶ [x86_673ca9ff1fae6a26038f2e8764d07033c451de06.cab](http://download.microsoft.com/download/8/D/7/8D7713E1-543D-434E-B80B-48495CC2244B/Windows6.0-KB971468-x64.msu)⁸⁰⁷ <http://download.microsoft.com/download/8/D/7/8D7713E1-543D-434E-B80B-48495CC2244B/Windows6.0-KB971468-x64.msu>⁸⁰⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2550>⁸⁰⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2551>⁸¹⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2552>⁸¹¹ <http://technet.microsoft.com/en-us/security/bulletin/MS10-054>⁸¹² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;982214>

	(windows-hotfix-ms10-054)	172.23.202.88:445 172.23.202.87:139 172.23.202.87:445 172.23.202.86:139 172.23.202.86:445 172.23.202.85:139 172.23.202.85:445 172.23.202.84:139 172.23.202.84:445 172.23.202.83:139 172.23.202.83:445 Opis je isti kao kod ranjivosti MS10-012			ili za 64-bitnu verziju Windows6.0-KB982214-x64.msu ⁸¹³
4.	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms11-020)	172.23.202.113:139 172.23.202.113:445 172.23.202.89:139 172.23.202.89:445 172.23.202.88:139 172.23.202.88:445 172.23.202.87:139 172.23.202.87:445 172.23.202.86:139 172.23.202.86:445 172.23.202.85:139 172.23.202.85:445 172.23.202.84:139 172.23.202.84:445 172.23.202.83:139 172.23.202.83:445 Opis je isti kao kod ranjivosti MS10-012	CVE CVE-2011-0661 ⁸¹⁴ MS: MS11-020 ⁸¹⁵ MSKB: 2508429 ⁸¹⁶	Kritičan	Uraditi download a zatim instalirati Microsoft patch windows6.0-kb2508429-x86.cab (332927 bytes) ⁸¹⁷ ili za 64-bitnu verziju Windows6.0-KB2508429-x64.msu ⁸¹⁸
5.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.113:139 172.23.202.113:445 172.23.202.89:139 172.23.202.89:445 172.23.202.88:139 172.23.202.88:445 172.23.202.87:139 172.23.202.87:445 172.23.202.86:139 172.23.202.86:445 172.23.202.85:139 172.23.202.85:445 172.23.202.84:139 172.23.202.84:445 172.23.202.83:139 172.23.202.83:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje	MSKB: 887429 ⁸¹⁹ URL1 ⁸²⁰	Ozbiljan	Metoda za konfiguracije SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429 . ⁸²¹ Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing</i> = <i>auto</i> ili da se zahteva SMB potpisivanje: <i>server signing</i> = <i>mandatory</i> .

⁸¹² [download.windowsupdate.com/msdownload/update/software/secu/2010/07/windows6.0-kb982214-](http://download.windowsupdate.com/msdownload/update/software/secu/2010/07/windows6.0-kb982214-x86_50d77476159fef060a2470a0f66e7e8ecb9808ea.cab)[x86_50d77476159fef060a2470a0f66e7e8ecb9808ea.cab](http://download.microsoft.com/download/5/8/D/58D3BE5D-9C2F-45DB-84C0-638AC2BEF57D/Windows6.0-KB982214-x64.msu)⁸¹³ <http://download.microsoft.com/download/5/8/D/58D3BE5D-9C2F-45DB-84C0-638AC2BEF57D/Windows6.0-KB982214-x64.msu>⁸¹⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661>⁸¹⁵ <http://technet.microsoft.com/en-us/security/bulletin/ms11-020>⁸¹⁶ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;2508429>⁸¹⁷ [download.windowsupdate.com/msdownload/update/software/secu/2011/03/windows6.0-kb2508429-](http://download.windowsupdate.com/msdownload/update/software/secu/2011/03/windows6.0-kb2508429-x86_2e7adf8e8e545432372edbd59952a925fb7a69da.cab)[x86_2e7adf8e8e545432372edbd59952a925fb7a69da.cab](http://download.microsoft.com/download/2/1/8/218341B5-0F6A-4359-8929-27D166C98031/Windows6.0-KB2508429-x64.msu)⁸¹⁸ <http://download.microsoft.com/download/2/1/8/218341B5-0F6A-4359-8929-27D166C98031/Windows6.0-KB2508429-x64.msu>⁸¹⁹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429>⁸²⁰ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>⁸²¹ <http://support.microsoft.com/kb/887429>

		može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).			
6.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.113:139 172.23.202.113:445 172.23.202.89:139 172.23.202.89:445 172.23.202.88:139 172.23.202.88:445 172.23.202.87:139 172.23.202.87:445 172.23.202.86:139 172.23.202.86:445 172.23.202.85:139 172.23.202.85:445 172.23.202.84:139 172.23.202.84:445 172.23.202.83:139 172.23.202.83:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti
7.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-ov zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatišu slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	OSVDB 95 ⁸²² CVE: CVE-1999-0524 ⁸²³ XF: icmp-netmask(306) ⁸²⁴ XF: icmp-timestamp(322) ⁸²⁵	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
8.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1 ⁸²⁶ URL2 ⁸²⁷ URL3 ⁸²⁸	Umeren	Onemogućavanje TCP timestamp odgovora na Windows OS. Podesiti Tcp1323Opts vrednost na sledećem ključu na 1: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

Tabela 23. Windows OS – Pronađeni servisi na IP adresi 172.23.202.113 (2011. godina)

SERVISI	CIFS ⁸²⁹ , CIFS Name Service ⁸³⁰ :

⁸²² <http://www.osvdb.org/95>⁸²³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁸²⁴ <http://xforce.iss.net/xforce/xfdb/306>⁸²⁵ <http://xforce.iss.net/xforce/xfdb/322>⁸²⁶ http://www.forensicswiki.org/wiki/TCP_timestamps⁸²⁷ <http://www.ietf.org/rfc/rfc1323.txt>⁸²⁸ <http://uptime.netcraft.com/>⁸²⁹ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).⁸³⁰ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	advertised-name-1: VISTAx86ULT (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: VISTAx86ULT (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) advertised-name-5: WORKGROUP (Master Browser) advertised-name-6: __MSBROWSE__ (Master Browser) mac-address: 000C29E3119B DCE RPC interface-uuid: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D interface-version: 1 name: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D object-interface-uuid: 765294BA-60BC-48B8-92E9-89FD77769D91 protocol-sequence: ncacn_ip_tcp:172.23.202.113[49152] interface-uuid: 06BBA54A-BE05-49F9-B0A0-30F790261023 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.113[49153] interface-uuid: 3473DD4D-2E88-4006-9CBA-22570909DD10 interface-version: 5 name: WinHttp Auto-Proxy Service protocol-sequence: ncacn_ip_tcp:172.23.202.113[49154] interface-uuid: FD7A0523-DC70-43DD-9B2E-9C5ED48225B1 interface-version: 1 name: AppInfo protocol-sequence: ncacn_ip_tcp:172.23.202.113[49155] interface-uuid: 12345778-1234-ABCD-EF00-0123456789AC interface-version: 1 name: 12345778-1234-ABCD-EF00-0123456789AC protocol-sequence: ncacn_ip_tcp:172.23.202.113[49156] interface-uuid: 367ABB81-9844-35F1-AD32-98F038001003 interface-version: 2 name: 367ABB81-9844-35F1-AD32-98F038001003 protocol-sequence: ncacn_ip_tcp:172.23.202.113[49157]

Tabela 24. Windows OS – Pronađeni servisi na IP adresi 172.23.202.89 (2011. godina)

SERVISI	CIFS⁸³¹, CIFS Name Service⁸³² : advertised-name-1: VISTAx86HoBa (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: VISTAx86HoBa (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) advertised-name-5: WORKGROUP (Master Browser) advertised-name-6: __MSBROWSE__ (Master Browser) mac-address: 333B29E3119B DCE RPC interface-uuid: D95ABA60-A6D5-4259-822E-2C84DA1DDB1A

⁸³¹ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

⁸³² Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	interface-version: 1 name: D95ABA60-A6D5-4259-822E-2C84DA1DDB1A object-interface-uuid: 888294BA-60BC-48B8-92E9-89FD77769D91 protocol-sequence: ncacn_ip_tcp:172.23.202.89[49152] interface-uuid: 17AAA54A-BE05-49F9-B0A0-50F790261333 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.89[49153] interface-uuid: 3473AAAA-2E88-4006-9CBA-11111909DD15 interface-version: 5 name: WinHttp Auto-Proxy Service protocol-sequence: ncacn_ip_tcp:172.23.202.89[49154] interface-uuid: B6B7A0523-AC70-42DD-9B2E-8C5ED48225C1 interface-version: 1 name: AppInfo protocol-sequence: ncacn_ip_tcp:172.23.202.89[49155] interface-uuid: 66666678-5555-CCCC-EF00-3213456789BA interface-version: 1 name: 66666678-5555-CCCC-EF00-3213456789BA protocol-sequence: ncacn_ip_tcp:172.23.202.89[49156] interface-uuid: 456ABB81-9844-35F1-BD33-98F038002004 interface-version: 2 name: 456ABB81-9844-35F1-BD33-98F038002004 protocol-sequence: ncacn_ip_tcp:172.23.202.89[49157]

Tabela 25. Windows OS – Pronađeni servisi na IP adresi 172.23.202.88 (2011. godina)

SERVISI	CIFS⁸³³, CIFS Name Service⁸³⁴ : advertised-name-1: VISTAx64HoBa (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: VISTAx64HoBa (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) advertised-name-5: WORKGROUP (Master Browser) advertised-name-6: __MSBROWSE__ (Master Browser) mac-address: 444C30E3129B DCE RPC interface-uuid: D95BBB70-A5D8-4359-832E-2B84DA1AAB0D interface-version: 1 name: D95BBB70-A5D8-4359-832E-2B84DA1AAB0D object-interface-uuid: 986494BA-60BC-24B8-36E9-89FD888691B1 protocol-sequence: ncacn_ip_tcp:172.23.202.88[49152] interface-uuid: 06DDA55A-CE06-49F9-B0B2-30A790231023 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.88[49153] interface-uuid: 3473DA4D-2E88-4096-9CBD-10570909BB22 interface-version: 5

⁸³³ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

⁸³⁴ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	name: WinHttp Auto-Proxy Service protocol-sequence: ncacn_ip_tcp:172.23.202.88[49154] interface-uuid: FB7A0523-DC70-43AA-9B2A-9C5ED48225B1 interface-version: 1 name: AppInfo protocol-sequence: ncacn_ip_tcp:172.23.202.88[49155] interface-uuid: 45689778-3333-B1B1-EF00-0122256789AC interface-version: 1 name: 45689778-3333-B1B1-EF00-0122256789AC protocol-sequence: ncacn_ip_tcp:172.23.202.88[49156] interface-uuid: 567ACC81-9944-35F1-AB32-12F038001004 interface-version: 2 name: 567ACC81-9944-35F1-AB32-12F038001004 protocol-sequence: ncacn_ip_tcp:172.23.202.88[49157]

Tabela 26. Windows OS – Pronađeni servisi na IP adresi 172.23.202.87 (2011. godina)

SERVISI	CIFS⁸³⁵, CIFS Name Service⁸³⁶ : advertised-name-1: VISTAx86HoPre (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: VISTAx86HoPre (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) advertised-name-5: WORKGROUP (Master Browser) advertised-name-6: __MSBROWSE__ (Master Browser) mac-address: AAA229E3229B DCE RPC interface-uuid: A65AFE70-B1D5-4259-822E-2C84DA1AAB01 interface-version: 1 name: A65AFE70-B1D5-4259-822E-2C84DA1AAB01 object-interface-uuid: 777794BA-62BC-46B8-92E8-89FD56568D91 protocol-sequence: ncacn_ip_tcp:172.23.202.87[49152] interface-uuid: 04BBA54A-BE05-59F9-B0A0-20F790261B23 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.87[49153] interface-uuid: 2473BB4D-2E66-4116-9CBA-33570909DD10 interface-version: 5 name: WinHttp Auto-Proxy Service protocol-sequence: ncacn_ip_tcp:172.23.202.87[49154] interface-uuid: FB7A0523-BC70-44AA-9B2E-8C5ED48225B1 interface-version: 1 name: AppInfo protocol-sequence: ncacn_ip_tcp:172.23.202.87[49155] interface-uuid: 91945778-3459-AB1A-EB00-0325458889BC interface-version: 1 name: 91945778-3459-AB1A-EB00-0325458889BC

⁸³⁵ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

⁸³⁶ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	protocol-sequence: ncacn_ip_tcp:172.23.202.87[49156] interface-uuid: 467ABC81-9898-35F4-AD32-66F036001222 interface-version: 2 name: 467ABC81-9898-35F4-AD32-66F036001222 protocol-sequence: ncacn_ip_tcp:172.23.202.87[49157]

Tabela 27. Windows OS – Pronađeni servisi na IP adresi 172.23.202.86 (2011. godina)

SERVISI	CIFS⁸³⁷, CIFS Name Service⁸³⁸ : advertised-name-1: VISTAx64HoPre (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: VISTAx64HoPre (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) advertised-name-5: WORKGROUP (Master Browser) advertised-name-6: __MSBROWSE__ (Master Browser) mac-address: 000B33E3229B DCE RPC interface-uuid: A45ABE70-A2D3-3259-322E-3C84DA1DDB0D interface-version: 1 name: A45ABE70-A2D3-3259-322E-3C84DA1DDB0D object-interface-uuid: 666694BA-58BC-42B8-90E9-90FD45669D92 protocol-sequence: ncacn_ip_tcp:172.23.202.86[49152] interface-uuid: 16BBA52A-AE02-47F9-B1A0-32F790261011 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.86[49153] interface-uuid: 1413DD41-2E18-1006-1CBA-12570909DD10 interface-version: 5 name: WinHttp Auto-Proxy Service protocol-sequence: ncacn_ip_tcp:172.23.202.86[49154] interface-uuid: 2D7A2523-DC72-23DD-2B2E-2C5ED28225B1 interface-version: 1 name: AppInfo protocol-sequence: ncacn_ip_tcp:172.23.202.86[49155] interface-uuid: 22545578-5234-A15D-1F0A-7127456789AB interface-version: 1 name: 22545578-5234-A15D-1F0A-7127456789AB protocol-sequence: ncacn_ip_tcp:172.23.202.86[49156] interface-uuid: 464ABB41-4844-45F1-BD32-48F038001024 interface-version: 2 name: 464ABB41-4844-45F1-BD32-48F038001024 protocol-sequence: ncacn_ip_tcp:172.23.202.86[49157]

⁸³⁷ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

⁸³⁸ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

Tabela 28. Windows OS – Pronađeni servisi na IP adresi 172.23.202.85 (2011. godina)

SERVISI	CIFS⁸³⁹, CIFS Name Service⁸⁴⁰ : advertised-name-1: VISTAx86Bsn (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: VISTAx86Bsn (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) advertised-name-5: WORKGROUP (Master Browser) advertised-name-6: __MSBROWSE__ (Master Browser) mac-address: 000C29E3119B DCE RPC interface-uuid: A85AFE60-16D5-1259-122E-1C84AA1DDB2D interface-version: 1 name: A85AFE60-16D5-1259-122E-1C84AA1DDB2D object-interface-uuid: 865894BA-80BC-88B8-82E9-88FD78769D92 protocol-sequence: ncacn_ip_tcp:172.23.202.85[49152] interface-uuid: 86BCA58A-BE08-89F9-B0A0-80F780261028 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.85[49153] interface-uuid: 5483DD4D-5E87-4206-9CAA-82580989DA10 interface-version: 5 name: WinHttp Auto-Proxy Service protocol-sequence: ncacn_ip_tcp:172.23.202.85[49154] interface-uuid: FA7A0823-BC80-83DD-9B8E-5C5EA48225B1 interface-version: 1 name: AppInfo protocol-sequence: ncacn_ip_tcp:172.23.202.85[49155] interface-uuid: 82845878-8234-8AC6-6F00-4153486589AF interface-version: 1 name: 82845878-8234-8AC6-6F00-4153486589AF protocol-sequence: ncacn_ip_tcp:172.23.202.85[49156] interface-uuid: 967AB981-9894-39F1-BD32-28F038021002 interface-version: 2 name: 967AB981-9894-39F1-BD32-28F038021002 protocol-sequence: ncacn_ip_tcp:172.23.202.85[49157]

Tabela 29. Windows OS – Pronađeni servisi na IP adresi 172.23.202.84 (2011. godina)

SERVISI	CIFS⁸⁴¹, CIFS Name Service⁸⁴² : advertised-name-1: VISTAx64Bsn (Computer Name)

⁸³⁹ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

⁸⁴⁰ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

⁸⁴¹ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

⁸⁴² Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: VISTAx64Bsn (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) advertised-name-5: WORKGROUP (Master Browser) advertised-name-6: __MSBROWSE__ (Master Browser) mac-address: 144C29E2118B DCE RPC interface-uuid: A96AFE60-6AD5-6256-622E-6C84DA1DDB0D interface-version: 1 name: A96AFE60-6AD5-6256-622E-6C84DA1DDB0D object-interface-uuid: 565254BA-50BC-58B8-32E9-59FD75768D92 protocol-sequence: ncacn_ip_tcp:172.23.202.84[49152] interface-uuid: 05BCA64A-CE06-29F8-B5A2-40F780261623 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.84[49153] interface-uuid: 5478DD4a-4A688-6226-6CBA-32570909DD10 interface-version: 5 name: WinHttp Auto-Proxy Service protocol-sequence: ncacn_ip_tcp:172.23.202.84[49154] interface-uuid: FA6A2543-AC80-23DD-2B2E-2C5ED28225B2 interface-version: 1 name: AppInfo protocol-sequence: ncacn_ip_tcp:172.23.202.84[49155] interface-uuid: 42315718-1134-12CD-EF4600-A3C426386432 interface-version: 1 name: 42315718-1134-12CD-EF4600-A3C426386432 protocol-sequence: ncacn_ip_tcp:172.23.202.84[49156] interface-uuid: 257ACB81-3044-32F2-AD38-288F83704223 interface-version: 2 name: 257ACB81-3044-32F2-AD38-288F83704223 protocol-sequence: ncacn_ip_tcp:172.23.202.84[49157]

Tabela 30. Windows OS – Pronađeni servisi na IP adresi 172.23.202.83 (2011. godina)

SERVISI	CIFS⁸⁴³, CIFS Name Service⁸⁴⁴ : advertised-name-1: VISTAx64ULT (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: VISTAx64ULT (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) advertised-name-5: WORKGROUP (Master Browser) advertised-name-6: __MSBROWSE__ (Master Browser) mac-address: 224B252818A DCE RPC interface-uuid: B98AFE80-8AD8-8254-422E-4C84DA2DBB0D

⁸⁴³ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

⁸⁴⁴ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	interface-version: 1 name: B98AFE80-8AD8-8254-422E-4C84DA2DBB0D object-interface-uuid: 464244FA-52BC-68B8-62E6-69FD35738D93 protocol-sequence: ncacn_ip_tcp:172.23.202.83[49152] interface-uuid: 35BCA34A-3E06-39F8-C5A2-30F780261633 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.83[49153] interface-uuid: 2473DD4A-3A688-8226-8CBB-52570309DD32 interface-version: 5 name: WinHttp Auto-Proxy Service protocol-sequence: ncacn_ip_tcp:172.23.202.83[49154] interface-uuid: BA3A2343-FC30-33DD-3B2E-3C5ED24225B4 interface-version: 1 name: AppInfo protocol-sequence: ncacn_ip_tcp:172.23.202.83[49155] interface-uuid: 32313718-3134-32CD-BF4633-A9C496389433 interface-version: 1 name: 32313718-3134-32CD-BF4633-A9C496389433 protocol-sequence: ncacn_ip_tcp:172.23.202.83[49156] interface-uuid: 2356AA81-4044-42F2-CC38-385F83704528 interface-version: 2 name: 2356AA81-4044-42F2-CC38-385F83704528 protocol-sequence: ncacn_ip_tcp:172.23.202.83[49157]

Tabela 31. Windows OS sa IP adresama 172.23.202.114, 172.23.202.82, 172.23.202.81, 172.23.202.80, 172.23.202.79, 172.23.202.78, 172.23.202.77 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.114		OS: : Microsoft Windows Vista ultimate x86 SP2, VISTAx86ULTSP2			7
IP adresa: 172.23.202.82		OS: Windows Vista Home Basic x86 SP2, VISTAx86HoBaSp2			7
IP adresa: 172.23.202.81		OS: Windows Vista Home Basic x64 SP2, VISTAx64HoBaSp2			7
IP adresa: 172.23.202.80		OS: Windows Vista Business x86 SP2, VISTAx86BsnSp2			7
IP adresa: 172.23.202.79		OS: Windows Vista Business x64 SP2, VISTAx64BsnSp2			7
IP adresa: 172.23.202.78		OS: Windows Vista Home Premium x86 SP2, VISTAx86HoPrSp2			7
IP adresa: 172.23.202.77		OS: Windows Vista Home Premium x64 SP2, VISTAx64HoPrSp2			7
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	MS09-050: Vulnerabilities in SMBv2 Could Allow Remote Code Execution (windows-hotfix-ms09-	Ovo ažuriranje bezbednosti rešava jednu javnu i nekoliko ranjivosti koje su privatno prijavljene u protokolu Microsoft Message Block-a 2 (SMBv2). Opasnost od ove ranjivosti leži u tome što bi ona omogućila	MS MS09-050 ⁸⁴⁵ MSKB 975517 ⁸⁴⁶ CVE CVE-2009-2526 ⁸⁴⁷ CVE CVE-2009-2532 ⁸⁴⁸ CVE CVE-2009-3103 ⁸⁴⁹ SECUNIA 36623 ⁸⁵⁰	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows6.0-KB975517-x86.cab (197912 bytes) ⁸⁵² , ili za 64-bitnu verziju

⁸⁴⁵ <http://technet.microsoft.com/en-us/security/bulletin/MS09-050>

⁸⁴⁶ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;975517>

⁸⁴⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2526>

⁸⁴⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2532>

⁸⁴⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3103>

	050)	daljinsko izvršavanje kôda ako napadač pošalje posebno kreiran SMB paket ka kompjuteru koji pokreće servis servera. Najbolje prakse zaštitnog zida i standardne konfiguracije zaštitnog zida po difoltu mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan okvira preduzeća. Za sisteme koji su stalno povezani na Internet preporuka je da imaju što manji broj izloženih portova.	URL ⁸⁵¹		Windows6.0-KB975517-x64.msu ⁸⁵³
2.	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-054)	172.23.202.114:139 172.23.202.114:445 172.23.202.82:139 172.23.202.82:445 172.23.202.81:139 172.23.202.81:445 172.23.202.80:139 172.23.202.80:445 172.23.202.79:139 172.23.202.79:445 172.23.202.78:139 172.23.202.78:445 172.23.202.77:139 172.23.202.77:445 Opis je isti kao kod ranjivosti MS10-012	CVE: CVE-2010-2550 ⁸⁵⁴ CVE: CVE-2010-2551 ⁸⁵⁵ CVE: CVE-2010-2552 ⁸⁵⁶ MS: MS10-054 ⁸⁵⁷ MSKB 982214 ⁸⁵⁸	Kritičan	Uraditi download a zatim instalirati Microsoft patch windows6.0-kb982214-x86.cab (325694 bytes) ⁸⁵⁹ , ili za 64-bitnu verziju Windows6.0-KB982214-x64.msu ⁸⁶⁰
3.	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms11-020)	172.23.202.114:139 172.23.202.114:445 172.23.202.82:139 172.23.202.82:445 172.23.202.81:139 172.23.202.81:445 172.23.202.80:139 172.23.202.80:445 172.23.202.79:139 172.23.202.79:445 172.23.202.78:139 172.23.202.78:445 172.23.202.77:139 172.23.202.77:445 Opis je isti kao kod ranjivosti MS10-012	CVE CVE-2011-0661 ⁸⁶¹ MS: MS11-020 ⁸⁶² MSKB: 2508429 ⁸⁶³	Kritičan	Uraditi download a zatim instalirati Microsoft patch windows6.0-kb2508429-x86.cab (332927 bytes) ⁸⁶⁴ , ili za 64-bitnu verziju Windows6.0-KB2508429-x64.msu ⁸⁶⁵
4.	SMB signing disabled (cifs-smb-signing-	172.23.202.114:139 172.23.202.114:445	MSKB: 887429 ⁸⁶⁶ URL ⁸⁶⁷	Ozbiljan	Metoda za konfiguracijue SMB potpisivanja je

⁸⁵⁰ <http://secunia.com/advisories/36623/>⁸⁵² [download.windowsupdate.com/msdownload/update/software/secu/2009/09/windows6.0-kb975517-](http://download.windowsupdate.com/msdownload/update/software/secu/2009/09/windows6.0-kb975517-x86_dc06eae8a89a24a1f1aa016bf6f0d10e76eca34d.cab)[x86_dc06eae8a89a24a1f1aa016bf6f0d10e76eca34d.cab](http://download.windowsupdate.com/msdownload/update/software/secu/2009/09/windows6.0-kb975517-x86_dc06eae8a89a24a1f1aa016bf6f0d10e76eca34d.cab)⁸⁵¹ <http://g-laurent.blogspot.com/2009/09/windows-vista7-smb20-negotiate-protocol.html>⁸⁵³ <http://download.microsoft.com/download/9/3/F/93F97002-436E-47FF-8D46-725F6150E53E/Windows6.0-KB975517-x64.msu>⁸⁵⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2550>⁸⁵⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2551>⁸⁵⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2552>⁸⁵⁷ <http://technet.microsoft.com/en-us/security/bulletin/MS10-054>⁸⁵⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;982214>⁸⁵⁹ [download.windowsupdate.com/msdownload/update/software/secu/2010/07/windows6.0-kb982214-](http://download.windowsupdate.com/msdownload/update/software/secu/2010/07/windows6.0-kb982214-x86_50d77476159fef060a2470a0f66e7e8ecb9808ea.cab)[x86_50d77476159fef060a2470a0f66e7e8ecb9808ea.cab](http://download.windowsupdate.com/msdownload/update/software/secu/2010/07/windows6.0-kb982214-x86_50d77476159fef060a2470a0f66e7e8ecb9808ea.cab)⁸⁶⁰ <http://download.microsoft.com/download/5/8/D/58D3BE5D-9C2F-45DB-84C0-638AC2BEF57D/Windows6.0-KB982214-x64.msu>⁸⁶¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661>⁸⁶² <http://technet.microsoft.com/en-us/security/bulletin/ms11-020>⁸⁶³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;2508429>⁸⁶⁴ [download.windowsupdate.com/msdownload/update/software/secu/2011/03/windows6.0-kb2508429-](http://download.windowsupdate.com/msdownload/update/software/secu/2011/03/windows6.0-kb2508429-x86_2e7adf8e8e545432372edbd59952a925fb7a69da.cab)[x86_2e7adf8e8e545432372edbd59952a925fb7a69da.cab](http://download.windowsupdate.com/msdownload/update/software/secu/2011/03/windows6.0-kb2508429-x86_2e7adf8e8e545432372edbd59952a925fb7a69da.cab)⁸⁶⁵ <http://download.microsoft.com/download/2/1/8/218341B5-0F6A-4359-8929-27D166C98031/Windows6.0-KB2508429-x64.msu>⁸⁶⁶ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429>

	disabled)	172.23.202.82:139 172.23.202.82:445 172.23.202.81:139 172.23.202.81:445 172.23.202.80:139 172.23.202.80:445 172.23.202.79:139 172.23.202.79:445 172.23.202.78:139 172.23.202.78:445 172.23.202.77:139 172.23.202.77:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).			specifična za svaki sistem i opisana je u KB 887429. ⁸⁶⁸ Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing</i> = <i>auto</i> ili da se zahteva SMB potpisivanje: <i>server signing</i> = <i>mandatory</i> .
5.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.114:139 172.23.202.114:445 172.23.202.82:139 172.23.202.82:445 172.23.202.81:139 172.23.202.81:445 172.23.202.80:139 172.23.202.80:445 172.23.202.79:139 172.23.202.79:445 172.23.202.78:139 172.23.202.78:445 172.23.202.77:139 172.23.202.77:445 This system enables, but does not require SMB signing.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti
6.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-ov zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	OSVDB 95 ⁸⁶⁹ CVE: CVE-1999-0524 ⁸⁷⁰ XF: icmp-netmask(306) ⁸⁷¹ XF: icmp-timestamp(322) ⁸⁷²	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
7.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada	URL1 ⁸⁷³ URL2 ⁸⁷⁴ URL3 ⁸⁷⁵	Umeren	Onemogućavanje TCP timestamp odgovora na Windows OS. Podesiti Tcp1323Opts vrednost na

⁸⁶⁷ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>⁸⁶⁸ <http://support.microsoft.com/kb/887429>⁸⁶⁹ <http://www.osvdb.org/95>⁸⁷⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁸⁷¹ <http://xforce.iss.net/xforce/xfdb/306>⁸⁷² <http://xforce.iss.net/xforce/xfdb/322>⁸⁷³ http://www.forensicswiki.org/wiki/TCP_timestamps⁸⁷⁴ <http://www.ietf.org/rfc/rfc1323.txt>⁸⁷⁵ <http://uptime.netcraft.com/>

		udaljenog hosta (što zlonamerni napadač može iskoristiti pri planiranju daljih napada). Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.			sledećem ključu na 1: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

Tabela 32. Windows OS – Pronađeni servisi na IP adresi 172.23.202.114 (2011. godina)

SERVISI	CIFS⁸⁷⁶, CIFS Name Service⁸⁷⁷ : advertised-name-1: VISTAx86ULTSP2 (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: VISTAx86ULTSP2 (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 000C295A0707 DCE RPC interface-uuid: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D interface-version: 1 name: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D object-interface-uuid: 765294BA-60BC-48B8-92E9-89FD77769D91 protocol-sequence: ncacn_ip_tcp:172.23.202.114[49152] interface-uuid: 06BBA54A-BE05-49F9-B0A0-30F790261023 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.114[49153] interface-uuid: FD7A0523-DC70-43DD-9B2E-9C5ED48225B1 interface-version: 1 name: AppInfo protocol-sequence: ncacn_ip_tcp:172.23.202.114[49154] interface-uuid: 89945778-5234-BBCD-EFE0-7777456789AC interface-version: 1 name: 89945778-5234-BBCD-EFE0-7777456789AC protocol-sequence: ncacn_ip_tcp:172.23.202.114[49155] interface-uuid: 367ABB81-9844-35F1-AD32-98F038001003 interface-version: 2 name: 367ABB81-9844-35F1-AD32-98F038001003 protocol-sequence: ncacn_ip_tcp:172.23.202.114[49156] interface-uuid: 6B5BDD1E-528C-422C-AF8C-A4079BE4FE48 interface-version: 1 name: Remote Fw APIs protocol-sequence: ncacn_ip_tcp:172.23.202.114[49158]

Tabela 33. Windows OS – Pronađeni servisi na IP adresi 172.23.202.82 (2011. godina)

SERVISI	CIFS⁸⁷⁸,

⁸⁷⁶ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

⁸⁷⁷ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	CIFS Name Service⁸⁷⁹ : advertised-name-1: VISTAx86HoBaSp2 (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: VISTAx86HoBaSp2 (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 320C295A0723 DCE RPC interface-uuid: D96AFE60-A3B2-4359-822E-2C84DA1DDB0C interface-version: 1 name: D96AFE60-A3B2-4359-822E-2C84DA1DDB0C object-interface-uuid: 665294BC-70BC-48B8-92E8-99FD77769D92 protocol-sequence: ncacn_ip_tcp:172.23.202.82[49152] iinterface-uuid: 16BBA54B-AE05-49F9-B0A1-20F790261042 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.82[49153] interface-uuid: CC7A0524-DC70-53DD-9B2A-2C5ED48225B9 interface-version: 1 name: AppInfo protocol-sequence: ncacn_ip_tcp:172.23.202.82[49154] interface-uuid: 49965771-2234-ABCD-AFE0-5777456789AA interface-version: 1 name: 49965771-2234-ABCD-AFE0-5777456789AA protocol-sequence: ncacn_ip_tcp:172.23.202.82[49155] interface-uuid: 265ACC81-2844-25F1-BD32-18F038001001 interface-version: 2 name: 265ACC81-2844-25F1-BD32-18F038001001 protocol-sequence: ncacn_ip_tcp:172.23.202.82[49156] interface-uuid: 1B7BDD1A-328C-322C-CF8C-A4079BE4FE22 interface-version: 1 name: Remote Fw APIs protocol-sequence: ncacn_ip_tcp:172.23.202.82[49158]

Tabela 34. Windows OS – Pronađeni servisi na IP adresi 172.23.202.81 (2011. godina)

SERVISI	CIFS⁸⁸⁰, CIFS Name Service⁸⁸¹ : advertised-name-1: VISTAx64HoBaSp2 (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: VISTAx64HoBaSp2 (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 333B295A0706 DCE RPC

⁸⁷⁸ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

⁸⁷⁹ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

⁸⁸⁰ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

⁸⁸¹ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	interface-uuid: A99AFE70-D6D5-9259-222E-7C84BC1AAB0D interface-version: 1 name: A99AFE70-D6D5-9259-222E-7C84BC1AAB0D object-interface-uuid: 763294DA-50BC-58B8-12E9-19FD71769D11 protocol-sequence: ncacn_ip_tcp:172.23.202.81[49152] iiinterface-uuid: 32CCA54A-CE05-89F9-A0A1-10F750261021 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.81[49153] interface-uuid: BC6A1523-AC90-93DD-1B2A-1C2ED38225B1 interface-version: 1 name: AppInfo protocol-sequence: ncacn_ip_tcp:172.23.202.81[49154] interface-uuid: 72925778-2234-DBCD-DFE0-8887456789AA interface-version: 1 name: 72925778-2234-DBCD-DFE0-8887456789AA protocol-sequence: ncacn_ip_tcp:172.23.202.81[49155] interface-uuid: 662AAA81-1834-45F1-5D32-78F038101001 interface-version: 2 name: 662AAA81-1834-45F1-5D32-78F038101001 protocol-sequence: ncacn_ip_tcp:172.23.202.81[49156] interface-uuid: 5C5B6D1E-626C-622B-2F8C-A4079B140120 interface-version: 1 name: Remote Fw APIs protocol-sequence: ncacn_ip_tcp:172.23.202.81[49158]

Tabela 35. Windows OS – Pronađeni servisi na IP adresi 172.23.202.80 (2011. godina)

SERVISI	CIFS⁸⁸², CIFS Name Service⁸⁸³ : advertised-name-1: VISTAx86BsnSp2 (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: VISTAx86BsnSp2 (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 444C495A0701 DCE RPC interface-uuid: A15ACE60-C6D5-7259-722E-1C94D11D2B0D interface-version: 1 name: A15ACE60-C6D5-7259-722E-1C94D11D2B0D object-interface-uuid: 262294CA-20BA-18B8-12E9-29FD72269D92 protocol-sequence: ncacn_ip_tcp:172.23.202.80[49152] iiinterface-uuid: 26AB254A-1E05-39F9-A1A0-70F790221021 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.80[49153] interface-uuid: A4760521-1C70-23DD-3B2E-4C5ED48225B5

⁸⁸² CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

⁸⁸³ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	interface-version: 1 name: AppInfo protocol-sequence: ncacn_ip_tcp:172.23.202.80[49154] interface-uuid: 02945738-5534-ABC7-E1E0-1177456789DD interface-version: 1 name: 02945738-5534-ABC7-E1E0-1177456789DD protocol-sequence: ncacn_ip_tcp:172.23.202.80[49155] interface-uuid: 246A881-2844-95F1-1D32-88F038001099 interface-version: 2 name: 246A881-2844-95F1-1D32-88F038001099 protocol-sequence: ncacn_ip_tcp:172.23.202.80[49156] interface-uuid: 415FDD1E-558C-525C-5F8C-B4079BE4F247 interface-version: 1 name: Remote Fw APIs protocol-sequence: ncacn_ip_tcp:172.23.202.80[49158]

Tabela 36. Windows OS – Pronađeni servisi na IP adresi 172.23.202.79 (2011. godina)

SERVISI	CIFS⁸⁸⁴, CIFS Name Service⁸⁸⁵ : advertised-name-1: VISTAx64BsnSp2 (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: VISTAx64BsnSp2 (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 101C295A0103 DCE RPC interface-uuid: D81AFE10-A4D4-6259-622E-1C84AA1D1B00 interface-version: 1 name: D81AFE10-A4D4-6259-622E-1C84AA1D1B00 object-interface-uuid: 162292BA-40BC-58B8-62E9-79FD78869D98 protocol-sequence: ncacn_ip_tcp:172.23.202.79[49152] iinterface-uuid: 36B1A543-1105-69F9-70A0-90F790261B023 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.79[49153] interface-uuid: A1D7A052-2170-23DD-3B2E-9C5E148225B2 interface-version: 1 name: AppInfo protocol-sequence: ncacn_ip_tcp:172.23.202.79[49154] interface-uuid: 79745778-9234-AACD-1FE0-2727456789A2 interface-version: 1 name: 79745778-9234-AACD-1FE0-2727456789A2 protocol-sequence: ncacn_ip_tcp:172.23.202.79[49155] interface-uuid: 467BBB82-1844-33F1-1D32-98F038011004 interface-version: 2 name: 467BBB82-1844-33F1-1D32-98F038011004 protocol-sequence: ncacn_ip_tcp:172.23.202.79[49156]

⁸⁸⁴ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

⁸⁸⁵ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	interface-uuid: 2B3BDD1F-328C-322C-3F8C-14079BE4FE48 interface-version: 1 name: Remote Fw APIs protocol-sequence: ncacn_ip_tcp:172.23.202.79[49158]

Tabela 37. Windows OS – Pronađeni servisi na IP adresi 172.23.202.78 (2011. godina)

SERVISI	CIFS⁸⁸⁶, CIFS Name Service⁸⁸⁷ : advertised-name-1: VISTAx86HoPrSp2 (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: VISTAx86HoPrSp2 (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 202B295A1703 DCE RPC interface-uuid: A32AFE70-B6D6-2259-122E-1C84DA1DAB1D interface-version: 1 name: A32AFE70-B6D6-2259-122E-1C84DA1DAB1D object-interface-uuid: 125294BA-12BC-23B8-24E9-45FD77769D67 protocol-sequence: ncacn_ip_tcp:172.23.202.78[49152] iinterface-uuid: 45BBA34A-BE32-67F9-B089-12F790261078 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.78[49153] interface-uuid: AB7A0523-AB70-75DD-292E-5A5E4B872251 interface-version: 1 name: AppInfo protocol-sequence: ncacn_ip_tcp:172.23.202.78[49154] interface-uuid: 34945328-5384-10CD-12E0-497745678939 interface-version: 1 name: 34945328-5384-10CD-12E0-497745678939 protocol-sequence: ncacn_ip_tcp:172.23.202.78[49155] interface-uuid: 567ABB43-6944-32B1-AC42-56F038771012 interface-version: 2 name: 567ABB43-6944-32B1-AC42-56F038771012 protocol-sequence: ncacn_ip_tcp:172.23.202.78[49156] interface-uuid: 2B9CDD1E-578A-322C-BF9C-14079BE4AE44 interface-version: 1 name: Remote Fw APIs protocol-sequence: ncacn_ip_tcp:172.23.202.78[49158]

Tabela 38. Windows OS – Pronađeni servisi na IP adresi 172.23.202.77 (2011. godina)

SERVISI	CIFS⁸⁸⁸,

⁸⁸⁶ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

⁸⁸⁷ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

⁸⁸⁸ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

	CIFS Name Service⁸⁸⁹ : advertised-name-1: VISTAx64HoPrSp2 (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: VISTAx64HoPrSp2 (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 569C285B0117 DCE RPC interface-uuid: A05ABE00-A0D0-4059-832E-3C84BA1D1B0A interface-version: 1 name: A05ABE00-A0D0-4059-832E-3C84BA1D1B0A object-interface-uuid: 438294BA-40B1-78B3-22E9-39FD56769D22 protocol-sequence: ncacn_ip_tcp:172.23.202.77[49152] iinterface-uuid: 12CCA54A-CE02-19F9-C0A0-01F290561011 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.77[49153] interface-uuid: AB2A0221-AC60-23D1-1B2E-1C6ED48225B7 interface-version: 1 name: AppInfo protocol-sequence: ncacn_ip_tcp:172.23.202.77[49154] interface-uuid: 11145778-1114-13CD-EF12-37745B4689A1 interface-version: 1 name: 11145778-1114-13CD-EF12-37745B4689A1 protocol-sequence: ncacn_ip_tcp:172.23.202.77[49155] interface-uuid: 467A2B82-6854-45F1-2D32-68F03700A001 interface-version: 2 name: 467A2B82-6854-45F1-2D32-68F03700A001 protocol-sequence: ncacn_ip_tcp:172.23.202.77[49156] interface-uuid: 3A52B4D1-228A-322C-A18C-A4069BE4FB42 interface-version: 1 name: Remote Fw APIs protocol-sequence: ncacn_ip_tcp:172.23.202.77[49158]

Tabela 39. Windows OS sa IP adresama 172.23.202.117, 172.23.202.68 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.117		OS: : Microsoft Windows 2008 Datacenter x86 SP1, 2008DTCX86SP1			7
IP adresa: 172.23.202.68		Wwindows 2008 server Enterprise x86 SP1, 2008EntX86SP1			7
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	MS09-050: Vulnerabilities in SMBv2 Could Allow Remote Code Execution (windows-hotfix-ms09-	Ovo ažuriranje bezbednosti rešava jednu javnu i nekoliko ranjivosti koje su privatno prijavljene u protokolu Microsoft Message Block-a 2 (SMBv2). Opasnost od ove ranjivosti	MS MS09-050 ⁸⁹⁰ MSKB 975517 ⁸⁹¹ CVE CVE-2009-2526 ⁸⁹² CVE CVE-2009-2532 ⁸⁹³ CVE CVE-2009-3103 ⁸⁹⁴	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows6.0-KB975517-x86.cab (197912 bytes) ⁸⁹⁷

⁸⁸⁹ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

⁸⁹⁰ <http://technet.microsoft.com/en-us/security/bulletin/MS09-050>

⁸⁹¹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;975517>

⁸⁹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2526>

⁸⁹³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2532>

⁸⁹⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3103>

	050)	leži u tome što bi ona omogućila daljinsko izvršenje kôda ako napadač pošalje posebno kreiran SMB paket ka kompjuteru koji pokreće servis servera. Najbolje prakse zaštitnog zida i standardne konfiguracije zaštitnog zida po difoltu mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan okvira preduzeća. Za sisteme koji su stalno povezani na Internet preporuka je da imaju što manji broj izloženih portova.	SECUNIA 36623 ⁸⁹⁵ URL1 ⁸⁹⁶		
2.	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-054)	172.23.202.117:139 172.23.202.117:445 172.23.202.68:139 172.23.202.68:445 Opis je isti kao kod ranjivosti MS10-012	CVE: CVE-2010-2550 ⁸⁹⁸ CVE: CVE-2010-2551 ⁸⁹⁹ CVE: CVE-2010-2552 ⁹⁰⁰ MS: MS10-054 ⁹⁰¹ MSKB 982214 ⁹⁰²	Kritičan	Uraditi download a zatim instalirati Microsoft patch windows6.0-kb982214-x86.cab (325694 bytes) ⁹⁰³
3.	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms11-020)	172.23.202.117:139 172.23.202.117:445 172.23.202.68:139 172.23.202.68:445 Opis je isti kao kod ranjivosti MS10-012	CVE CVE-2011-0661 ⁹⁰⁴ MS: MS11-020 ⁹⁰⁵ MSKB: 2508429 ⁹⁰⁶	Kritičan	Uraditi download a zatim instalirati Microsoft patch windows6.0-kb2508429-x86.cab (332927 bytes) ⁹⁰⁷
4.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.117:139 172.23.202.117:445 172.23.202.68:139 172.23.202.68:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB: 887429 ⁹⁰⁸ URL1 ⁹⁰⁹	Ozbiljan	Metoda za konfiguracije SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429. ⁹¹⁰ Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing</i> = <i>auto</i> ili da se zahteva SMB potpisivanje: <i>server signing</i> = <i>mandatory</i> .
5.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.117:139 172.23.202.117:445 172.23.202.68:139 172.23.202.68:445	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti

⁸⁹⁷ download.windowsupdate.com/msdownload/update/software/secu/2009/09/windows6.0-kb975517-

x86_dc06eae8a89a24a1f1aa016bf6fd10e7eca34d.cab

⁸⁹⁵ http://secunia.com/advisories/36623/⁸⁹⁶ http://g-laurent.blogspot.com/2009/09/windows-vista7-smb20-negotiate-protocol.html⁸⁹⁸ http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2550⁸⁹⁹ http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2551⁹⁰⁰ http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2552⁹⁰¹ http://technet.microsoft.com/en-us/security/bulletin/MS10-054⁹⁰² http://support.microsoft.com/default.aspx?scid=kb;EN-US;982214⁹⁰³ download.windowsupdate.com/msdownload/update/software/secu/2010/07/windows6.0-kb982214-

x86_50d77476159fef060a2470a0f66e7e8ecb9808ea.cab

⁹⁰⁴ http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661⁹⁰⁵ http://technet.microsoft.com/en-us/security/bulletin/ms11-020⁹⁰⁶ http://support.microsoft.com/default.aspx?scid=kb;EN-US;2508429⁹⁰⁷ download.windowsupdate.com/msdownload/update/software/secu/2011/03/windows6.0-kb2508429-

x86_2e7adf8e8e545432372edbd59952a925fb7a69da.cab

⁹⁰⁸ http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429⁹⁰⁹ http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx⁹¹⁰ http://support.microsoft.com/kb/887429

		Sistem omogućava, ali ne zahteva SMB potpisivanje.	ranjivosti		
6.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	OSVDB ⁹¹¹ CVE: CVE-1999-0524 ⁹¹² XF: icmp-netmask(306) ⁹¹³ XF: icmp-timestamp(322) ⁹¹⁴	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost
7.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta (što zlonamerni napadač može iskoristiti pri planiranju daljih napada). Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1 ⁹¹⁵ URL2 ⁹¹⁶ URL3 ⁹¹⁷	Umeren	Onemogućavanje TCP timestamp odgovora na Windows OS. Podesiti Tcp1323Opts vrednost na sledećem ključu na 1: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

Tabela 40. Windows OS – Pronađeni servisi na IP adresi 172.23.202.117 (2011. godina)

SERVISI	CIFS⁹¹⁸, CIFS Name Service⁹¹⁹ : advertised-name-1: 2008DTCX86SP1 (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: 2008DTCX86SP1 (File Server Service) mac-address: 555C28D59399 DCE RPC interface-uuid: A99AFE90-A9D9-9259-722E-9C84DA1DAB5D interface-version: 1 name: A99AFE90-A9D9-9259-722E-9C84DA1DAB5D object-interface-uuid: 164294CA-40BC-68B9-72E9-89FB55869D27 protocol-sequence: ncacn_ip_tcp:172.23.202.117[49152] interface-uuid: 4A3728C4-23AB-298B-83A1-81E01EB0A6D4 interface-version: 1 name: DHCP Client LRPC Endpoint protocol-sequence: ncacn_ip_tcp:172.23.202.117[49153]

⁹¹¹ <http://www.osvdb.org/95>⁹¹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁹¹³ <http://xforce.iss.net/xforce/xfdb/306>⁹¹⁴ <http://xforce.iss.net/xforce/xfdb/322>⁹¹⁵ http://www.forensicswiki.org/wiki/TCP_timestamps⁹¹⁶ <http://www.ietf.org/rfc/rfc1323.txt>⁹¹⁷ <http://uptime.netcraft.com/>⁹¹⁸ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).⁹¹⁹ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	interface-uuid: A408C522-A50A-43DA-BB7A-4C1E0503A522 interface-version: 1 name: IKE/Authip API protocol-sequence: ncacn_ip_tcp:172.23.202.117[49154] interface-uuid: 6A665728-E4B3-43B2-EF22-26399B6789AD interface-version: 1 name: 6A665728-E4B3-43B2-EF22-26399B6789AD protocol-sequence: ncacn_ip_tcp:172.23.202.117[49155] interface-uuid: 468ABA82-9824-35F3-AB32-38F068001D04 interface-version: 2 name: 468ABA82-9824-35F3-AB32-38F068001D04 protocol-sequence: ncacn_ip_tcp:172.23.202.117[49156] interface-uuid: 7D441D1E-548C-522C-5F8C-12078BE4AE22 interface-version: 1 name: Remote Fw APIs protocol-sequence: ncacn_ip_tcp:172.23.202.117[49158]

Tabela 41. Windows OS – Pronađeni servisi na IP adresi 172.23.202.68 (2011. godina)

SERVISI	CIFS⁹²⁰, CIFS Name Service⁹²¹ : advertised-name-1: 2008EntX86SP1 (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: 2008EntX86SP1 (File Server Service) mac-address: 320C22D56321 DCE RPC interface-uuid: B22AFE32-A1D7-3455-233E-1A82DA2123B5 interface-version: 1 name: B22AFE32-A1D7-3455-233E-1A82DA2123B5 object-interface-uuid: 365432CA-42BC-28B9-62E9-66FA52807D33 protocol-sequence: ncacn_ip_tcp:172.23.202.68[49152] interface-uuid: 3A3328C2-130B-334B-78A1-21E01340A1D0 interface-version: 1 name: DHCP Client LRPC Endpoint protocol-sequence: ncacn_ip_tcp:172.23.202.68[49153] interface-uuid: B208C331-A55A-21DA-BA71-5C1E3473A225 interface-version: 1 name: IKE/Authip API protocol-sequence: ncacn_ip_tcp:172.23.202.68[49154] interface-uuid: 6A370478-E1B1-45B2-EF81-26690B3191A1 interface-version: 1 name: 6A370478-E1B1-45B2-EF81-26690B3191A1 protocol-sequence: ncacn_ip_tcp:172.23.202.68[49155] interface-uuid: 233CB281-2679-31F1-5B32-18F058101D12 interface-version: 2 name: 233CB281-2679-31F1-5B32-18F058101D12 protocol-sequence: ncacn_ip_tcp:172.23.202.68[49156] interface-uuid: 4A331D13-679C-244C-1F7C-76787BE4AA38

⁹²⁰ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

⁹²¹ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	interface-version: 1 name: Remote Fw APIs protocol-sequence: ncacn_ip_tcp:172.23.202.68[49158]

Tabela 42. Windows OS sa IP adresama 172.23.202.108 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.108		OS: : Microsoft Windows XP Pro Sp3 x86, WINXPproSP3x86			4
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.108:139 172.23.202.108:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB: 887429 ⁹²² URL ⁹²³	Ozbiljan	Metoda za konfiguracije SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429. ⁹²⁴ Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing</i> = <i>auto</i> ili da se zahteva SMB potpisivanje: <i>server signing</i> = <i>mandatory</i> .
2.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.108:139 172.23.202.108:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti
3.	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server. Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko poziva udaljenih procedura (RPC). Ovi servisi su i u prošlosti bili skloni ranjivostima.. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinjenije napade.	BID: 494 ⁹²⁵ CVE: CVE-1999-0519 ⁹²⁶ MSKB: 143474 ⁹²⁷ URL ⁹²⁸	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost
4.	ICMP timestamp response (generic-icmp-)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-ov zahtev za	CVE: CVE-1999-0524 ⁹²⁹ XF: icmp-netmask(306) ⁹³⁰	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow

⁹²² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429>⁹²³ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>⁹²⁴ <http://support.microsoft.com/kb/887429>⁹²⁵ <http://www.securityfocus.com/bid/494>⁹²⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>⁹²⁷ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>⁹²⁸ http://www.hsc.fr/ressources/presentations/null_sessions/⁹²⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>

timestamp)	vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatišu slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	XF: timestamp(322) ⁹³¹ icmp-	incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.

Tabela 43. Windows OS – Pronađeni servisi na IP adresi 172.23.202.108 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni deljeni resurs, mount-point: C:\
SERVISI	CIFS ⁹³² , CIFS Name Service ⁹³³ : advertised-name-1: WINXPproSP3x86 (Computer Name) advertised-name-2: WINXPproSP3x86 (File Server Service) advertised-name-3: WORKGROUP (Domain Name) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 000C29B4C742 NTP : 172.23.202.108 udp 123

Tabela 44. Windows OS sa IP adresama 172.23.202.105 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.105		OS: : Microsoft Windows XP Professional x86, WINXPprox86			15
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Microsoft Server Service / CanonicalizePathName() Remote Code Execution Vulnerability (dcerpc-msnetapi-netpathcanonicalize-dos)	Određene verzije Microsoft Windows-a su ranjive na daljinsko preopterećenje bafera (privremene memorije) koje bi moglo da kompromituje određeni računar. Posebno opremljen paket se može koristiti sa pozivom ka NetPathCanonicalize RPC ruti na servisu servera, pri čemu bi napadač mogao da izvrši kod pod sistemskim nivoom pristupa.	CVE: CVE-2006-3439 ⁹³⁴ , MS: MS06-040 ⁹³⁵ , MSKB: 921883 ⁹³⁶ , SANS-06: W4 ⁹³⁷ , SANS-07: S2 ⁹³⁸	Kritičan	Instalirati Microsoft service pack Windows XP Service Pack 1 Uraditi download a zatim instalirati Microsoft patch WindowSXP-KB921883-x86-ENU.EXE ⁹³⁹

⁹³⁰ <http://xforce.iss.net/xforce/xfdb/306>⁹³¹ <http://xforce.iss.net/xforce/xfdb/322>⁹³² CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).⁹³³ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.⁹³⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-3439>⁹³⁵ <http://technet.microsoft.com/en-us/security/bulletin/ms06-040>⁹³⁶ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;921883>⁹³⁷ <http://www.sans.org/critical-security-controls/#w4>⁹³⁸ <http://www.sans.org/critical-security-controls/#s2>⁹³⁹ download.microsoft.com/download/c/2/b/c2b41862-1113-4e40-a81a-d6971733e361/WindowsXP-KB921883-x86-ENU.exe

2.	MS03-039: Buffer Overrun In RPCSS Service Could Allow Code Execution (824146) (windows-hotfix-ms03-039)	Napadač koji je uspešno iskoristio ove ranjivosti bi mogao biti u mogućnosti da pokrene kôd sa privilegijama lokalnog sistema na pogođenom sistemu ili bi mogao da prouzrokuje kvar RPCSS servisa. Napadač bi tada mogao biti u mogućnosti da preduzme bilo kakvu radnju na sistemu, uključujući instaliranje programa, pregledavanje, menjanje i brisanje podataka ili stvaranje novih naloga sa svim privilegijama. Da bi iskoristio ove ranjivosti, napadač bi morao da napravi program sa kojim bi poslao malicioznu RPC poruku ranjivom sistemu, ciljajući na RPCSS servis.	BID: 8458 ⁹⁴⁰ , CVE: CVE-2003-0528 ⁹⁴¹ , CVE: CVE-2003-0605 ⁹⁴² , CVE: CVE-2003-0715 ⁹⁴³ , MSKB: 824146 ⁹⁴⁴ , MS:MS03-039 ⁹⁴⁵	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB824146-x86-ENU.exe (1543456 bytes) ⁹⁴⁶ , Uraditi download a zatim instalirati Microsoft patch DirectX9-KB819696-x86-ENU.exe (970312 bytes) ⁹⁴⁷
3.	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (windows-hotfix-ms08-067)	172.23.202.105:139 172.23.202.105:445 Ova bezbednosna ispravka rešava ranjivost koja je prijavljena od strane privatnog lica. Ranjivost bi mogla da omogućiti daljinsko izvršavanje koda ukoliko je napadnuti sistem primio posebno opremljeni RPC zahtev. Na sistemima Microsoft Windows 2000, Windows XP, i Windows Server 2003, napadač bi mogao da iskoristi ovu ranjivost bez overavanja autentičnosti i da pokrene proizvoljan kôd. Moguće je da ova ranjivost može biti upotrebljena za intenziviranje skrivenog korišćenja. Najbolje prakse zaštitnog zida i standardne konfiguracije zaštitnog zida po defaultu mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan okvira preduzeća.	MS: MS08-067 ⁹⁴⁸ MSKB: 958644 ⁹⁴⁹ CVE: CVE-2008-4250 ⁹⁵⁰ SECUNIA: 32326 ⁹⁵¹ URL1 ⁹⁵² URL2 ⁹⁵³ URL3 ⁹⁵⁴	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB958644-x86-ENU.exe (648560 bytes) ⁹⁵⁵
4.	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution	172.23.202.105:139 172.23.202.105:445 Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti koje su privatno prijavljene, a odnose se na protokol	MS: MS09-001 ⁹⁵⁶ MSKB: 958687 ⁹⁵⁷ CVE: CVE-2008-4114 ⁹⁵⁸ CVE: CVE-2008-4835 ⁹⁵⁹ CVE: CVE-2008-4834 ⁹⁶⁰	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB958687-x86-ENU.exe (658288

⁹⁴⁰ <http://www.securityfocus.com/bid/8458>⁹⁴¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0528>⁹⁴² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0605>⁹⁴³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0715>⁹⁴⁴ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;824146>⁹⁴⁵ <http://technet.microsoft.com/en-us/security/bulletin/ms03-039>⁹⁴⁶ www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb824146-x86-enu_b957699c7365c462446bd552cd6d203.exe⁹⁴⁷ www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/directx9-kb819696-x86-enu_977f8cc86c1e151a0168d1296210913.exe⁹⁴⁸ <http://technet.microsoft.com/en-us/security/bulletin/ms08-067>⁹⁴⁹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958644>⁹⁵⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4250>⁹⁵¹ <http://secunia.com/advisories/32326/>⁹⁵² blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx⁹⁵³ <http://blogs.msdn.com/b/sdl/archive/2008/10/22/ms08-067.aspx>⁹⁵⁴ <http://blogs.technet.com/b/msrc/archive/2008/10/23/ms08-067-released.aspx>⁹⁵⁵ http://download.windowsupdate.com/msdownload/update/software/secu/2008/10/windowsxpkb958644-x86-enu_5c135a8dae5721849430afe27af255f83e64f62b.exe⁹⁵⁶ <http://technet.microsoft.com/en-us/security/bulletin/MS09-001>⁹⁵⁷ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958687>⁹⁵⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4114>⁹⁵⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4835>⁹⁶⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4834>

	(windows-hotfix-ms09-001)	Microsoft Server Message Block-a (SMB). Ranjivosti mogu da omoguće daljinsko izvršenje kôda na ugroženim sistemima. Napadač koji je uspešno iskoristio ove ranjivosti može da instalira programe, pregleda, menja ili briše podatke ili otvara nove naloge sa potpunim korisničkim pravima. Praksa je pokazala da zaštitni zid i njegove standardne konfiguracije po defaultu mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan okvira organizacije. Za sisteme koji su stalno povezani na Internet preporuka je da imaju što manji broj izloženih portova.	SECUNIA: 31883 ⁹⁶¹ URL1 ⁹⁶² URL2 ⁹⁶³ URL3 ⁹⁶⁴		bytes) ⁹⁶⁵
5.	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-012)	172.23.202.105:139 172.23.202.105:445 Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti koje su privatno prijavljene u Microsoft Windows-u. Opasnost od ove ranjivosti leži u tome što bi ona omogućila daljinsko izvršavanje kôda ukoliko bi napadač kreirao posebno opremljen SMB paket i poslao ga ugroženom sistemu. Praksa je pokazala da upotreba zaštitnog zida može da pomogne u zaštiti mrežnih resursa od napada (koji bi pokušali da iskoriste ove ranjivosti), a koje potiču izvan okvira organizacije.	MS: MS10-012 ⁹⁶⁶ MSKB - 971468 ⁹⁶⁷ CVE: CVE-2010-0020 ⁹⁶⁸ CVE: CVE-2010-0021 ⁹⁶⁹ CVE: CVE-2010-0022 ⁹⁷⁰ CVE CVE-2010-0231 ⁹⁷¹ SECUNIA 38510 ⁹⁷²	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB971468-x86-ENU.exe (664952 bytes) ⁹⁷³
6.	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-054)	172.23.202.105:139 172.23.202.105:445 Opis je isti kao kod ranjivosti MS10-012	CVE: CVE-2010-2550 ⁹⁷⁴ CVE: CVE-2010-2551 ⁹⁷⁵ CVE: CVE-2010-2552 ⁹⁷⁶ MS: MS10-054 ⁹⁷⁷ MSKB 982214 ⁹⁷⁸	Kritičan	Uraditi download a zatim instalirati Microsoft patch windowsxp-kb982214-x86-enu.exe (661368 bytes) ⁹⁷⁹
7.	MS11-020: Vulnerability in SMB Server Could Allow	172.23.202.105:139 172.23.202.105:445 Opis je isti kao kod ranjivosti MS10-	CVE: CVE-2011-0661 ⁹⁸⁰ MS: MS11-020 ⁹⁸¹ MSKB: 2508429 ⁹⁸²	Kritičan	Uraditi download a zatim instalirati Microsoft patch windowsxp-kb2508429-

⁹⁶¹ <http://secunia.com/advisories/31883/>⁹⁶² http://www.vallejo.cc/proyectos/vista_SMB_write_DoS.htm⁹⁶³ <http://www.zerodayinitiative.com/advisories/ZDI-09-001/>⁹⁶⁴ <http://www.zerodayinitiative.com/advisories/ZDI-09-002/>⁹⁶⁵ http://download.windowsupdate.com/msdownload/update/software/secu/2008/12/windowsxp-kb958687-x86-enu_a9b85264e9b75e552ae10cd212937b8686a96833.exe⁹⁶⁶ <http://technet.microsoft.com/en-us/security/bulletin/MS10-012>⁹⁶⁷ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;971468>⁹⁶⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0020>⁹⁶⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0021>⁹⁷⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0022>⁹⁷¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0231>⁹⁷² <http://secunia.com/advisories/38510/>⁹⁷³ http://download.windowsupdate.com/msdownload/update/software/secu/2010/01/windowsxp-kb971468-x86-enu_68d7899c8b8462219daf40f02c6fb9f362b1ee6b.exe⁹⁷⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2550>⁹⁷⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2551>⁹⁷⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2552>⁹⁷⁷ <http://technet.microsoft.com/en-us/security/bulletin/MS10-054>⁹⁷⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;982214>⁹⁷⁹ http://download.windowsupdate.com/msdownload/update/software/secu/2010/07/windowsxp-kb982214-x86-enu_a24853f682dad3157da4e4a39372951a8ec1e407.exe⁹⁸⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661>⁹⁸¹ <http://technet.microsoft.com/en-us/security/bulletin/ms11-020>

	Remote Code Execution (windows-hotfix-ms11-020)	012			x86-enu.exe (664960 bytes) ⁹⁸³
8.	MS03-026: Buffer Overrun In RPC Interface Could Allow Code Execution (823980) (windows-hotfix-ms03-026)	Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti u Windows Distributed Component Object Model-u (DCOM) preko Remote Procedure Call-a (RPC). Napadač koji bi uspešno iskoristio ovu ranjivost mogao bi da pokrene kôd sa privilegijama lokalnog sistema na napadnutom sistemu. Napadač bi mogao da preduzme bilo kakvu akciju na sistemu, uključujući instaliranje programa, pregledanje, izmenu ili brisanje podataka ili otvaranje novih naloga sa svim privilegijama. Da bi iskoristio ovu ranjivost, napadač bi morao da pošalje posebno formiran zahtev udaljenom računaru ka specifičnim RPC portovima.	CVE: CVE-2003-0352 ⁹⁸⁴ MS: MS03-026 ⁹⁸⁵ BID: 8205 ⁹⁸⁶ MSKB: 823980 ⁹⁸⁷	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB823980-x86-ENU.exe (1291040 bytes) ⁹⁸⁸
9.	MS04-011: Security Update for Microsoft Windows (835732) (windows-hotfix-ms04-011)	172.23.202.105:139 172.23.202.105:445 Ovo ažuriranje rešava nekoliko novootkrivenih ranjivosti. Napadač koji uspešno iskoristi ovu ranjivost bi mogao da preuzme potpunu kontrolu nad napadnutim sistemom, uključujući instaliranje programa, pregledanje, menjanje ili brisanje podataka ili čak otvaranje novih naloga sa svim privilegijama.	BID 10108 ⁹⁸⁹ BID 10113 ⁹⁹⁰ BID 10114 ⁹⁹¹ BID 10115 ⁹⁹² BID 10117 ⁹⁹³ BID 10118 ⁹⁹⁴ BID 10119 ⁹⁹⁵ BID 10120 ⁹⁹⁶ BID 10122 ⁹⁹⁷ BID 10124 ⁹⁹⁸ BID 10125 ⁹⁹⁹ BID 10126 ¹⁰⁰⁰ CERT-VN 122076 ¹⁰⁰¹ CERT-VN 150236 ¹⁰⁰² CERT-VN 206468 ¹⁰⁰³ CERT-VN 255924 ¹⁰⁰⁴ CERT-VN 260588 ¹⁰⁰⁵ CERT-VN 353956 ¹⁰⁰⁶ CERT-VN 471260 ¹⁰⁰⁷	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB835732-x86-ENU.EXE (2710296 bytes) ¹⁰⁸⁴

⁹⁸² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;2508429>⁹⁸³ http://download.windowsupdate.com/msdownload/update/software/secu/2011/03/windowsxp-kb2508429-x86-enu_e0b40d81f2ecc1bad43439a6bd0a9e2a0ab7dd56.exe⁹⁸⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0352>⁹⁸⁵ <http://technet.microsoft.com/en-us/security/bulletin/ms03-026>⁹⁸⁶ <http://www.securityfocus.com/bid/8205>⁹⁸⁷ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;823980>⁹⁸⁸ http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb823980-x86-enu_1d296adab6699e66210e5a350236381.exe⁹⁸⁹ <http://www.securityfocus.com/bid/10108>⁹⁹⁰ <http://www.securityfocus.com/bid/10113>⁹⁹¹ <http://www.securityfocus.com/bid/10114>⁹⁹² <http://www.securityfocus.com/bid/10115>⁹⁹³ <http://www.securityfocus.com/bid/10117>⁹⁹⁴ <http://www.securityfocus.com/bid/10118>⁹⁹⁵ <http://www.securityfocus.com/bid/10119>⁹⁹⁶ <http://www.securityfocus.com/bid/10120>⁹⁹⁷ <http://www.securityfocus.com/bid/10122>⁹⁹⁸ <http://www.securityfocus.com/bid/10124>⁹⁹⁹ <http://www.securityfocus.com/bid/10125>¹⁰⁰⁰ <http://www.securityfocus.com/bid/10126>¹⁰⁰¹ <http://www.kb.cert.org/vuls/id/122076>¹⁰⁰² <http://www.kb.cert.org/vuls/id/150236>¹⁰⁰³ <http://www.kb.cert.org/vuls/id/206468>¹⁰⁰⁴ <http://www.kb.cert.org/vuls/id/255924>¹⁰⁰⁵ <http://www.kb.cert.org/vuls/id/260588>¹⁰⁰⁶ <http://www.kb.cert.org/vuls/id/353956>¹⁰⁰⁷ <http://www.kb.cert.org/vuls/id/471260>

			CERT-VN 526084 ¹⁰⁰⁸ CERT-VN 547028 ¹⁰⁰⁹ CERT-VN 586540 ¹⁰¹⁰ CERT-VN 638548 ¹⁰¹¹ CERT-VN 639428 ¹⁰¹² CVE CVE-2003-0663 ¹⁰¹³ CVE CVE-2003-0719 ¹⁰¹⁴ CVE CVE-2003-0806 ¹⁰¹⁵ CVE CVE-2003-0906 ¹⁰¹⁶ CVE CVE-2003-0907 ¹⁰¹⁷ CVE CVE-2003-0908 ¹⁰¹⁸ CVE CVE-2003-0909 ¹⁰¹⁹ CVE CVE-2003-0910 ¹⁰²⁰ CVE CVE-2004-0117 ¹⁰²¹ CVE CVE-2004-0118 ¹⁰²² CVE CVE-2004-0119 ¹⁰²³ CVE CVE-2004-0120 ¹⁰²⁴ CVE CVE-2004-0123 ¹⁰²⁵ OVAL OVAL1004 ¹⁰²⁶ OVAL OVAL1007 ¹⁰²⁷ OVAL OVAL1016 ¹⁰²⁸ OVAL OVAL1046 ¹⁰²⁹ OVAL OVAL1054 ¹⁰³⁰ OVAL OVAL1064 ¹⁰³¹ OVAL OVAL1076 ¹⁰³² OVAL OVAL1093 ¹⁰³³ OVAL OVAL1512 ¹⁰³⁴ OVAL OVAL1718 ¹⁰³⁵ OVAL OVAL1808 ¹⁰³⁶ OVAL OVAL1962 ¹⁰³⁷ OVAL OVAL1997 ¹⁰³⁸ OVAL OVAL883 ¹⁰³⁹ OVAL OVAL885 ¹⁰⁴⁰ OVAL OVAL886 ¹⁰⁴¹		

¹⁰⁸⁴ http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb835732-x86-enu_99fc98fc8e8cbf6720f28028a1f05eb.exe

¹⁰⁰⁸ <http://www.kb.cert.org/vuls/id/526084>

¹⁰⁰⁹ <http://www.kb.cert.org/vuls/id/547028>

¹⁰¹⁰ <http://www.kb.cert.org/vuls/id/586540>

¹⁰¹¹ <http://www.kb.cert.org/vuls/id/638548>

¹⁰¹² <http://www.kb.cert.org/vuls/id/639428>

¹⁰¹³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0663>

¹⁰¹⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0719>

¹⁰¹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0806>

¹⁰¹⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0906>

¹⁰¹⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0907>

¹⁰¹⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0908>

¹⁰¹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0909>

¹⁰²⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0910>

¹⁰²¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0117>

¹⁰²² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0118>

¹⁰²³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0119>

¹⁰²⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0120>

¹⁰²⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0123>

¹⁰²⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1004>

¹⁰²⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1007>

¹⁰²⁸ oval.mitre.org/oval/definitions/data/OVAL1016.html

¹⁰²⁹ oval.mitre.org/oval/definitions/data/OVAL1046.html

¹⁰³⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1054>

¹⁰³¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1064>

¹⁰³² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1076>

¹⁰³³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1093>

¹⁰³⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1512>

¹⁰³⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1718>

¹⁰³⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1808>

¹⁰³⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1962>

¹⁰³⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1997>

¹⁰³⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:883>

¹⁰⁴⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:885>

¹⁰⁴¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:886>

			OVAL OVAL889 ¹⁰⁴² OVAL OVAL890 ¹⁰⁴³ OVAL OVAL892 ¹⁰⁴⁴ OVAL OVAL895 ¹⁰⁴⁵ OVAL OVAL896 ¹⁰⁴⁶ OVAL OVAL897 ¹⁰⁴⁷ OVAL OVAL898 ¹⁰⁴⁸ OVAL OVAL903 ¹⁰⁴⁹ OVAL OVAL904 ¹⁰⁵⁰ OVAL OVAL907 ¹⁰⁵¹ OVAL OVAL911 ¹⁰⁵² OVAL OVAL919 ¹⁰⁵³ OVAL OVAL924 ¹⁰⁵⁴ OVAL OVAL946 ¹⁰⁵⁵ OVAL OVAL951 ¹⁰⁵⁶ OVAL OVAL959 ¹⁰⁵⁷ OVAL OVAL964 ¹⁰⁵⁸ URL1 ¹⁰⁵⁹ URL2 ¹⁰⁶⁰ URL3 ¹⁰⁶¹ URL4 ¹⁰⁶² URL5 ¹⁰⁶³ URL6 ¹⁰⁶⁴ URL7 ¹⁰⁶⁵ URL8 ¹⁰⁶⁶ XF ssl-message- dos(15712) ¹⁰⁶⁷ XF win-asn1-double- free(15713) ¹⁰⁶⁸ XF win-h323- bo(15710) ¹⁰⁶⁹ XF win-hcpurl-code- execution(15704) ¹⁰⁷⁰ XF win-ldt-gain- privileges(15707) ¹⁰⁷¹ XF win-lsass- bo(15699) ¹⁰⁷²		

¹⁰⁴² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:889>
¹⁰⁴³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:890>
¹⁰⁴⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:892>
¹⁰⁴⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:895>
¹⁰⁴⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:896>
¹⁰⁴⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:897>
¹⁰⁴⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:898>
¹⁰⁴⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:903>
¹⁰⁵⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:904>
¹⁰⁵¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:907>
¹⁰⁵² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:911>
¹⁰⁵³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:919>
¹⁰⁵⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:924>
¹⁰⁵⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:946>
¹⁰⁵⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:951>
¹⁰⁵⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:959>
¹⁰⁵⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:964>
¹⁰⁵⁹ <http://archives.neohapsis.com/archives/vulnwatch/2004-q1/0081.html>
¹⁰⁶⁰ <http://archives.neohapsis.com/archives/vulnwatch/2004-q1/0082.html>
¹⁰⁶¹ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020065.html>
¹⁰⁶² <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020068.html>
¹⁰⁶³ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020069.html>
¹⁰⁶⁴ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020070.html>
¹⁰⁶⁵ <http://www.securiteam.com/windowsntfocus/5LP0C2ACKU.html>
¹⁰⁶⁶ <http://www.securityfocus.com/archive/1/361836>
¹⁰⁶⁷ <http://xforce.iss.net/xforce/xfdb/15712>
¹⁰⁶⁸ <http://xforce.iss.net/xforce/xfdb/15713>
¹⁰⁶⁹ <http://xforce.iss.net/xforce/xfdb/15710>
¹⁰⁷⁰ <http://xforce.iss.net/xforce/xfdb/15704>
¹⁰⁷¹ <http://xforce.iss.net/xforce/xfdb/15707>
¹⁰⁷² <http://xforce.iss.net/xforce/xfdb/15699>

			XF win-spp-bo(15715)¹⁰⁷³ XF win-vdm-gain-privileges(15714)¹⁰⁷⁴ XF win-winlogon-bo(15702)¹⁰⁷⁵ XF win2k-lsass-ldap-dos(15700)¹⁰⁷⁶ XF win2k-utilitymgr-gain-privileges(15632) MS: MS04-011¹⁰⁷⁷ , CVE: CVE-2003-0533¹⁰⁷⁸ MSKB: 835732¹⁰⁷⁹ OVAL: OVAL1000¹⁰⁸⁰ CERT-VN: 753212¹⁰⁸¹ CERT-VN: 783748¹⁰⁸² XF: winxp-task-gain-privileges(15678)¹⁰⁸³		
10.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.105:139 172.23.202.105:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB: 887429¹⁰⁸⁵ URL1¹⁰⁸⁶	Ozbiljan	Metoda za konfiguracije SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429¹⁰⁸⁷ . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing = auto</i> ili da se zahteva SMB potpisivanje: <i>server signing = mandatory</i> .
11.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.105:139 172.23.202.105:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti
12.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	172.23.202.105:135: Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hедера i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji	BID: 10183¹⁰⁸⁸ CERT-VN: 415294¹⁰⁸⁹ CVE CVE-2004-0230¹⁰⁹⁰ MS: MS05-019¹⁰⁹¹ MS: MS06-064¹⁰⁹² NETBSD: NetBSD-SA2004-006¹⁰⁹³ OVAL: OVAL2689¹⁰⁹⁴	Ozbiljan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB893066-v2-x86-ENU.exe (791280 bytes) ¹¹⁰²

¹⁰⁷³ <http://xforce.iss.net/xforce/xfdb/15715>¹⁰⁷⁴ <http://xforce.iss.net/xforce/xfdb/15714>¹⁰⁷⁵ <http://xforce.iss.net/xforce/xfdb/15702>¹⁰⁷⁶ <http://xforce.iss.net/xforce/xfdb/15700>¹⁰⁷⁷ <http://technet.microsoft.com/en-us/security/bulletin/ms04-011>¹⁰⁷⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0533>¹⁰⁷⁹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;835732>¹⁰⁸⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1000>¹⁰⁸¹ <http://www.kb.cert.org/vuls/id/753212>¹⁰⁸² <http://www.kb.cert.org/vuls/id/783748>¹⁰⁸³ <http://xforce.iss.net/xforce/xfdb/15678>¹⁰⁸⁵ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429>¹⁰⁸⁶ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>¹⁰⁸⁷ <http://support.microsoft.com/kb/887429>¹⁰⁸⁸ <http://www.securityfocus.com/bid/10183>¹⁰⁸⁹ <http://www.kb.cert.org/vuls/id/415294>¹⁰⁹⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>¹⁰⁹¹ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>¹⁰⁹² <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>¹⁰⁹³ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>¹⁰⁹⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>

		koriste dugotrajne veze, kao npr. BGP.	OVAL: OVAL270¹⁰⁹⁵ OVAL OVAL3508¹⁰⁹⁶ OVAL OVAL4791¹⁰⁹⁷ OVAL OVAL5711¹⁰⁹⁸ SECUNIA: 11440¹⁰⁹⁹ SECUNIA: 22341¹¹⁰⁰ SGI 20040403-01-A¹¹⁰¹		
13.	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server . Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko poziva udaljenih procedura (RPC). Ovi servisi su i u prošlosti bili skloni ranjivostima.. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinjenije napade.	BID: 494¹¹⁰³ CVE: CVE-1999-0519¹¹⁰⁴ MSKB: 143474¹¹⁰⁵ URL1¹¹⁰⁶	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost
14.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-ov zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	CVE: CVE-1999-0524¹¹⁰⁷ XF: icmp-netmask(306)¹¹⁰⁸ XF: icmp-timestamp(322)¹¹⁰⁹	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
15.	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (windows-hotfixms06-	Ovo ažuriranje rešava nekoliko otkrivenih i privatno prijavljenih ranjivosti. Preporučuje se da korisnici odmah primene update.	SANS-06 W4¹¹¹⁰ SANS-07 S2¹¹¹¹ CVE CVE-2006-1314¹¹¹² CVE CVE-2006-1315¹¹¹³ MS MS06-035¹¹¹⁴ MSKB 917159¹¹¹⁵	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB917159-x86-ENU.exe (725304 bytes) ¹¹¹⁹

¹¹⁰²http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb893066-v2-x86-enu_3d2029a4300c0b7943b20c1287c8143087045d52.exe

¹⁰⁹⁵<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>

¹⁰⁹⁶<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>

¹⁰⁹⁷<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>

¹⁰⁹⁸<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>

¹⁰⁹⁹<http://secunia.com/advisories/11440/>

¹¹⁰⁰<http://secunia.com/advisories/22341/>

¹¹⁰¹<ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>

¹¹⁰³<http://www.securityfocus.com/bid/494>

¹¹⁰⁴<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>

¹¹⁰⁵<http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>

¹¹⁰⁶http://www.hsc.fr/ressources/presentations/null_sessions/

¹¹⁰⁷<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>

¹¹⁰⁸<http://xforce.iss.net/xforce/xfdb/306>

¹¹⁰⁹<http://xforce.iss.net/xforce/xfdb/322>

¹¹¹⁰<http://www.sans.org/critical-security-controls/#w4>

¹¹¹¹<http://www.sans.org/critical-security-controls/#s2>

¹¹¹²<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1314>

¹¹¹³<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1315>

¹¹¹⁴<http://technet.microsoft.com/en-us/security/bulletin/ms06-035>

¹¹¹⁵<http://support.microsoft.com/default.aspx?scid=kb;EN-US;917159>

035)		SECUNIA 21007 ¹¹¹⁶ XF win-mailslot- bo(26818) ¹¹¹⁷ XF win-smb-information- disclosure(26820) ¹¹¹⁸		

Tabela 45. Windows OS – Pronađeni servisi na IP adresi 172.23.202.105 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni dedljeni resuers, mount-point: C:\
SERVISI	CIFS ¹¹²⁰ , CIFS Name Service ¹¹²¹ : advertised-name-1: WINXPprox86 (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: WINXPprox86 (Logged-on User) advertised-name-4: WINXPprox86 (File Server Service) advertised-name-5: WORKGROUP (Browser Service Elections) mac-address: 000C29EE93C8 DCE RPC interface-uuid: 5A7B91F8-FF00-11D0-A9B2-00C04FB6E6FC interface-version: 1 name: Messenger Service protocol-sequence: ncacn_ip_tcp:172.23.202.105[1025] NTP : 172.23.202.105 udp 123 UPnP-HTTP : 172.23.202.105 tcp 5000

Tabela 46. Windows OS sa IP adresama 172.23.202.115, 172.23.202.116, 172.23.202.100, 172.23.202.99, 172.23.202.98, 172.23.202.97, 172.23.202.96, 172.23.202.95, 172.23.202.94, 172.23.202.93, 172.23.202.92, 172.23.202.91, 172.23.202.90 (2011. godina)

Datum: 20.08.2011	Operativni sistem i ime računara	Broj ranjivosti
IP adresa: 172.23.202.115	OS: : Microsoft Windows 7 Ultimate SP1 x86, WIN7x86ULTSP1	4
IP adresa: 172.23.202.116	OS: : windows 7 ultimate x64, WIN7x64ULT	4
IP adresa: 172.23.202.100	OS: : Windows 7 Home Basic SP1 x64, WIN7x64HoBaSp1	4
IP adresa: 172.23.202.99	OS: : Windows 7 Home Basic SP1 x86, WIN7x86HoBaSp1	4
IP adresa: 172.23.202.98	OS: : Windows 7 Home Premium SP1 x64, WIN7x64HoPreSp1	4

¹¹¹⁹ www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb917159-x86-enu_5ed838e18ceae61a8d94f8c4be2462a8e19212d7.exe

¹¹¹⁶ <http://secunia.com/advisories/21007/>

¹¹¹⁷ <http://xforce.iss.net/xforce/xfdb/26818>

¹¹¹⁸ <http://xforce.iss.net/xforce/xfdb/26820>

¹¹²⁰ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

¹¹²¹ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

IP adresa: 172.23.202.97		OS: : Windows 7 Home Premium SP1 x86, WIN7x86HoPreSp1			4
IP adresa: 172.23.202.96		OS: : Windows 7 Professional SP1 x64, WIN7x64ProSp1			4
IP adresa: 172.23.202.95		OS: : Windows 7 Professional SP1 x86, WIN7x86ProSp1			4
IP adresa: 172.23.202.94		OS: : Windows 7 starter, WIN7starter			4
IP adresa: 172.23.202.93		OS: : Windows 7 Professional N x64, WIN7ProNx64			4
IP adresa: 172.23.202.92		OS: : Windows 7 Professional N x86, WIN7ProNx86			4
IP adresa: 172.23.202.91		OS: : Windows 7 Professional x64, WIN7Prox64			4
IP adresa: 172.23.202.90		OS: : Windows 7 Professional x86, WIN7Prox86			4
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.115:139 172.23.202.115:445 172.23.202.116:139 172.23.202.116:445 172.23.202.100:139 172.23.202.100:445 172.23.202.99:139 172.23.202.99:445 172.23.202.98:139 172.23.202.98:445 172.23.202.97:139 172.23.202.97:445 172.23.202.96:139 172.23.202.96:445 172.23.202.95:139 172.23.202.95:445 172.23.202.94:139 172.23.202.94:445 172.23.202.93:139 172.23.202.93:445 172.23.202.92:139 172.23.202.92:445 172.23.202.91:139 172.23.202.91:445 172.23.202.90:139 172.23.202.90:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB 887429 URL ¹¹²²	Ozbiljan	Metoda za konfiguracije SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429 ¹¹²³ . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing = auto</i> ili da se zahteva SMB potpisivanje: <i>server signing = mandatory</i>
2.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.115:139 172.23.202.115:445 172.23.202.116:139 172.23.202.116:445 172.23.202.100:139 172.23.202.100:445 172.23.202.99:139	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti

¹¹²² <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>¹¹²³ <http://support.microsoft.com/kb/887429>

		172.23.202.99:445 172.23.202.98:139 172.23.202.98:445 172.23.202.97:139 172.23.202.97:445 172.23.202.96:139 172.23.202.96:445 172.23.202.95:139 172.23.202.95:445 172.23.202.94:139 172.23.202.94:445 172.23.202.93:139 172.23.202.93:445 172.23.202.92:139 172.23.202.92:445 172.23.202.91:139 172.23.202.91:445 172.23.202.90:139 172.23.202.90:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.			
3.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-ov zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	OSVDB 95 ¹¹²⁴ CVE: CVE-1999-0524 ¹¹²⁵ XF: icmp-netmask(306) ¹¹²⁶ XF: icmp-timestamp(322) ¹¹²⁷	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost
4.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta (što zlonamerni napadač može iskoristiti pri planiranju daljih napada). Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1 ¹¹²⁸ URL2 ¹¹²⁹ URL3 ¹¹³⁰	Umeren	Onemogućavanje TCP timestamp odgovora na Windows OS. Podesiti Tcp1323Opts vrednost na sledećem ključu na 1: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

Tabela 47. Windows OS – Pronađeni servisi na IP adresi 172.23.202.115 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni dedljeni resuers, mount-point: C:\
SERVISI	CIFS ¹¹³¹ , CIFS Name Service ¹¹³² :

¹¹²⁴ <http://www.osvdb.org/95>¹¹²⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>¹¹²⁶ <http://xforce.iss.net/xforce/xfdb/306>¹¹²⁷ <http://xforce.iss.net/xforce/xfdb/322>¹¹²⁸ http://www.forensicswiki.org/wiki/TCP_timestamps¹¹²⁹ <http://www.ietf.org/rfc/rfc1323.txt>¹¹³⁰ <http://uptime.netcraft.com/>¹¹³¹ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).¹¹³² Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	advertised-name-1: WIN7x86ULTSP1 (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: WIN7x86ULTSP1 (File Server Service) advertised-name-4: WORKGROUP (Browser Service Elections) advertised-name-5: WORKGROUP (Master Browser) advertised-name-6: __MSBROWSE__ (Master Browser) mac-address: 000C297B7546 DCE RPC interface-uuid: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D interface-version: 1 name: D95AFE70-A6D5-4259-822E-2C84DA1DDB0D object-interface-uuid: 765294BA-60BC-48B8-92E9-89FD77769D91 protocol-sequence: ncacn_ip_tcp:172.23.202.115[49152] interface-uuid: 06BBA54A-BE05-49F9-B0A0-30F790261023 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.115[49153] interface-uuid: A398E520-D59A-4BDD-AA7A-3C1E0303A511 interface-version: 1 name: IKE/Authip API protocol-sequence: ncacn_ip_tcp:172.23.202.115[49154] interface-uuid: 12345778-1234-ABCD-EF00-0123456789AC interface-version: 1 name: 12345778-1234-ABCD-EF00-0123456789AC protocol-sequence: ncacn_ip_tcp:172.23.202.115[49155] interface-uuid: 367ABB81-9844-35F1-AD32-98F038001003 interface-version: 2 name: 367ABB81-9844-35F1-AD32-98F038001003 protocol-sequence: ncacn_ip_tcp:172.23.202.115[49156] interface-uuid: 12545678-7234-12CD-EF99-2347456789A1 interface-version: 1 name: IPSec Policy agent endpoint protocol-sequence: ncacn_ip_tcp:172.23.202.115[49158]

Tabela 48. Windows OS – Pronađeni servisi na IP adresi 172.23.202.116 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin)
	C\$ - difoltni dedljeni resuers, mount-point: C:\
SERVISI	CIFS¹¹³³, CIFS Name Service¹¹³⁴ : advertised-name-1: WIN7x64ULT (File Server Service) advertised-name-2: WIN7x64ULT (Computer Name) advertised-name-3: WORKGROUP (Domain Name) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 000C294FA632

¹¹³³ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

¹¹³⁴ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	DCE RPC interface-uuid: D45AFE70-A7D5-7259-832E-2C94DA1D1B1A interface-version: 1 name: D45AFE70-A7D5-7259-832E-2C94DA1D1B1A object-interface-uuid: 665294BA-70BC-58B8-92B9-29FD77769D32 protocol-sequence: ncacn_ip_tcp:172.23.202.116[49152] interface-uuid: 66BBA54B-A305-48F2-C1A0-20F790261024 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.116[49153] interface-uuid: B408E520-B69A-4BCC-CC7A-4C1E0303A534 interface-version: 1 name: IKE/Authip API protocol-sequence: ncacn_ip_tcp:172.23.202.116[49154] interface-uuid: 32845428-2809-B1C1-EC20-1564326759AA interface-version: 1 name: 32845428-2809-B1C1-EC20-1564326759AA protocol-sequence: ncacn_ip_tcp:172.23.202.116[49155] interface-uuid: 467AAA81-6544-99F1-CD31-98F088008008 interface-version: 2 name: 467AAA81-6544-99F1-CD31-98F088008008 protocol-sequence: ncacn_ip_tcp:172.23.202.116[49156] interface-uuid: 96288678-3389-A2A3-AF29-7427547789AB interface-version: 1 name: IPSec Policy agent endpoint protocol-sequence: ncacn_ip_tcp:172.23.202.116[49158]

Tabela 49. Windows OS – Pronađeni servisi na IP adresi 172.23.202.100 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni dedljeni resuers, mount-point: C:\
SERVISI	CIFS ¹¹³⁵ , CIFS Name Service ¹¹³⁶ : advertised-name-1: WIN7x64HoBaSp1 (File Server Service) advertised-name-2: WIN7x64HoBaSp1 (Computer Name) advertised-name-3: WORKGROUP (Domain Name) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 024C294FA985 DCE RPC interface-uuid: A43AFE72-A8D6-6259-852E-1C94DA2D2B2A interface-version: 1 name: A43AFE72-A8D6-6259-852E-1C94DA2D2B2A object-interface-uuid: 569994BA-45BC-79B8-22B9-49FD76909D25 protocol-sequence: ncacn_ip_tcp:172.23.202.100[49152] interface-uuid: 54BBA77B-B705-84F3-C2A0-901F79026102 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.100[49153] interface-uuid: B308F520-F66A-6BCC-AB7BA-3C1E0203C532

¹¹³⁵ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

¹¹³⁶ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	interface-version: 1 name: IKE/Authip API protocol-sequence: ncacn_ip_tcp:172.23.202.100[49154] interface-uuid: 27789428-1553-B2C4-EB23-2564226259A1 interface-version: 1 name: 27789428-1553-B2C4-EB23-2564226259A1 protocol-sequence: ncacn_ip_tcp:172.23.202.100[49155] interface-uuid: 532ABA82-9544-49F1-AD32-34F083002012 interface-version: 2 name: 532ABA82-9544-49F1-AD32-34F083002012 protocol-sequence: ncacn_ip_tcp:172.23.202.100[49156] interface-uuid: 36284678-2389-B7A1-AB22-542B547A89A1 interface-version: 1 name: IPSec Policy agent endpoint protocol-sequence: ncacn_ip_tcp:172.23.202.100[49158]

Tabela 50. Windows OS – Pronađeni servisi na IP adresi 172.23.202.99 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni dedljeni resuers, mount-point: C:\
SERVISI	CIFS¹¹³⁷, CIFS Name Service¹¹³⁸ : advertised-name-1: WIN7x86HoBaSp1 (File Server Service) advertised-name-2: WIN7x86HoBaSp1 (Computer Name) advertised-name-3: WORKGROUP (Domain Name) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 032C294AA682 DCE RPC interface-uuid: C44AFA71-18D4-6359-752A-6C99D12D2B36 interface-version: 1 name: C44AFA71-18D4-6359-752A-6C99D12D2B36 object-interface-uuid: 469387BA-45BA-39B7-42B6-89FD76303D23 protocol-sequence: ncacn_ip_tcp:172.23.202.99[49152] interface-uuid: 34B3A73C-C703-54F1-C1A0-801F79023101 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.99[49153] interface-uuid: 12308F42-166F-3B14-A37B-2C5E0803A549 interface-version: 1 name: IKE/Authip API protocol-sequence: ncacn_ip_tcp:172.23.202.99[49154] interface-uuid: 47589628-3513-B1C8-1B24-456B227259A3 interface-version: 1 name: 47589628-3513-B1C8-1B24-456B227259A3 protocol-sequence: ncacn_ip_tcp:172.23.202.99[49155]

¹¹³⁷ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

¹¹³⁸ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	interface-uuid: 566ABA69-4344-21F3-34DB-5A0354056F12 interface-version: 2 name: 566ABA69-4344-21F3-34DB-5A0354056F12 protocol-sequence: ncacn_ip_tcp:172.23.202.99[49156] interface-uuid: 32A34671-35F4-B6A3-AB48-392B547A76A9 interface-version: 1 name: IPSec Policy agent endpoint protocol-sequence: ncacn_ip_tcp:172.23.202.99[49158]

Tabela 51. Windows OS – Pronađeni servisi na IP adresi 172.23.202.98 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni dedljeni resuers, mount-point: C:\
SERVISI	CIFS¹¹³⁹, CIFS Name Service¹¹⁴⁰ : advertised-name-1: WIN7x64HoPreSp1 (File Server Service) advertised-name-2: WIN7x64HoPreSp1 (Computer Name) advertised-name-3: WORKGROUP (Domain Name) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 72C2457AA682 DCE RPC interface-uuid: 3B4AF321-98D4-5351-732A-9C93D34B2B99 interface-version: 1 name: 3B4AF321-98D4-5351-732A-9C93D34B2B99 object-interface-uuid: 357997BA-33BA-70B7-22B6-20FA76333D66 protocol-sequence: ncacn_ip_tcp:172.23.202.98[49152] interface-uuid: 67B3B22C-B901-34F1-21A0-446F75998122 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.98[49153] interface-uuid: 5379F224-985F-3B23-A97C-4B6F0603A341 interface-version: 1 name: IKE/Authip API protocol-sequence: ncacn_ip_tcp:172.23.202.98[49154] interface-uuid: 63987721-2316-B1C9-1B34-779B238199A1 interface-version: 1 name: 63987721-2316-B1C9-1B34-779B238199A1 protocol-sequence: ncacn_ip_tcp:172.23.202.98[49155] interface-uuid: 48FAEA45-3790-32F3-38DB-4A0324049F11 interface-version: 2 name: 48FAEA45-3790-32F3-38DB-4A0324049F11 protocol-sequence: ncacn_ip_tcp:172.23.202.98[49156] interface-uuid: 56A37901-67F4-B1A2-AB56-598B547A22A3 interface-version: 1 name: IPSec Policy agent endpoint protocol-sequence: ncacn_ip_tcp:172.23.202.98[49158]

¹¹³⁹ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

¹¹⁴⁰ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

Tabela 52. Windows OS – Pronađeni servisi na IP adresi 172.23.202.97 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni dedljeni resuers, mount-point: C:\
SERVISI	CIFS¹¹⁴¹, CIFS Name Service¹¹⁴² : advertised-name-1: WIN7x86HoPreSp1 (File Server Service) advertised-name-2: WIN7x86HoPreSp1 (Computer Name) advertised-name-3: WORKGROUP (Domain Name) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 32C2457BA634 DCE RPC interface-uuid: 2B4AF221-28D4-2351-132A-1C93D31B2B91 interface-version: 1 name: 2B4AF221-28D4-2351-132A-1C93D31B2B91 object-interface-uuid: 446699BA-27BA-50B7-29B6-20AB76348D23 protocol-sequence: ncacn_ip_tcp:172.23.202.97[49152] interface-uuid: 33B3B11C-B380-33F1-29A0-16F759543256 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.97[49153] interface-uuid: 8901F234-345F-3B56-A97B-2B6F0629A342 interface-version: 1 name: IKE/Authip API protocol-sequence: ncacn_ip_tcp:172.23.202.97[49154] interface-uuid: 3619482A-2669-B1C1-3B34-446B227912A3 interface-version: 1 name: 3619482A-2669-B1C1-3B34-446B227912A3 protocol-sequence: ncacn_ip_tcp:172.23.202.97[49155] interface-uuid: 57F1E145-2590-59F3-58DB-4A0327655F12 interface-version: 2 name: 257F1E145-2590-59F3-58DB-4A0327655F12 protocol-sequence: ncacn_ip_tcp:172.23.202.97[49156] interface-uuid: 90A64236-17B4-C1A3-1B56-125B547A48A9 interface-version: 1 name: IPSec Policy agent endpoint protocol-sequence: ncacn_ip_tcp:172.23.202.97[49158]

Tabela 53. Windows OS – Pronađeni servisi na IP adresi 172.23.202.96 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni dedljeni resuers, mount-point: C:\
SERVISI	CIFS¹¹⁴³,

¹¹⁴¹ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

¹¹⁴² Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	CIFS Name Service¹¹⁴⁴ : advertised-name-1: WIN7x64ProSp1 (File Server Service) advertised-name-2: WIN7x64ProSp1 (Computer Name) advertised-name-3: WORKGROUP (Domain Name) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 45B2427CA321 DCE RPC interface-uuid: 3F5AF359-31D4-3880-217A-2B93A26B2B22 interface-version: 1 name: 3F5AF359-31D4-3880-217A-2B93A26B2B22 object-interface-uuid: 356399EA-34BB-32B7-38B6-12AB21698D21 protocol-sequence: ncacn_ip_tcp:172.23.202.96[49152] interface-uuid: 67B2B12C-A216-21C1-34A1-18F32695B235 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.96[49153] interface-uuid: 35689F256-321F-3B79-A13A-2A6F2765A219 interface-version: 1 name: IKE/Authip API protocol-sequence: ncacn_ip_tcp:172.23.202.96[49154] interface-uuid: 5438869A-2168-B2C4-1B31-399B232890A1 interface-version: 1 name: 5438869A-2168-B2C4-1B31-399B232890A1 protocol-sequence: ncacn_ip_tcp:172.23.202.96[49155] interface-uuid: 448A1A126-37A1-37F2-28DB-2A3764952F23 interface-version: 2 name: 448A1A126-37A1-37F2-28DB-2A3764952F23 protocol-sequence: ncacn_ip_tcp:172.23.202.96[49156] interface-uuid: 69A37976-30B4-C2A9-1B32-327B498A28A1 interface-version: 1 name: IPSec Policy agent endpoint protocol-sequence: ncacn_ip_tcp:172.23.202.96[49158]

Tabela 54. Windows OS – Pronađeni servisi na IP adresi 172.23.202.95 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni dedljeni resuers, mount-point: C:\
SERVISI	CIFS¹¹⁴⁵, CIFS Name Service¹¹⁴⁶ : advertised-name-1: WIN7x86ProSp1 (File Server Service) advertised-name-2: WIN7x86ProSp1 (Computer Name) advertised-name-3: WORKGROUP (Domain Name) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 34B2479CA346 DCE RPC

¹¹⁴³ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

¹¹⁴⁴ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

¹¹⁴⁵ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

¹¹⁴⁶ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	interface-uuid: 6A5AB267-45A4-2680-215A-4B94A25C2B53 interface-version: 1 name: 6A5AB267-45A4-2680-215A-4B94A25C2B53 object-interface-uuid: 358332A1-671B-1B47-78B1-19AB32189D22 protocol-sequence: ncacn_ip_tcp:172.23.202.95[49152] interface-uuid: 237B5B1A-C211-43C2-15A1-67F33481B752 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.95[49153] interface-uuid: 4331C239-987F-3B32-A911-3B7F2765A344 interface-version: 1 name: IKE/Authip API protocol-sequence: ncacn_ip_tcp:172.23.202.95[49154] interface-uuid: 6792145A-3890-B1C1-1C32-337B233161A2 interface-version: 1 name: 6792145A-3890-B1C1-1C32-337B233161A2 protocol-sequence: ncacn_ip_tcp:172.23.202.95[49155] interface-uuid: 76A1E399-59A1-67A1-23DC-1A3464942F79 interface-version: 2 name: 76A1E399-59A1-67A1-23DC-1A3464942F79 protocol-sequence: ncacn_ip_tcp:172.23.202.95[49156] interface-uuid: 39A34941-28C1-A2A2-2B99-479B266A28A9 interface-version: 1 name: IPSec Policy agent endpoint protocol-sequence: ncacn_ip_tcp:172.23.202.95[49158]

Tabela 55. Windows OS – Pronađeni servisi na IP adresi 172.23.202.94 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin)
	C\$ - difoltni dedljeni resuers, mount-point: C:\
SERVISI	CIFS¹¹⁴⁷, CIFS Name Service¹¹⁴⁸ : advertised-name-1: WIN7starter (File Server Service) advertised-name-2: WIN7starter (Computer Name) advertised-name-3: WORKGROUP (Domain Name) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 24A2576CA649 DCE RPC interface-uuid: 4A51B238-25A4-4723-985A-1B93A23C2B31 interface-version: 1 name: 4A51B238-25A4-4723-985A-1B93A23C2B31 object-interface-uuid: 622543B2-329B-2B98-23B1-36AB67831D45 protocol-sequence: ncacn_ip_tcp:172.23.202.94[49152] interface-uuid: 378B5B11-3211-45C1-57A3-78F21693B754 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.94[49153] interface-uuid: 6921C239-456F-3B98-A921-3A5F2789A214 interface-version: 1 name: IKE/Authip API

¹¹⁴⁷ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

¹¹⁴⁸ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	protocol-sequence: ncacn_ip_tcp:172.23.202.94[49154] interface-uuid: 435789B1-B810-C424-1C65-1327B23456B1 interface-version: 1 name: 435789B1-B810-C424-1C65-1327B23456B1 protocol-sequence: ncacn_ip_tcp:172.23.202.94[49155] interface-uuid: 43A2E344-42A1-57A1-32DC-7A2352A52F19 interface-version: 2 name: 43A2E344-42A1-57A1-32DC-7A2352A52F19 protocol-sequence: ncacn_ip_tcp:172.23.202.94[49156] interface-uuid: 45A23741-3211-12A2-269B-328A4B6A28A9 interface-version: 1 name: IPSec Policy agent endpoint protocol-sequence: ncacn_ip_tcp:172.23.202.94[49158]

Tabela 56. Windows OS – Pronađeni servisi na IP adresi 172.23.202.93 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni dedljeni resuers, mount-point: C:\
SERVISI	CIFS¹¹⁴⁹, CIFS Name Service¹¹⁵⁰ : advertised-name-1: WIN7ProNx64 (File Server Service) advertised-name-2: WIN7ProNx64 (Computer Name) advertised-name-3: WORKGROUP (Domain Name) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 56A792CA233 DCE RPC interface-uuid: 2A45B324-32A4-5682-324A-2B322232A2B3 interface-version: 1 name: 2A45B324-32A4-5682-324A-2B322232A2B3 object-interface-uuid: 529401B2-325B-2181-32B1-76AB73725D21 protocol-sequence: ncacn_ip_tcp:172.23.202.93[49152] interface-uuid: 451B5A12-7859-32C1-76A1-32F23744B767 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.93[49153] interface-uuid: 8489C213-989F-3B34-A127-8A8F2289A222 interface-version: 1 name: IKE/Authip API protocol-sequence: ncacn_ip_tcp:172.23.202.93[49154] interface-uuid: 679922B1-B236-C779-1C32-4471B26722B4 interface-version: 1 name: 679922B1-B236-C779-1C32-4471B26722B4 protocol-sequence: ncacn_ip_tcp:172.23.202.93[49155] interface-uuid: 87A2E231-53A1-89A1-12DC-2A2252A42F84 interface-version: 2 name: 87A2E231-53A1-89A1-12DC-2A2252A42F84 protocol-sequence: ncacn_ip_tcp:172.23.202.93[49156] interface-uuid: 15A83880-2030-32A2-589B-229A4B6A54A1 interface-version: 1

¹¹⁴⁹ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

¹¹⁵⁰ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	name: IPSec Policy agent endpoint protocol-sequence: ncacn_ip_tcp:172.23.202.93[49158]

Tabela 57. Windows OS – Pronađeni servisi na IP adresi 172.23.202.92 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni dedljeni resuers, mount-point: C:\
SERVISI	CIFS¹¹⁵¹, CIFS Name Service¹¹⁵² : advertised-name-1: WIN7ProNx86 (File Server Service) advertised-name-2: WIN7ProNx86 (Computer Name) advertised-name-3: WORKGROUP (Domain Name) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 42A447CA379 DCE RPC interface-uuid: 1A41B321-12A4-1682-314A-1B324382A2C7 interface-version: 1 name: 1A41B321-12A4-1682-314A-1B324382A2C7 object-interface-uuid: 369227B2-125B-6161-62B1-90AB73349D33 protocol-sequence: ncacn_ip_tcp:172.23.202.92[49152] interface-uuid: 328B5A12-3853-30C1-70A1-30F23004B436 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.92[49153] interface-uuid: 4488C213-109F-3B04-A107-4A8F2009A210 interface-version: 1 name: IKE/Authip API protocol-sequence: ncacn_ip_tcp:172.23.202.92[49154] interface-uuid: 599021B1-B399-C022-1B44-6098B06504B1 interface-version: 1 name: 599021B1-B399-C022-1B44-6098B06504B1 protocol-sequence: ncacn_ip_tcp:172.23.202.92[49155] interface-uuid: 50A2E400-54A2-88A1-26DC-3A2000A41F77 interface-version: 2 name: 50A2E400-54A2-88A1-26DC-3A2000A41F77 protocol-sequence: ncacn_ip_tcp:172.23.202.92[49156] interface-uuid: 32A34090-2B12-12A4-784B-226A4B6A12A7 interface-version: 1 name: IPSec Policy agent endpoint protocol-sequence: ncacn_ip_tcp:172.23.202.92[49158]

Tabela 58. Windows OS – Pronađeni servisi na IP adresi 172.23.202.91 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni dedljeni resuers, mount-point: C:\
SERVISI	CIFS¹¹⁵³,

¹¹⁵¹ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

¹¹⁵² Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	CIFS Name Service¹¹⁵⁴ : advertised-name-1: WIN7Prox64 (File Server Service) advertised-name-2: WIN7Prox64 (Computer Name) advertised-name-3: WORKGROUP (Domain Name) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 46A437BC556 DCE RPC interface-uuid: 2458B320-32A4-1333-678A-1B310960A2C4 interface-version: 1 name: 2458B320-32A4-1333-678A-1B310960A2C4 object-interface-uuid: 578220B2-555B-8861-45B1-71AB45501D22 protocol-sequence: ncacn_ip_tcp:172.23.202.91[49152] interface-uuid: 442C4A11-5078-21C1-76A1-34F23224B400 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.91[49153] interface-uuid: 4309B212-111F-3B30-A132-7A8F3017A312 interface-version: 1 name: IKE/Authip API protocol-sequence: ncacn_ip_tcp:172.23.202.91[49154] interface-uuid: 697021B1-B494-A012-1B14-1098B01504C2 interface-version: 1 name: 697021B1-B494-A012-1B14-1098B01504C2 protocol-sequence: ncacn_ip_tcp:172.23.202.91[49155] interface-uuid: 46A2A410-32A2-44A1-21DA-6A3255A41F56 interface-version: 2 name: 46A2A410-32A2-44A1-21DA-6A3255A41F56 protocol-sequence: ncacn_ip_tcp:172.23.202.91[49156] interface-uuid: 12D33266-1B10-10A4-654B-220A4B3A12D1 interface-version: 1 name: IPSec Policy agent endpoint protocol-sequence: ncacn_ip_tcp:172.23.202.91[49158]

Tabela 59. Windows OS – Pronađeni servisi na IP adresi 172.23.202.90 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni dedljeni resuers, mount-point: C:\
SERVISI	CIFS¹¹⁵⁵, CIFS Name Service¹¹⁵⁶ : advertised-name-1: WIN7Prox86 (File Server Service) advertised-name-2: WIN7Prox86 (Computer Name) advertised-name-3: WORKGROUP (Domain Name) advertised-name-4: WORKGROUP (Browser Service Elections) mac-address: 53AA782C991 DCE RPC

¹¹⁵³ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

¹¹⁵⁴ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

¹¹⁵⁵ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

¹¹⁵⁶ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

interface-uuid: 4290B1668-17A4-2890-110A-4A215890A1B1 interface-version: 1 name: 4290B1668-17A4-2890-110A-4A215890A1B1 object-interface-uuid: 343245B2-344B-2200-32B8-21BD33779B29 protocol-sequence: ncacn_ip_tcp:172.23.202.90[49152] interface-uuid: 909C4223-3388-34C9-23A1-66F24190B245 interface-version: 1 name: Security Center protocol-sequence: ncacn_ip_tcp:172.23.202.90[49153] interface-uuid: 4799B631-700F-1B30-A144-4A8F4017A417 interface-version: 1 name: IKE/Authip API protocol-sequence: ncacn_ip_tcp:172.23.202.90[49154] interface-uuid: 559901C1-C556-A230-1B28-2867B54344B4 interface-version: 1 name: 559901C1-C556-A230-1B28-2867B54344B4 protocol-sequence: ncacn_ip_tcp:172.23.202.90[49155] interface-uuid: 76A2A890-21A2-56A1-78DA-2A7844A41A32 interface-version: 2 name: 76A2A890-21A2-56A1-78DA-2A7844A41A32 protocol-sequence: ncacn_ip_tcp:172.23.202.90[49156] interface-uuid: 50D45334-1C20-20A4-254B-667B4B1A11D1 interface-version: 1 name: IPSec Policy agent endpoint protocol-sequence: ncacn_ip_tcp:172.23.202.90[49158]	

Tabela 60. Windows OS sa IP adresama 172.23.202.118 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.118		OS: Microsoft Windows server 2008 Enterprise R2 SP1 x64 Updated Jun 2011, 2008entR2X64SP1			4
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.118:139 172.23.202.118:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje omogućava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB 887429 URL1 ¹¹⁵⁷	Ozbiljan	Metoda za konfiguracije SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429 ¹¹⁵⁸ . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing = auto</i> ili da se zahteva SMB potpisivanje: <i>server signing = mandatory</i> .
2.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.118:139 172.23.202.118:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti

¹¹⁵⁷ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>¹¹⁵⁸ <http://support.microsoft.com/kb/887429>

3.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-ov zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	OSVDB 95 ¹¹⁵⁹ CVE: CVE-1999-0524 ¹¹⁶⁰ XF: icmp-netmask(306) ¹¹⁶¹ XF: icmp-timestamp(322) ¹¹⁶²	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost
4.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta (što zlonamerni napadač može iskoristiti pri planiranju daljih napada). Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1 ¹¹⁶³ URL2 ¹¹⁶⁴ URL3 ¹¹⁶⁵	Umeren	Onemogućavanje TCP timestamp odgovora na Windows OS. Podesiti Tcp1323Opts vrednost na sledećem ključu na 1: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

Tabela 61. Windows OS – Pronađeni servisi na IP adresi 172.23.202.118 (2011. godina)

FAJLOVI I DIREKTORIJUMI	ADMIN\$ - (remote admin) C\$ - difoltni dedljeni resuers, mount-point: C:\
SERVISI	CIFS¹¹⁶⁶, CIFS Name Service¹¹⁶⁷ : advertised-name-1: 2008entR2X64SP1 (File Server Service) advertised-name-2: 2008entR2X64SP1 (Computer Name) advertised-name-3: WORKGROUP (Domain Name) mac-address: 000C29AEE95B DCE RPC interface-uuid: A96AFE77-B6D4-7259-722E-7C42DA1AAB12 interface-version: 1 name: A96AFE77-B6D4-7259-722E-7C42DA1AAB12 object-interface-uuid: 432778BA-20BC-28B8-55E9-89FD77769D91 protocol-sequence: ncacn_ip_tcp:172.23.202.118[49152] interface-uuid: C23411C5-A0A1-218B-BBA1-3CE01EB0A2D2 interface-version: 1 name: DHCPv6 Client LRPC Endpoint protocol-sequence: ncacn_ip_tcp:172.23.202.118[49153] interface-uuid: A408E331-D21A-4BAA-117A-1B1E034A512 interface-version: 1

¹¹⁵⁹ <http://www.osvdb.org/95>¹¹⁶⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>¹¹⁶¹ <http://xforce.iss.net/xforce/xfdb/306>¹¹⁶² <http://xforce.iss.net/xforce/xfdb/322>¹¹⁶³ http://www.forensicswiki.org/wiki/TCP_timestamps¹¹⁶⁴ <http://www.ietf.org/rfc/rfc1323.txt>¹¹⁶⁵ <http://uptime.netcraft.com/>¹¹⁶⁶ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).¹¹⁶⁷ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	name: IKE/Authip API protocol-sequence: ncacn_ip_tcp:172.23.202.118[49154] interface-uuid: 390AB232-2223-15F1-1D32-23F038001003 interface-version: 2 name: 390AB232-2223-15F1-1D32-23F038001003 protocol-sequence: ncacn_ip_tcp:172.23.202.118[49155] interface-uuid: 45622301-9302-A12C-12AA-29002917A2AC interface-version: 1 name: 45622301-9302-A12C-12AA-29002917A2AC protocol-sequence: ncacn_ip_tcp:172.23.202.118[49156] interface-uuid: 83839201-2233-12BB-EF12-2393472623AB interface-version: 1 name: IPSec Policy agent endpoint protocol-sequence: ncacn_ip_tcp:172.23.202.118[49158]

Tabela 62. Windows OS sa IP adresama 172.23.202.103 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.103		OS: Windows 98 se, WIN98SE			3
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	172.23.202.103:135: Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183 ¹¹⁶⁸ CERT-VN: 415294 ¹¹⁶⁹ CVE CVE-2004-0230 ¹¹⁷⁰ MS: MS05-019 ¹¹⁷¹ MS: MS06-064 ¹¹⁷² NETBSD: NetBSD-SA2004-006 ¹¹⁷³ OVAL: OVAL2689 ¹¹⁷⁴ OVAL: OVAL270 ¹¹⁷⁵ OVAL OVAL3508 ¹¹⁷⁶ OVAL OVAL4791 ¹¹⁷⁷ OVAL OVAL5711 ¹¹⁷⁸ SECUNIA: 11440 ¹¹⁷⁹ SECUNIA: 22341 ¹¹⁸⁰ SGI 20040403-01-A ¹¹⁸¹	Ozbiljan	Nema adekvatne zakrpe osim osim blokiranja porta 135. Rešenje je da se ažurira sistem novijom verzijom.
2.	ICMP netmask response (generic-icmp-netmask)	Received ICMP netmask response [255.255.255.0] from 172.23.202.103 Udaljeni host je odgovorio na ICMP-ov netmask zahtev. ICMP netmask odgovor sadrži mrežnu masku (network mask) udaljenog host-a (na mestu na kojem je obrađen zahtev).	CVE CVE-1999-0524 OSVDB 95 XF icmp-netmask(306) XF icmp-timestamp(322)	Umeren	Konfigurisati fajervol tako da blokira ulazne i izlazne ICMP pakete sa ICMP tipovima 17 (netmask zahtev) i 18 (netmask odgovor).

¹¹⁶⁸ <http://www.securityfocus.com/bid/10183>¹¹⁶⁹ <http://www.kb.cert.org/vuls/id/415294>¹¹⁷⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>¹¹⁷¹ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>¹¹⁷² <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>¹¹⁷³ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>¹¹⁷⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>¹¹⁷⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>¹¹⁷⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>¹¹⁷⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>¹¹⁷⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>¹¹⁷⁹ <http://secunia.com/advisories/11440/>¹¹⁸⁰ <http://secunia.com/advisories/22341/>¹¹⁸¹ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>

		Ovu informaciju zlonamerni napadač može da iskoristi sa ciljem preciznijeg mapiranja strukture interne mreže. Takođe je moguće otkriti mrežne adrese koje se koriste, kao i informacije o ruterima koji su zaduženi za interne mreže. Zlonamernim napadačima je ovom ranjivošću olakšana realizacija napada "SMURF attack" (SMURF napad), koristeći usmerene broadcast ICMP ping pakete.			
3.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-ov zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	OSVDB 95 ¹¹⁸² CVE: CVE-1999-0524 ¹¹⁸³ XF: icmp-netmask(306) ¹¹⁸⁴ XF: icmp-timestamp(322) ¹¹⁸⁵	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost

Tabela 63. Windows OS – Pronađeni servisi na IP adresi 172.23.202.103 (2011. godina)

SERVISI	CIFS ¹¹⁸⁶ , CIFS Name Service ¹¹⁸⁷ : advertised-name-1: WIN98SE (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: WIN98SE (Logged-on User) mac-address: 000C29882E7D

Tabela 64. Windows OS sa IP adresama 172.23.202.104 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.104		OS: Windows ME, WINME			2
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti

¹¹⁸² <http://www.osvdb.org/95>¹¹⁸³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>¹¹⁸⁴ <http://xforce.iss.net/xforce/xfdb/306>¹¹⁸⁵ <http://xforce.iss.net/xforce/xfdb/322>¹¹⁸⁶ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).¹¹⁸⁷ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

1.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	172.23.202.104:135: Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183 ¹¹⁸⁸ CERT TA04-111A ¹¹⁸⁹ CERT-VN: 415294 ¹¹⁹⁰ CVE CVE-2004-0230 ¹¹⁹¹ MS: MS05-019 ¹¹⁹² MS: MS06-064 ¹¹⁹³ NETBSD: NetBSD-SA2004-006 ¹¹⁹⁴ OVAL: OVAL2689 ¹¹⁹⁵ OVAL: OVAL270 ¹¹⁹⁶ OVAL OVAL3508 ¹¹⁹⁷ OVAL OVAL4791 ¹¹⁹⁸ OVAL OVAL5711 ¹¹⁹⁹ SECUNIA: 11440 ¹²⁰⁰ SECUNIA: 22341 ¹²⁰¹ SECUNIA 11458 ¹²⁰² SGI 20040403-01-A ¹²⁰³ XF tcp-rst-dos(15886) ¹²⁰⁴ URL1 ¹²⁰⁵ URL2 ¹²⁰⁶	Ozbiljan	Nema adekvatne zakrpe osim osim blokiranja porta 135. Rešenje je da se ažurira sistem novijom verzijom.
2.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-ov zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	OSVDB 95 ¹²⁰⁷ CVE: CVE-1999-0524 ¹²⁰⁸ XF: icmp-netmask(306) ¹²⁰⁹ XF: icmp-timestamp(322) ¹²¹⁰	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.

Tabela 65. Windows OS – Pronađeni servisi na IP adresi 172.23.202.104 (2011. godina)

SERVISI	CIFS ¹²¹¹ , CIFS Name Service ¹²¹² :

¹¹⁸⁸ <http://www.securityfocus.com/bid/10183>¹¹⁸⁹ <http://www.us-cert.gov/ncas/alerts/ta04-111a>¹¹⁹⁰ <http://www.kb.cert.org/vuls/id/415294>¹¹⁹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>¹¹⁹² <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>¹¹⁹³ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>¹¹⁹⁴ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>¹¹⁹⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>¹¹⁹⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>¹¹⁹⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>¹¹⁹⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>¹¹⁹⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>¹²⁰⁰ <http://secunia.com/advisories/11440/>¹²⁰¹ <http://secunia.com/advisories/22341/>¹²⁰² <http://secunia.com/advisories/11458/>¹²⁰³ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>¹²⁰⁴ <http://xforce.iss.net/xforce/xfdb/15886>¹²⁰⁵ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>¹²⁰⁶ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>¹²⁰⁷ <http://www.osvdb.org/95>¹²⁰⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>¹²⁰⁹ <http://xforce.iss.net/xforce/xfdb/306>¹²¹⁰ <http://xforce.iss.net/xforce/xfdb/322>¹²¹¹ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

	advertised-name-1: WINME (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: WINME (Logged-on User) advertised-name-4: VANJA (Logged-on User) mac-address: 000C29DB0AE2

Tabela 66. Windows OS sa IP adresama 172.23.202.102 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.102		OS: Microsoft Windows 95 OSR 2.5, WIN95osr25			2
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	172.23.202.102:135: Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183 ¹²¹³ CERT TA04-111A ¹²¹⁴ CERT-VN: 415294 ¹²¹⁵ CVE CVE-2004-0230 ¹²¹⁶ MS: MS05-019 ¹²¹⁷ MS: MS06-064 ¹²¹⁸ NETBSD: NetBSD-SA2004-006 ¹²¹⁹ OVAL: OVAL2689 ¹²²⁰ OVAL: OVAL270 ¹²²¹ OVAL OVAL3508 ¹²²² OVAL OVAL4791 ¹²²³ OVAL OVAL5711 ¹²²⁴ SECUNIA: 11440 ¹²²⁵ SECUNIA: 22341 ¹²²⁶ SECUNIA 11458 ¹²²⁷ SGI 20040403-01-A ¹²²⁸ XF tcp-rst-dos(15886) ¹²²⁹ URL1 ¹²³⁰ URL2 ¹²³¹	Ozbiljan	Nema adekvatne zakrpe osim osim blokiranja porta 135. Rešenje je da se ažurira sistem novijom verzijom.
2.	ICMP netmask response (generic-icmp-netmask)	Received ICMP netmask response [255.255.255.0] from 172.23.202.102 Udaljeni host je odgovorio na ICMP-ov netmask zahtev. ICMP netmask odgovor sadrži mrežnu masku (network mask) udaljenog host-a (na mestu na kojem je obrađen zahtev). Ovu informaciju zlonamerni napadač	CVE CVE-1999-0524 OSVDB 95 XF icmp-netmask(306) XF icmp-timestamp(322)	Umeren	Konfigurisati fajervol tako da blokira ulazne i izlazne ICMP pakete sa ICMP tipovima 17 (netmask zahtev) i 18 (netmask odgovor).

¹²¹² Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

¹²¹³ <http://www.securityfocus.com/bid/10183>

¹²¹⁴ <http://www.us-cert.gov/ncas/alerts/ta04-111a>

¹²¹⁵ <http://www.kb.cert.org/vuls/id/415294>

¹²¹⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>

¹²¹⁷ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>

¹²¹⁸ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>

¹²¹⁹ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>

¹²²⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>

¹²²¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>

¹²²² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>

¹²²³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>

¹²²⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>

¹²²⁵ <http://secunia.com/advisories/11440/>

¹²²⁶ <http://secunia.com/advisories/22341/>

¹²²⁷ <http://secunia.com/advisories/11458/>

¹²²⁸ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>

¹²²⁹ <http://xforce.iss.net/xforce/xfdb/15886>

¹²³⁰ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>

¹²³¹ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>

		može da iskoristi sa ciljem preciznijeg mapiranja strukture interne mreže. Takođe je moguće otkriti mrežne adrese koje se koriste, kao i informacije o ruterima koji su zaduženi za interne mreže. Zlonamernim napadačima je ovom ranjivošću olakšana realizacija napada "SMURF attack" (SMURF napad), koristeći usmerene broadcast ICMP ping pakete.			

Tabela 67. Windows OS – Pronađeni servisi na IP adresi 172.23.202.102 (2011. godina)

SERVISI	CIFS¹²³², CIFS Name Service¹²³³ : advertised-name-1: WIN95osr25 (Computer Name) advertised-name-2: WORKGROUP (Domain Name) advertised-name-3: WIN95osr25 (Logged-on User) advertised-name-4: VANJA (Logged-on User) mac-address: 000C29354588

4.3.2 LINUX OPERATIVNI SISTEMI - SKENIRANJE SERVISA NA RANJIVOSTI U 2011.

Osim difoltne instalacije, dodati su apache, mysql, php, tomcat (kod nekih) ssh ftp servisi koji su difoltno instalirani.

Tabela 68. Linux OS sa IP adresama 172.23.202.124, 172.23.202.220 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.124		OS: Mandriva Linux Enterprise Server 5.2 x86, mandriva52enx86			43
IP adresa: 172.23.202.220		OS: Mandriva Linux Enterprise Server 5.2 x64, mandriva52enx64			43
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti

¹²³² CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

¹²³³ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

1.	Apache httpd mod_isapi module unload flaw (CVE-2010-0425) (apache-httpd-2_2_x-mod_isapi-moduleunload-flaw-cve-2010-0425)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 U modulu mod_isapi je pronađen propust, koji će pokušati da ukloni ISAPI dll kada naiđe na greške. To može ostaviti povratne pozive u nedefinisano stanju i kao posledica može da se javi segmentation fault. Na Windows platformama koje koriste mod_isapi, udaljeni napadač bi mogao da pošalje zlonameran zahtev da pokrene ovaj problem, a kako win32 MPM pokreće samo jedan proces, to bi kao ishod imalo odbijanje servisa i potencijalno dozvolilo da se pokrene proizvoljan kôd. Napomena: Zahvaljujući Brett Gervasoni-ju iz "Sense of Security" ovaj problem je prijavljen i za njega je predložena zakrpa.	BID 38494 ¹²³⁴ CERT-VN 280613 ¹²³⁵ CVE CVE-2010-0425 ¹²³⁶ OVAL OVAL8439 ¹²³⁷ SECUNIA 38978 ¹²³⁸ SECUNIA 39628 ¹²³⁹ URL1 ¹²⁴⁰ XF apache-http-modisapi-ocp- unspecified(56624) ¹²⁴¹	Kritičan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz
2.	Apache httpd APR apr_palloc heap overflow (CVE-2009-2412) (http-apache-apr_palloc-heap-overflow)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 U modulu apr_palloc() je pronađen propust u sklopu APR-a, koji može prouzrokovati velika preopterećenja u programima koji pokušaju da kontrolišu apr_palloc() veličinu zadatu od strane korisnika. Sam Apache HTTP server ne dopušta prolaz ka ovoj funkciji neproverenim veličinama koje zadaje korisnik, tako da se on može pokrenuti samo preko neke druge aplikacije koja koristi apr_palloc() na ranjiv način.	APPLE APPLE-SA-2009-11-09 ¹²⁴² BID 35949 ¹²⁴³ CVE CVE-2009-2412 ¹²⁴⁴ OSVDB 56765 ¹²⁴⁵ OSVDB 56766 ¹²⁴⁶ OVAL OVAL8394 ¹²⁴⁷ OVAL OVAL9958 ¹²⁴⁸ SECUNIA 36138 ¹²⁴⁹ SECUNIA 36140 ¹²⁵⁰ SECUNIA 36166 ¹²⁵¹ SECUNIA 36233 ¹²⁵² SECUNIA 37152 ¹²⁵³ SECUNIA 37221 ¹²⁵⁴ SUSE SUSE-SA:2009:050 ¹²⁵⁵ URL1 ¹²⁵⁶	Kritičan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.13.tar.gz
3.	Apache httpd mod_proxy_ftp FTP command injection	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80	APPLE APPLE-SA-2010-03-29 ¹²⁵⁷ CVE CVE-2009-3095 ¹²⁵⁸	Kritičan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati:

¹²³⁴ <http://www.securityfocus.com/bid/38494>¹²³⁵ <http://www.kb.cert.org/vuls/id/280613>¹²³⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0425>¹²³⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8439>¹²³⁸ <http://secunia.com/advisories/38978/>¹²³⁹ <http://secunia.com/advisories/39628/>¹²⁴⁰ http://httpd.apache.org/security/vulnerabilities_22.html¹²⁴¹ <http://xforce.iss.net/xforce/xfdb/56624>¹²⁴² <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>¹²⁴³ <http://www.securityfocus.com/bid/35949>¹²⁴⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2412>¹²⁴⁵ <http://osvdb.org/56765>¹²⁴⁶ <http://osvdb.org/56766>¹²⁴⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8394>¹²⁴⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9958>¹²⁴⁹ <http://secunia.com/advisories/36138/>¹²⁵⁰ <http://secunia.com/advisories/36140/>¹²⁵¹ <http://secunia.com/advisories/36166/>¹²⁵² <http://secunia.com/advisories/36233/>¹²⁵³ <http://secunia.com/advisories/37152/>¹²⁵⁴ <http://secunia.com/advisories/37221/>¹²⁵⁵ <https://www.suse.com/support/security/advisories/>¹²⁵⁶ http://httpd.apache.org/security/vulnerabilities_22.html¹²⁵⁷ <http://lists.apple.com/archives/security-announce/2010/Mar/msg00001.html>¹²⁵⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3095>

	(CVE-2009-3095) (apache-httpd-2.2.xmod_proxy_ftp-ftp-command-injection-cve-2009-3095)	172.23.202.220:443 U modulu mod_proxy_ftp je pronađen propust. U reverznoj proxy konfiguraciji, udaljeni napadač bi mogao da iskoristi ovaj defekt da zaobiđe uobičajenu zabranu pristupa tako što bi kreirao pažljivo izrađen HTTP Authorization heder, koji omogućava napadaču da šalje proizvoljne komande FTP serveru.	DEBIAN DSA-1934 ¹²⁵⁹ OVAL OVAL8662 ¹²⁶⁰ OVAL OVAL9363 ¹²⁶¹ SECUNIA 37152 ¹²⁶² SUSE- SA:2009:050 ¹²⁶³ URL1 ¹²⁶⁴		http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.gz
4.	Apache httpd APR-util XML DoS (CVE-2009-1955) (http-apache-apr-util-xml-dos)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Ranjivost na DOS napad otkrivena je u sklopu kopije kompleta APR-util library Extensible Markup Language (XML) prevodioca (eng. parser). Udaljeni napadač bi mogao da kreira posebno izrađen XML dokument koji bi prouzrokovao ogromno zauzeće memorije kada ga procesira XML decoding engine.	APPLE APPLE-SA-2009-11-09 ¹²⁶⁵ BID 35253 ¹²⁶⁶ CVE CVE-2009-1955 ¹²⁶⁷ DEBIAN DSA-1812 ¹²⁶⁸ OVAL OVAL10270 ¹²⁶⁹ REDHAT RHSA-2009:1107 ¹²⁷⁰ REDHAT RHSA-2009:1108 ¹²⁷¹ SECUNIA 34724 ¹²⁷² SECUNIA 35284 ¹²⁷³ SECUNIA 35360 ¹²⁷⁴ SECUNIA 35395 ¹²⁷⁵ SECUNIA 35444 ¹²⁷⁶ SECUNIA 35487 ¹²⁷⁷ SECUNIA 35565 ¹²⁷⁸ SECUNIA 35710 ¹²⁷⁹ SECUNIA 35797 ¹²⁸⁰ SECUNIA 35843 ¹²⁸¹ SECUNIA 36473 ¹²⁸² SECUNIA 37221 ¹²⁸³ URL1 ¹²⁸⁴	Kritičan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz
5.	HTTP Basic Authentication Enabled (http-basic-auth-cleartext)	172.23.202.124:8080 172.23.202.220:8080 HTTP Basic Authentication šema se ne smatra sigurnom metodom autentifikacije korisnika (ukoliko se ne koristi u kombinaciji sa nekim spoljnim sigurnosnim sistemom, kao TLS/SSL), s obzirom da se korisničko	URL1 ¹²⁸⁵	Kritičan	Koristiti Osnovnu Autentifikaciju preko TLS/SSL (HTTPS). Omogućiti HTTPS na Web serveru. TLS/SSL protokol će zaštititi akreditivne osnovne autentifikacije u običnom tekstu. Koristiti Digest Authentication

¹²⁵⁹ <http://www.debian.org/security/DSA-/DSA-1934>¹²⁶⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8662>¹²⁶¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9363>¹²⁶² <http://secunia.com/advisories/37152/>¹²⁶³ <https://www.suse.com/support/security/advisories/>¹²⁶⁴ http://httpd.apache.org/security/vulnerabilities_22.html¹²⁶⁵ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>¹²⁶⁶ <http://www.securityfocus.com/bid/35253>¹²⁶⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1955>¹²⁶⁸ <http://lists.debian.org/debian-security-announce/2009/msg00124.html>¹²⁶⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10270>¹²⁷⁰ <http://rhn.redhat.com/errata/RHSA-2009-1107.html>¹²⁷¹ <http://rhn.redhat.com/errata/RHSA-2009-1108.html>¹²⁷² <http://secunia.com/advisories/34724/>¹²⁷³ <http://secunia.com/advisories/35284/>¹²⁷⁴ <http://secunia.com/advisories/35360/>¹²⁷⁵ <http://secunia.com/advisories/35395/>¹²⁷⁶ <http://secunia.com/advisories/35444/>¹²⁷⁷ <http://secunia.com/advisories/35487/>¹²⁷⁸ <http://secunia.com/advisories/35565/>¹²⁷⁹ <http://secunia.com/advisories/35710/>¹²⁸⁰ <http://secunia.com/advisories/35797/>¹²⁸¹ <http://secunia.com/advisories/35843/>¹²⁸² <http://secunia.com/advisories/36473/>¹²⁸³ <http://secunia.com/advisories/37221/>¹²⁸⁴ http://httpd.apache.org/security/vulnerabilities_22.html¹²⁸⁵ <http://tools.ietf.org/html/rfc2617>

		ime i lozinka preko mreže prenose kao običan tekst. Primer: Pokretanje ranjivog HTTP servisa. http://localhost:8080/manager/jmxproxy/advertise.inc http://localhost:8080/manager/jmxproxy/WS_FTP.LOG 1: Basic realm="Tomcat Manager Application"			Replace Basic Authentication sa alternativnom Digest Authentication shemom. Po savremenim kriptografskim standardima, Digest Authentication je slaba. Ali za širok spektar namena, ona je korisna zamena za Basic Authentication (osnovnu autentifikaciju). Ona ispravlja neke, ali ne sve, slabosti Basic Authentication (osnovne autentifikacije). Videti RFC 2617 ¹²⁸⁶ (odjeljak 4 Security Considerations) za više informacija.
6.	Apache httpd mod_deflate DoS (CVE-2009-1891) (http://apache-mod_deflate-dos)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Ranjivost na DOS napad otkrivena je u modulu mod_deflate. Ovaj modul nastavlja da kompresuje velike fajlove sve dok se kompresija ne završi, čak i kada je mrežna konekcija koja je zahtevala taj sadržaj prekinuta pre nego što je kompresija završena. To dovodi do toga da mod_deflate zauzima veliku količinu CPU-a ukoliko je mod_deflate bio omogućen za velike fajlove.	APPLE APPLE-SA-2009-11-09 ¹²⁸⁷ CVE CVE-2009-1891 ¹²⁸⁸ DEBIAN DSA-1834 ¹²⁸⁹ OSVDB 55782 ¹²⁹⁰ OVAL OVAL8632 ¹²⁹¹ OVAL OVAL9248 ¹²⁹² REDHAT RHSA-2009:1148 ¹²⁹³ REDHAT RHSA-2009:1156 ¹²⁹⁴ SECUNIA 35721 ¹²⁹⁵ SECUNIA 35781 ¹²⁹⁶ SECUNIA 35793 ¹²⁹⁷ SECUNIA 35865 ¹²⁹⁸ SECUNIA 37152 ¹²⁹⁹ SECUNIA 37221 ¹³⁰⁰ SUSE SUSE-SA:2009:050 ¹³⁰¹ URL1 ¹³⁰²	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz
7.	Apache httpd mod_proxy reverse proxy DoS (CVE-2009-1890) (http://apache-mod_proxy-reverse-proxy-dos)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja prisustva	APPLE APPLE-SA-2009-11-09 ¹³⁰³ CVE CVE-2009-1890 ¹³⁰⁴ DEBIAN DSA-1834 ¹³⁰⁵ OSVDB 55553 ¹³⁰⁶ OVAL OVAL8616 ¹³⁰⁷ OVAL OVAL9403 ¹³⁰⁸ REDHAT RHSA-	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

¹²⁸⁶ <http://tools.ietf.org/html/rfc2617#section-4>¹²⁸⁷ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>¹²⁸⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1891>¹²⁸⁹ <http://www.debian.org/security/2009/dsa-1834>¹²⁹⁰ <http://osvdb.org/55782>¹²⁹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8632>¹²⁹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9248>¹²⁹³ <http://rhn.redhat.com/errata/RHSA-2009-1148.html>¹²⁹⁴ <http://rhn.redhat.com/errata/RHSA-2009-1156.html>¹²⁹⁵ <http://secunia.com/advisories/35721/>¹²⁹⁶ <http://secunia.com/advisories/35781/>¹²⁹⁷ <http://secunia.com/advisories/35793/>¹²⁹⁸ <http://secunia.com/advisories/35865/>¹²⁹⁹ <http://secunia.com/advisories/37152/>¹³⁰⁰ <http://secunia.com/advisories/37221/>¹³⁰¹ <https://www.suse.com/support/security/advisories/>¹³⁰² http://httpd.apache.org/security/vulnerabilities_22.html¹³⁰³ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>¹³⁰⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1890>¹³⁰⁵ <http://www.debian.org/security/2009/dsa-1834>¹³⁰⁶ <http://osvdb.org/55553>¹³⁰⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8616>¹³⁰⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9403>

		mod_proxy modula. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy. Zlonamerni napadač bi mogao da iskoristi ovaj propust na takav način da primora proxy proces da zauzme veliku količinu CPU vremena.	2009:1148 ¹³⁰⁹ REDHAT RHSA-2009:1156 ¹³¹⁰ SECUNIA 35691 ¹³¹¹ SECUNIA 35721 ¹³¹² SECUNIA 35793 ¹³¹³ SECUNIA 35865 ¹³¹⁴ SECUNIA 37152 ¹³¹⁵ SECUNIA 37221 ¹³¹⁶ SUSE SUSE-SA:2009:050 ¹³¹⁷ URL1 ¹³¹⁸		
8.	Apache httpd APR-util off-by-one overflow (CVE-2009-1956) (http://apache-apr-util-off-by-one-overflow)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Propust prepunjavanja bafera "off-by-one" je otkriven u načinu na koji sklop kopije APR-util library komplet procesira promenljivu listu argumenata. Napadač bi mogao da kreira posebno izrađeni string kao input za već formatiranu output rutu konverzije, koja bi, na velikim platformama, potencijalno mogla da dovede do otkrivanja povreljivih informacija ili do odbijanja servisa.	APPLE APPLE-SA-2009-11-09 ¹³¹⁹ BID 35251 ¹³²⁰ CVE CVE-2009-1956 ¹³²¹ OVAL OVAL11567 ¹³²² REDHAT RHSA-2009:1107 ¹³²³ REDHAT RHSA-2009:1108 ¹³²⁴ SECUNIA 34724 ¹³²⁵ SECUNIA 35284 ¹³²⁶ SECUNIA 35395 ¹³²⁷ SECUNIA 35487 ¹³²⁸ SECUNIA 35565 ¹³²⁹ SECUNIA 35710 ¹³³⁰ SECUNIA 35797 ¹³³¹ SECUNIA 35843 ¹³³² SECUNIA 37221 ¹³³³ URL1 ¹³³⁴	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz
9.	Apache httpd expat DoS (CVE-2009-3560) (apache-httpd-2_2_x-cve-2009-3560)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u mogućnosti da dovede do toga da Apache parsira nepoverljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti.	BID 37203 ¹³³⁶ CVE CVE-2009-3560 ¹³³⁷ DEBIAN DSA-1953 ¹³³⁸ OVAL OVAL10613 ¹³³⁹ OVAL OVAL6883 ¹³⁴⁰ SECUNIA 37537 ¹³⁴¹ SECUNIA 38231 ¹³⁴² SECUNIA 38794 ¹³⁴³ SECUNIA 38832 ¹³⁴⁴ SECUNIA 38834 ¹³⁴⁵ SECUNIA 39478 ¹³⁴⁶	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz

¹³⁰⁹ <http://rhn.redhat.com/errata/RHSA-2009-1148.html>¹³¹⁰ <http://rhn.redhat.com/errata/RHSA-2009-1156.html>¹³¹¹ <http://secunia.com/advisories/35691/>¹³¹² <http://secunia.com/advisories/35721/>¹³¹³ <http://secunia.com/advisories/35793/>¹³¹⁴ <http://secunia.com/advisories/35865/>¹³¹⁵ <http://secunia.com/advisories/37152/>¹³¹⁶ <http://secunia.com/advisories/37221/>¹³¹⁷ <https://www.suse.com/support/security/advisories/>¹³¹⁸ http://httpd.apache.org/security/vulnerabilities_22.html¹³¹⁹ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>¹³²⁰ <http://www.securityfocus.com/bid/35251>¹³²¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1956>¹³²² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11567>¹³²³ <http://rhn.redhat.com/errata/RHSA-2009-1107.html>¹³²⁴ <http://rhn.redhat.com/errata/RHSA-2009-1108.html>¹³²⁵ <http://secunia.com/advisories/34724/>¹³²⁶ <http://secunia.com/advisories/35284/>¹³²⁷ <http://secunia.com/advisories/35395/>¹³²⁸ <http://secunia.com/advisories/35487/>¹³²⁹ <http://secunia.com/advisories/35565/>¹³³⁰ <http://secunia.com/advisories/35710/>¹³³¹ <http://secunia.com/advisories/35797/>¹³³² <http://secunia.com/advisories/35843/>¹³³³ <http://secunia.com/advisories/37221/>¹³³⁴ http://httpd.apache.org/security/vulnerabilities_22.html

		Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module). ¹³³⁵	SECUNIA 41701 ¹³⁴⁷ SECUNIA 43300 ¹³⁴⁸ URL1 ¹³⁴⁹		
10.	Apache httpd expat DoS (CVE-2009-3720) (apache-httpd-2_2_x-cve-2009-3720)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako je napadač u mogućnosti da dovede do toga da Apache parsira nepoverljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module). ¹³⁵⁰	CVE CVE-2009-3720 ¹³⁵¹ OVAL OVAL11019 ¹³⁵² OVAL OVAL7112 ¹³⁵³ REDHAT RHSA-2010:0002 ¹³⁵⁴ SECUNIA 37324 ¹³⁵⁵ SECUNIA 37537 ¹³⁵⁶ SECUNIA 37925 ¹³⁵⁷ SECUNIA 38050 ¹³⁵⁸ SECUNIA 38231 ¹³⁵⁹ SECUNIA 38794 ¹³⁶⁰ SECUNIA 38832 ¹³⁶¹ SECUNIA 38834 ¹³⁶² SECUNIA 39478 ¹³⁶³ SECUNIA 41701 ¹³⁶⁴ SECUNIA 43300 ¹³⁶⁵ URL1 ¹³⁶⁶	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz

¹³³⁶ <http://www.securityfocus.com/bid/37203>¹³³⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3560>¹³³⁸ <http://www.debian.org/security/2009/dsa-1953>¹³³⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10613>¹³⁴⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6883>¹³⁴¹ <http://secunia.com/advisories/37537/>¹³⁴² <http://secunia.com/advisories/38231/>¹³⁴³ <http://secunia.com/advisories/38794/>¹³⁴⁴ <http://secunia.com/advisories/38832/>¹³⁴⁵ <http://secunia.com/advisories/38834/>¹³⁴⁶ <http://secunia.com/advisories/39478/>¹³³⁵ Prefork i Worker su dva tipa modula za Apache-ov multiprocessing. Oba imaju prednosti i mane. Prefork MPM koristi višestruke child procese sa po jednim thread-om za svaki proces, a svaki proces upravlja jednom konekcijom u jednom trenutku. Worker MPM koristi višestruke child procese sa višestrukim thread-ovim za svaki proces, a svaki thread upravlja jednom konekcijom u jednom trenutku.¹³⁴⁷ <http://secunia.com/advisories/41701/>¹³⁴⁸ <http://secunia.com/advisories/43300/>¹³⁴⁹ http://httpd.apache.org/security/vulnerabilities_22.html¹³⁵⁰ Prefork i Worker su dva tipa modula za Apache-ov multiprocessing. Oba imaju prednosti i mane. Prefork MPM koristi višestruke child procese sa po jednim thread-om za svaki proces, a svaki proces upravlja jednom konekcijom u jednom trenutku. Worker MPM koristi višestruke child procese sa višestrukim thread-ovim za svaki proces, a svaki thread upravlja jednom konekcijom u jednom trenutku.¹³⁵¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3720>¹³⁵² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11019>¹³⁵³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7112>¹³⁵⁴ <http://rhn.redhat.com/errata/RHSA-2010-0002.html>¹³⁵⁵ <http://secunia.com/advisories/37324/>¹³⁵⁶ <http://secunia.com/advisories/37537/>¹³⁵⁷ <http://secunia.com/advisories/37925/>¹³⁵⁸ <http://secunia.com/advisories/38050/>¹³⁵⁹ <http://secunia.com/advisories/38231/>¹³⁶⁰ <http://secunia.com/advisories/38794/>¹³⁶¹ <http://secunia.com/advisories/38832/>¹³⁶² <http://secunia.com/advisories/38834/>¹³⁶³ <http://secunia.com/advisories/39478/>¹³⁶⁴ <http://secunia.com/advisories/41701/>¹³⁶⁵ <http://secunia.com/advisories/43300/>¹³⁶⁶ http://httpd.apache.org/security/vulnerabilities_22.html

11.	Apache httpd apr_bridage_split_line DoS (CVE-2010-1623) (apache-httpd-2_2_x- cve-2010-1623)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako Apache procesira ne-SSL zahteve. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_brigade_split_line() u sklopu APR-util library, koji se koristi za procesiranje ne-SSL zahteva. Zlonamerni napadač bi mogao da šalje zahteve, pažljivo izrađujući tajming za pojedinačne bajtove, što bi polako zauzimalo memoriju i potencijalno dovelo do odbijanja servisa.	BID 43673 ¹³⁶⁷ CVE CVE-2010-1623 ¹³⁶⁸ REDHAT RHSA- 2010:0950 ¹³⁶⁹ SECUNIA 41701 ¹³⁷⁰ SECUNIA 42015 ¹³⁷¹ SECUNIA 42361 ¹³⁷² SECUNIA 42367 ¹³⁷³ SECUNIA 42403 ¹³⁷⁴ SECUNIA 42537 ¹³⁷⁵ SECUNIA 43211 ¹³⁷⁶ SECUNIA 43285 ¹³⁷⁷ URL1 ¹³⁷⁸	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
12.	Apache httpd mod_cache and mod_dav DoS (CVE- 2010-1452) (apache- httpd-2_2_x- mod_cache-andmod_ dav-dos-cve-2010- 1452)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako web server izvršava jedan od sledećih modula: mod_cache, mod_dav. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u obradi zahteva od strane mod_cache i mod_dav. Zlonamerni napadač bi mogao da pošalje pažljivo izrađen zahtev i prouzrokuje da httpd child proces krahira. Ovakvo krahiranje bi se manifestovalo samo kao odbijanje servisa ako se koristi Worker MPM. Ovaj problem se dalje može ublažiti ako na mod_dav samo utiču zahtevi za koje postoji mogućnost autentifikovanja, a mod_cache je pod uticajem samo ako se koristi neuobičajena „CacheIgnoreURLSessionIdentifiers“ direktiva, uvedena u verziji 2.2.14. Ovaj problem je prijavio Mark Drayton.	APPLE APPLE-SA- 2011-03-21 ¹³⁷⁹ CVE CVE-2010-1452 ¹³⁸⁰ OVAL OVAL11683 ¹³⁸¹ REDHAT RHSA- 2010:0659 ¹³⁸² SECUNIA 42367 ¹³⁸³ URL1 ¹³⁸⁴	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.16.tar.gz
13.	Apache httpd Timeout detection flaw (mod_proxy_http)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80	APPLE APPLE-SA- 2011-03-21 ¹³⁸⁵ BID 40827 ¹³⁸⁶	Ozbiljan	Mnoge platforme i mnogi distributeri daju unapred formirane binarne pakete za

¹³⁶⁷ <http://www.securityfocus.com/bid/43673>¹³⁶⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1623>¹³⁶⁹ <http://rhn.redhat.com/errata/RHSA-2010-0950.html>¹³⁷⁰ <http://secunia.com/advisories/41701/>¹³⁷¹ <http://secunia.com/advisories/42015/>¹³⁷² <http://secunia.com/advisories/42361/>¹³⁷³ <http://secunia.com/advisories/42367/>¹³⁷⁴ <http://secunia.com/advisories/42403/>¹³⁷⁵ <http://secunia.com/advisories/42537/>¹³⁷⁶ <http://secunia.com/advisories/43211/>¹³⁷⁷ <http://secunia.com/advisories/43285/>¹³⁷⁸ http://httpd.apache.org/security/vulnerabilities_22.html¹³⁷⁹ <http://lists.apple.com/archives/security-announce/2011/Mar/msg00006.html>¹³⁸⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1452>¹³⁸¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11683>¹³⁸² <http://rhn.redhat.com/errata/RHSA-2010-0659.html>¹³⁸³ <http://secunia.com/advisories/42367/>¹³⁸⁴ http://httpd.apache.org/security/vulnerabilities_22.html¹³⁸⁵ <http://lists.apple.com/archives/security-announce/2011/Mar/msg00006.html>

	(CVE-2010-2068) (apache-httpd-2_2_x-timeoutdetection-flaw-mod_proxy_http-cve-2010-2068)	172.23.202.220:443 Propust sa kojim je omogućeno otkrivanje informacija je otkriven u modulu mod_proxy_http na verzijama 2.2.9 do 2.2.15, 2.3.4-alpha i 2.3.5-alpha. Pod određenim tajmout uslovima, server bi mogao da uzvрати odgovorom koji je namenjen drugom korisniku. Ugrožene su one konfiguracije koje pokreću korišćenje proxy worker pool-ova. Na ranijim verzijama nije bilo ranjivosti, jer proxy pool-ovi još nisu bili uvedeni. Zahvaljujući Loren Anderson-u ovaj problem je prijavljen, a najjednostavniji način njegovog izbegavanja jeste opšte konfigurisanje.	CVE CVE-2010-2068 ¹³⁸⁷ OVAL OVAL11491 ¹³⁸⁸ OVAL OVAL6931 ¹³⁸⁹ SECUNIA 40206 ¹³⁹⁰ SECUNIA 41480 ¹³⁹¹ SECUNIA 41490 ¹³⁹² SECUNIA 41722 ¹³⁹³ XF apache-modproxyhttp-timeout-info-disc(59413) ¹³⁹⁴ URL1 ¹³⁹⁵		Apache. Ovi unapred formirani paketi su najčešće standardizovani i optimizirani za određenu distribuciju, pa se zato savetuje korišćenje paketa predefinisanih za određeni OS, ukoliko su dostupni. Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.16.tar.gz
14.	Apache httpd Timeout detection flaw (mod_proxy_http) (CVE-2010-2791) (apache-httpd-2_2_x-timeoutdetection-flaw-mod_proxy_http-cve-2010-2791)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako web server izvršava jedan od sledećih modula: mod_proxy_http. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust sa kojim je omogućeno otkrivanje informacija je otkriven u modulu mod_proxy_http, samo u verziji 2.2.9 na Unix platformama. Pod određenim tajmout uslovima, server bi mogao da uzvрати odgovorom koji je namenjen drugom korisniku. Ugrožene su samo one konfiguracije koje pokreću korišćenje proxy worker pool-ova. Na ranijim verzijama nije bilo ranjivosti, jer proxy pool-ovi još nisu bili uvedeni.	BID 42102 ¹³⁹⁶ CVE CVE-2010-2791 ¹³⁹⁷ REDHAT RHSA-2010-0659 ¹³⁹⁸ XF apache-modproxy-info-disclosure(60883) ¹³⁹⁹ URL1 ¹⁴⁰⁰	Ozbiljan	Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.10.tar.gz
15.	X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch)	172.23.202.124:443 172.23.202.220:443 Rubrika u sertifikatu X.509 sa uobičajenim nazivom subjekta (CN) ne poklapa se sa imenom pojedinca koje je navedeno u sertifikatu. Pre izdavanja sertifikata, Certification Authority (CA) mora da proveri identitet pojedinca koji potražuje sertifikat, kako je navedeno u CA-ovom Certification Practice Statement (CPS). Zbog toga,		Ozbiljan	Rubrika sa uobičajenim nazivom subjekta (CN) u sertifikatu X.509 treba da bude podešena da sadrži ime pojedinca koji prikazuje sertifikat (npr. ime hosta). To se postiže izradom novog sertifikata, koji najčešće potpisuje Certification Authority (CA), koji je od poverenja kako za klijenta, tako i za

¹³⁸⁶ <http://www.securityfocus.com/bid/40827>¹³⁸⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2068>¹³⁸⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11491>¹³⁸⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6931>¹³⁹⁰ <http://secunia.com/advisories/40206/>¹³⁹¹ <http://secunia.com/advisories/41480/>¹³⁹² <http://secunia.com/advisories/41490/>¹³⁹³ <http://secunia.com/advisories/41722/>¹³⁹⁴ <http://xforce.iss.net/xforce/xfdb/59413>¹³⁹⁵ http://httpd.apache.org/security/vulnerabilities_22.html¹³⁹⁶ <http://www.securityfocus.com/bid/42102>¹³⁹⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2791>¹³⁹⁸ <http://rhn.redhat.com/errata/RHSA-2010-0659.html>¹³⁹⁹ <http://xforce.iss.net/xforce/xfdb/60883>¹⁴⁰⁰ http://httpd.apache.org/security/vulnerabilities_22.html

		uobičajene procedure validacije sertifikata zahtevaju da rubrika sertifikata sa CN subjektom odgovara pravom imenu pojedinca koji prikazuje sertifikat. Na primer, u sertifikatu prikazanom na „https://www.example.com/“, naziv subjekta (CN) treba da bude „www.example.com“. U cilju otkrivanja i sprečavanja napada prisluškivanja, validnost sertifikata mora da bude overena, jer bi u suprotnom napadač mogao da otpočne napad preko posrednika i da stekne potpunu kontrolu nad protokom podataka. Od posebne važnosti je validnost naziva subjekta (CN), koji treba da se poklapa sa imenom pojedinca (imenom host-a). Neodgovarajući CN se najčešće javlja usled greške u konfiguraciji, iako on takođe može da ukazuje na to da se sprovodi napad preko posrednika.			server.
16.	FTP access with ftp account (ftp-generic-0001)	172.23.202.124:21 172.23.202.220:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisničkim ID-jem „ftp“ i šifrom „ftp“. Dosadašnja praksa je pokazala da treba ukloniti difoltnu naloge, ako je to moguće. Za naloge koje zahteva sistem, treba promeniti difoltnu šifru.	CVE CVE-1999-0497 ¹⁴⁰¹	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko to nije kritično za dalje funkcionisanje sistema. U suprotnom, treba promeniti lozinku u nedifoltnu vrednost.
17.	FTP access with anonymous account (ftp-generic-0002)	172.23.202.124:21 172.23.202.220:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisničkim ID-jem „anonymous“ i šifrom „ftp@“. Dosadašnja praksa je pokazala da treba ukloniti difoltnu naloge, ako je to moguće. Za naloge koje zahteva sistem, treba promeniti difoltnu šifru.	CVE CVE-1999-0497 ¹⁴⁰²	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko to nije kritično za dalje funkcionisanje sistema. U suprotnom, treba promeniti lozinku u nedifoltnu vrednost.
18.	FTP server does not support AUTH command (ftp-generic-0007)	172.23.202.124:21 172.23.202.220:21 Klijenti na FTP server po difoltu šalju poverljive podatke (korisnički ID i šifru) u vidu čitkog teksta. Ova okolnost dozvoljava zlonamernim korisnicima omogućava da presreću poverljive podatke ukoliko prisluškuju vezu. Noviji FTP serveri podržavaju komandu AUTH, koja daje veće opcije autentifikacije, kao TLS, Kerberos, GSSAPI, itd. Njih treba koristiti da bi se sprečilo prisluškivanje na FTP vezama.		Ozbiljan	Nadograditi/Ažurirati na a FTP server koji podržava komandu AUTH.
19.	Apache httpd AllowOverride Options handling bypass (CVE-2009-1195) (http-apache-	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je osjetljiv na ovu	APPLE APPLE-SA-2009-11-09¹⁴⁰³ BID 35115¹⁴⁰⁴ CVE CVE-2009-1195¹⁴⁰⁵ DEBIAN DSA-1816¹⁴⁰⁶	Ozbiljan	Apache >= 2.2 and < 2.3 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

¹⁴⁰¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>¹⁴⁰² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>¹⁴⁰³ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>¹⁴⁰⁴ <http://www.securityfocus.com/bid/35115>¹⁴⁰⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1195>¹⁴⁰⁶ <http://www.debian.org/security/2009/dsa-1816>

	allowoverrideoptions-handling-bypass)	ranjivost SAMO ako web server izvršava direktivu AllowOverride sa određenim opcijama koje se koriste. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u obradi direktiva „Options“ i „AllowOverride“. U konfiguracijama koje koriste direktivu „AllowOverride“ sa određenim „Options“ argumentima, lokalni korisnici mogu da izvršavaju komande iz web-serverskih skripti.	OSVDB 54733 ¹⁴⁰⁷ OVAL OVAL11094 ¹⁴⁰⁸ OVAL OVAL8704 ¹⁴⁰⁹ REDHAT RHSA-2009:1075 ¹⁴¹⁰ REDHAT RHSA-2009:1156 ¹⁴¹¹ SECUNIA 35261 ¹⁴¹² SECUNIA 35264 ¹⁴¹³ SECUNIA 35395 ¹⁴¹⁴ SECUNIA 35453 ¹⁴¹⁵ SECUNIA 35721 ¹⁴¹⁶ SECUNIA 37152 ¹⁴¹⁷ SUSE SA:2009:050 ¹⁴¹⁸ XF apache-allowoverrides-security-bypass(50808) ¹⁴¹⁹ URL1 ¹⁴²⁰		
20.	Apache httpd mod_proxy_ajp DoS (CVE-2010-0408) (http://apache-mod_proxy_ajp-dos)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ajp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Mod_proxy_ajp će vratiti pogrešan kôd statusa ako naide na grešku, prouzrokujući da backend server bude stavljen u status greške dok ne istekne vreme za ponovni pokušaj. Udaljeni napadač bi mogao da pošalje zlonameran zahtev da bi pokrenuo ovaj problem, što bi dovelo do odbijanja servisa. Zahvaljujući Niku Toivola iz Sulake Corporation ovaj problem je prijavljen uz predloženu adekvatnu meru zaštite u vidu zakrpe.	BID 38491 ¹⁴²¹ CVE CVE-2010-0408 ¹⁴²² DEBIAN DSA-2035 ¹⁴²³ OVAL OVAL8619 ¹⁴²⁴ OVAL OVAL9935 ¹⁴²⁵ REDHAT RHSA-2010:0168 ¹⁴²⁶ SECUNIA 39100 ¹⁴²⁷ SECUNIA 39501 ¹⁴²⁸ SECUNIA 39628 ¹⁴²⁹ SECUNIA 39632 ¹⁴³⁰ SECUNIA 39656 ¹⁴³¹ SECUNIA 40096 ¹⁴³² URL1 ¹⁴³³	Ozbiljan	Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz

¹⁴⁰⁷ <http://osvdb.org/54733>¹⁴⁰⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11094>¹⁴⁰⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8704>¹⁴¹⁰ <http://rhn.redhat.com/errata/RHSA-2009-1075.html>¹⁴¹¹ <http://rhn.redhat.com/errata/RHSA-2009-1156.html>¹⁴¹² <http://secunia.com/advisories/35261/>¹⁴¹³ <http://secunia.com/advisories/35264/>¹⁴¹⁴ <http://secunia.com/advisories/35395/>¹⁴¹⁵ <http://secunia.com/advisories/35453/>¹⁴¹⁶ <http://secunia.com/advisories/35721/>¹⁴¹⁷ <http://secunia.com/advisories/37152/>¹⁴¹⁸ <https://www.suse.com/support/security/advisories/>¹⁴¹⁹ <http://xforce.iss.net/xforce/xfdb/50808>¹⁴²⁰ http://httpd.apache.org/security/vulnerabilities_22.html¹⁴²¹ <http://www.securityfocus.com/bid/38491>¹⁴²² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0408>¹⁴²³ <http://www.debian.org/security/2010/dsa-2035>¹⁴²⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8619>¹⁴²⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9935>¹⁴²⁶ <http://rhn.redhat.com/errata/RHSA-2010-0168.html>¹⁴²⁷ <http://secunia.com/advisories/39100/>¹⁴²⁸ <http://secunia.com/advisories/39501/>¹⁴²⁹ <http://secunia.com/advisories/39628/>¹⁴³⁰ <http://secunia.com/advisories/39632/>¹⁴³¹ <http://secunia.com/advisories/39656/>¹⁴³² <http://secunia.com/advisories/40096/>¹⁴³³ http://httpd.apache.org/security/vulnerabilities_22.html

21.	Apache httpd mod_proxy_ftp DoS (CVE-2009-3094) (http-apache-mod_proxy_ftp-dos)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ftp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust NULL pointer dereference (pointer sa NULL vrednošću upotrebljen kao da ukazuje na validnu memorijsku oblast) otkriven u modulu mod_proxy_ftp. Zlonamerni FTP server, kojem su zahtevi proksirani, mogao bi da iskoristi ovaj propust u smislu obaranja http child procesa uz pomoć namerno izmenjenog odgovora EPSV ili PASV komandi, što bi dovelo do delimičnog odbijanja servisa.	CVE CVE-2009-3094 ¹⁴³⁴ DEBIAN DSA-1934 ¹⁴³⁵ OVAL OVAL10981 ¹⁴³⁶ OVAL OVAL8087 ¹⁴³⁷ SECUNIA 36549 ¹⁴³⁸ SECUNIA 37152 ¹⁴³⁹ SUSE SA:2009:050 ¹⁴⁴⁰ URL1 ¹⁴⁴¹	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz
22.	Apache httpd Solaris pollset DoS (CVE-2009-2699) (http-apache-solaris-pollset-dos)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Otkriven je Faulty error prouzrokovan bagom u APR-u. Zlonamerni napadač bi mogao da pokrene ovaj problem na Solaris serverima koji koriste prefork ili event MPM-ove ¹⁴⁴² , što bi dovelo do odbijanja servisa.	BID 36596 ¹⁴⁴³ CVE CVE-2009-2699 ¹⁴⁴⁴ XF apache-solaris-pollset-dos(53666) ¹⁴⁴⁵ URL1 ¹⁴⁴⁶	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.gz
23.	Browsableable web directory (http-generic-browsable-dir)	172.23.202.124:8080 172.23.202.220:8080 Otkriven je direktorijum na web serveru koji može biti pretraživan, što znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice - spajdering (prateći hiperlinkove), ili - kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute force napadom na liste uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skrivenne“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice.		Ozbiljan	Za Apache: onemogućiti brauzovanje direktorijuma mreže za sve direktorijume i poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim ako postoji potreba da ovi fajlovi budu dostupni preko web-a. Povremeno proći kroz web direktorijume i obrisati

¹⁴³⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3094>¹⁴³⁵ <http://www.debian.org/security/2009/dsa-1934>¹⁴³⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10981>¹⁴³⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8087>¹⁴³⁸ <http://secunia.com/advisories/36549/>¹⁴³⁹ <http://secunia.com/advisories/37152/>¹⁴⁴⁰ <https://www.suse.com/support/security/advisories/>¹⁴⁴¹ http://httpd.apache.org/security/vulnerabilities_22.html¹⁴⁴² Event MPM je eksperimentalna varijanta worker MPM-a dizajnirana sa ciljem da se omogući istovremena obrada više zahteva prepuštajući određene procese pomoćnim thread-ovima, oslobađajući glavne thread-ove za rad na novim zahtevima. Dostupno na <http://httpd.apache.org/docs/2.2/mod/event.html>, 10.02.2013¹⁴⁴³ <http://www.securityfocus.com/bid/36596>¹⁴⁴⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2699>¹⁴⁴⁵ <http://xforce.iss.net/xforce/xfdb/53666>¹⁴⁴⁶ http://httpd.apache.org/security/vulnerabilities_22.html

					svaki koji nije u upotrebi, koji je zastsareo, kao i nepoznate fajlove i direktorijume. Za Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote: Onemogućiti brauzovanje direktorijuma mreže za sve direktorijume i poddirektorijume. Uključiti Tomcat-ov web.xml file. U odeljku „default“, promeniti parametar „listings“ iz „true“ u „false“. Restartovati server. Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim ako ne postoji potreba da ovi fajlovi budu dostupni preko web-a. Povremeno proći kroz web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastsareo, kao i nepoznate fajlove i direktorijume.
24.	WebDAV PROPFIND Method Allows Web Directory Browsing (http-generic-propfind-dir-browsing)	172.23.202.124:8080 172.23.202.220:8080 Moguće je koristiti WebDAV PROPFIND metodu da bi se pretraživali web direktorijumi na serveru, što za posledicu ima otkrivanje sadržaja koji bi trebalo da bude sakriven. Ovo bi potencijalno omogućilo napadaču da dođe do osetljivih informacija, kao što su fajlovi podataka i backup fajlovi, ili bi dobio inofrmacije o strukturi direktorijuma, koje bi se kasnije mogle koristiti za mnogo prefinjeniji napad. Sledeći HTTP objekti su preuzeti korišćenjem PROPFIND kroz /webdav/: /webdav//webdav/tomcat.gif/webdav/tomcat-power.gif/webdav/index.html			Apache ograničena HTTP PROPFIND Metoda za Apache. PROPFIND metoda bi trebalo da bude nedostupna za anonimne zahteve. Isključiti autentifikaciju na WebDAV direktorijumu tako da samo ovlašćeni korisnici mogu da pozovu ovu metodu i realizuju legitimne akcije, kao: <pre><Location /webdav_dir/*> <LimitExcept GET HEAD OPTIONS POST> AuthType Basic AuthName „WebDAV Authentication“ AuthUserFile /path/to/userfile AuthGroupFile /path/to/groupfile potražujte grupne webdav korisnike </LimitExcept> </Location></pre> Zatim napraviti fajl za lozinku i fajl za grupu: <pre>htpasswd -cs /path/to/userfile bob echo „webdavusers: bob“ > /path/to/groupfile</pre> Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-

				Coyote Ograničena HTTP PROPFIND metoda za Tomcat: U konfiguracionom fajlu web.xml za WebDAV-onemogućeni direktorijum, dodati sledeće da bi se ograničila funkcionalnost WebDAV za određenog korisnika (korisnike): <pre> <security-constraint> <web-resource-collection> <web-resource-name>WebDav Directory</web-resource-name> <url-pattern>/*</url-pattern> </web-resource-collection> <auth-constraint> <role-name>webdav-user</role-name> </auth-constraint> </security-constraint> <login-config> <auth-method>BASIC</auth-method> <realm-name>WebDAV Realm</realm-name> </login-config> <security-role> <description> Ovlastiti WebDAV korisnike </description> <role-name>webdav-user</role-name> </security-role> U fajlu conf/tomcat-users.xml, dodati WebDAV korisnika kao: <?xml version='1.0' encoding='utf-8'?> <tomcat-users> <role rolename="webdav-user"/> <user username="bob" password="b0bsp455w0rdy0!" roles="webdav-user"/> </tomcat-users> </pre>
25.	Form action submits sensitive data in the clear (http-generic-sensitive-form-data-unencrypted)	172.23.202.124:8080 172.23.202.220:8080 Web forma sadrži rubrike sa podacima koji su možda po prirodi osetljivi. Ovakvi podaci se prenose preko nezaštićene veze, koja bi mogla da omogući zlonamernim napadačima da prisluškujući mrežu pregledaju podatke u vidu običnog teksta. Formatiranje preko http://localhost:8080/jsp-examples/security/protected/j_security_check prosleđuje sledeće nezaštićene osetljive rubrike: j_password		Ozbiljan Isključiti HTTPS protokol na serveru. Promeniti „action“ URL na oznaci rubrike da koristi HTTPS protokol („https://...“) umesto samo HTTP protokol („http://...“). Sve osetljive podatke treba slati preko HTTPS umesto preko HTTP.

26.	TLS/SSL Server Supports Weak Cipher Algorithms (ssl-weak-ciphers)	172.23.202.124:443 172.23.202.220:443 negotiated the SSL_DHE_RSA_WITH_DES_CBC_SHA cipher suite TLS/SSL server podržava šifre koje se zasnivaju na slabim algoritmima. To napadaču može omogućiti da pokrene napade preko posrednika i da pregleda ili čačka osetljive podatke. Uopšteno, sledeće šifre se smatraju slabim: Tzv. „null“ (nula) šifre, jer ne šifruju podatke. Eksportne šifre koje koriste dužine tajnih ključeva ograničene na 40 bitova. Na to najčešće ukazuje reč EXP/EXPORT u nazivu šifre. Zastareli algoritmi za šifrovanje čije se dužine tajnih ključeva po današnjim standardima smatraju kratkim, npr. DES ili RC4 sa 56-bitnim ključevima.		Ozbiljan	Konfigurisati server tako da onemogući podršku za slabe šifre. Za Apache web servere sa mod_ssl, uključiti fajl Apache konfiguracije i izmeniti liniju SSLCipherSuite tako da u njoj piše: SSLCipherSuite ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
27.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	172.23.202.124:3306 172.23.202.220:3306: Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hедера i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183¹⁴⁴⁷ CERT-VN: 415294¹⁴⁴⁸ CVE CVE-2004-0230¹⁴⁴⁹ MS: MS05-019¹⁴⁵⁰ MS: MS06-064¹⁴⁵¹ NETBSD: NetBSD-SA2004-006¹⁴⁵² OVAL: OVAL2689¹⁴⁵³ OVAL: OVAL270¹⁴⁵⁴ OVAL OVAL3508¹⁴⁵⁵ OVAL OVAL4791¹⁴⁵⁶ OVAL OVAL5711¹⁴⁵⁷ SECUNIA: 11440¹⁴⁵⁸ SECUNIA 11458¹⁴⁵⁹ SECUNIA: 22341¹⁴⁶⁰ SGI 20040403-01-A¹⁴⁶¹ XF tcp-rst-dos(15886)¹⁴⁶² URL1¹⁴⁶³ URL2¹⁴⁶⁴	Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC 2385 ¹⁴⁶⁵ . Ono je napravljeno da smanji opasnost od određenih napada na BGP, kao što su TCP reseti.
28.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podesi na jedinstvenu vrednost i da se koristi u	BID 4314¹⁴⁶⁶ CVE CVE-2002-0510¹⁴⁶⁷ XF linux-udp-fingerprint(8588)¹⁴⁶⁸	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili pak ranjivost koju treba popravljati, tako da ne

¹⁴⁴⁷ <http://www.securityfocus.com/bid/10183>¹⁴⁴⁸ <http://www.kb.cert.org/vuls/id/415294>¹⁴⁴⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>¹⁴⁵⁰ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>¹⁴⁵¹ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>¹⁴⁵² <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>¹⁴⁵³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>¹⁴⁵⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>¹⁴⁵⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>¹⁴⁵⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>¹⁴⁵⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>¹⁴⁵⁸ <http://secunia.com/advisories/11440/>¹⁴⁵⁹ <http://secunia.com/advisories/11458/>¹⁴⁶⁰ <http://secunia.com/advisories/22341/>¹⁴⁶¹ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>¹⁴⁶² <http://xforce.iss.net/xforce/xfdb/15886>¹⁴⁶³ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>¹⁴⁶⁴ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>¹⁴⁶⁵ <http://www.ietf.org/rfc/rfc2385.txt>¹⁴⁶⁶ <http://www.securityfocus.com/bid/4314>¹⁴⁶⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>¹⁴⁶⁸ <http://xforce.iss.net/xforce/xfdb/8588>

		rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da fingerprint-uje operativni sistem.			postoje rešenja koja se mogu kupiti. Jedino se može postaviti fajervol ili neka druga sprava za filtriranje između napadnutog i neprijateljskog napada koji je u mogućnosti da randomizuje IP ID-jeve.
29.	Apache httpd mod_proxy_ftp globbing XSS (CVE-2008-2939) (apache-httpd-2_2_x-mod_proxy_ftpglobbing - xss-cve-2008-2939)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani sistem je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ftp. Pregledajte konfiguraciju vašeg web servera radi validacije. Propust je otkriven u modulu mod_proxy_ftp prilikom obrade "wildcard"-a ukoliko se on nađe na putanji FTP URL. Ukoliko je mod_proxy_ftp omogućen da podržava FTP-over-HTTP, zahtevi koji sadrže specijalne karaktere mogu da dovedu do cross-site scripting-a (XSS).	APPLE APPLE-SA-2009-05-12 ¹⁴⁶⁹ BID 30560 ¹⁴⁷⁰ CERT TA09-133A ¹⁴⁷¹ CERT-VN 663763 ¹⁴⁷² CVE CVE-2008-2939 ¹⁴⁷³ OVAL OVAL11316 ¹⁴⁷⁴ OVAL OVAL7716 ¹⁴⁷⁵ REDHAT RHSA-2008:0966 ¹⁴⁷⁶ REDHAT RHSA-2008:0967 ¹⁴⁷⁷ SECUNIA 31384 ¹⁴⁷⁸ SECUNIA 31673 ¹⁴⁷⁹ SECUNIA 32685 ¹⁴⁸⁰ SECUNIA 32838 ¹⁴⁸¹ SECUNIA 33156 ¹⁴⁸² SECUNIA 33797 ¹⁴⁸³ SECUNIA 34219 ¹⁴⁸⁴ SECUNIA 35074 ¹⁴⁸⁵ XF apache-modproxyftp-xss(44223) ¹⁴⁸⁶ URL1 1487	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.10.tar.gz
30.	Apache httpd apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpd-cve-2011-0419)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_autoindex. Pregledajte konfiguraciju vašeg web servera radi validacije. Propust je otkriven u funkciji apr_fnmatch() u sklopu APR biblioteke. Ako je omogućen mod_autoindex, a indksi	CVE CVE-2011-0419 ¹⁴⁸⁸ REDHAT RHSA-2011:0507 ¹⁴⁸⁹ SECUNIA 44490 ¹⁴⁹⁰ SECUNIA 44564 ¹⁴⁹¹ SECUNIA 44574 ¹⁴⁹² URL1 1493	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.18.tar.gz

¹⁴⁶⁹ <http://lists.apple.com/archives/security-announce/2009/May/msg00001.html>¹⁴⁷⁰ <http://www.securityfocus.com/bid/30560>¹⁴⁷¹ <http://www.us-cert.gov/ncas/alerts/TA09-133A>¹⁴⁷² <http://www.kb.cert.org/vuls/id/663763>¹⁴⁷³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-2939>¹⁴⁷⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11316>¹⁴⁷⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7716>¹⁴⁷⁶ <http://rhn.redhat.com/errata/RHSA-2008-0966.html>¹⁴⁷⁷ <http://rhn.redhat.com/errata/RHSA-2008-0967.html>¹⁴⁷⁸ <http://secunia.com/advisories/31384/>¹⁴⁷⁹ <http://secunia.com/advisories/31673/>¹⁴⁸⁰ <http://secunia.com/advisories/32685/>¹⁴⁸¹ <http://secunia.com/advisories/32838/>¹⁴⁸² <http://secunia.com/advisories/33156/>¹⁴⁸³ <http://secunia.com/advisories/33797/>¹⁴⁸⁴ <http://secunia.com/advisories/34219/>¹⁴⁸⁵ <http://secunia.com/advisories/35074/>¹⁴⁸⁶ <http://xforce.iss.net/xforce/xfdb/44223>¹⁴⁸⁷ http://httpd.apache.org/security/vulnerabilities_22.html¹⁴⁸⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419>¹⁴⁸⁹ <http://rhn.redhat.com/errata/RHSA-2011-0507.html>¹⁴⁹⁰ <http://secunia.com/advisories/44490/>¹⁴⁹¹ <http://secunia.com/advisories/44564/>¹⁴⁹² <http://secunia.com/advisories/44574/>¹⁴⁹³ http://httpd.apache.org/security/vulnerabilities_22.html

		direktorijuma mod_autoindex su sadržavali fajlove sa dovoljno dugim nazivima, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do preterane upotrebe CPU-a. Ovo bi moglo da bude iskorišćeno u napadu odbijanja servisa. Ovaj problem je prijavio Maksymilian Arciemowicz.			
31.	Apache httpd APR-util heap underwrite (CVE-2009-0023) (http://apache-apr-util-heap-underwrite)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je osjetljiv na ovu ranjivost SAMO ako napadač poseduje posebno kreiranu ključnu reč za pretraživanje one funkcije koja upravlja kompajliranjem formi zahtevane pretrage. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u načinu na koji komplet APR-biblioteke kompajlira forme zahtevanih pretraživanja. Napadač bi mogao da formuliše posebno izrađenu ključnu reč pretraživanja koja bi se proizvodnim prepisivanjem gomilala u memoriji prilikom obrađivanja zahteva za pretragu.	BID 35221 ¹⁴⁹⁴ CVE CVE-2009-0023 ¹⁴⁹⁵ DEBIAN DSA-1812 ¹⁴⁹⁶ OVAL OVAL10968 ¹⁴⁹⁷ REDHAT RHSA-2009:1107 ¹⁴⁹⁸ REDHAT RHSA-2009:1108 ¹⁴⁹⁹ SECUNIA 34724 ¹⁵⁰⁰ SECUNIA 35284 ¹⁵⁰¹ SECUNIA 35360 ¹⁵⁰² SECUNIA 35395 ¹⁵⁰³ SECUNIA 35444 ¹⁵⁰⁴ SECUNIA 35487 ¹⁵⁰⁵ SECUNIA 35565 ¹⁵⁰⁶ SECUNIA 35710 ¹⁵⁰⁷ SECUNIA 35797 ¹⁵⁰⁸ SECUNIA 35843 ¹⁵⁰⁹ SECUNIA 37221 ¹⁵¹⁰ XF apache-aprstrmatchprecompile-dos(50964) ¹⁵¹¹ URL1 ¹⁵¹²	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz
32.	Apache Etag Inode Information Leakage (http://apache-etag-inode-leak)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 U određenim konfiguracijama, Apache HTTP server dozvoljava udaljenim napadačima da dobiju poverljive informacije preko (1) Etag heder-a, koji otkriva broj inoda ili (2) razdvajanje višedelnih MIME-a, koja ukazuje na ID child procesa (PID). Određene verzije Apache-a koriste	BID 6939 ¹⁵¹³ BID 6943 ¹⁵¹⁴ CVE CVE-2003-1418 ¹⁵¹⁵ XF apache-mime-information-disclosure(11438) ¹⁵¹⁶	Ozbiljan	Onemogućiti Etag mehanizam ¹⁵¹⁷ tipa "inod-based" konfiguraciji Apache-a. Takođe, inod informacije je moguće ukloniti iz Etag heder-a tako što će se dodati direktiva u Apache konfiguraciju: <i>FileETag Mtime Size</i>

¹⁴⁹⁴ <http://www.securityfocus.com/bid/35221>¹⁴⁹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-0023>¹⁴⁹⁶ <http://lists.debian.org/debian-security-announce/2009/msg00124.html>¹⁴⁹⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10968>¹⁴⁹⁸ <http://rhn.redhat.com/errata/RHSA-2009-1107.html>¹⁴⁹⁹ <http://rhn.redhat.com/errata/RHSA-2009-1108.html>¹⁵⁰⁰ <http://secunia.com/advisories/34724/>¹⁵⁰¹ <http://secunia.com/advisories/35284/>¹⁵⁰² <http://secunia.com/advisories/35360/>¹⁵⁰³ <http://secunia.com/advisories/35395/>¹⁵⁰⁴ <http://secunia.com/advisories/35444/>¹⁵⁰⁵ <http://secunia.com/advisories/35487/>¹⁵⁰⁶ <http://secunia.com/advisories/35565/>¹⁵⁰⁷ <http://secunia.com/advisories/35710/>¹⁵⁰⁸ <http://secunia.com/advisories/35797/>¹⁵⁰⁹ <http://secunia.com/advisories/35843/>¹⁵¹⁰ <http://secunia.com/advisories/37221/>¹⁵¹¹ <http://xforce.iss.net/xforce/xfdb/50964>¹⁵¹² http://httpd.apache.org/security/vulnerabilities_22.html¹⁵¹³ <http://www.securityfocus.com/bid/6939>¹⁵¹⁴ <http://www.securityfocus.com/bid/6943>¹⁵¹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-1418>¹⁵¹⁶ <http://xforce.iss.net/xforce/xfdb/11438>¹⁵¹⁷ Entity tags predstavljaju mehanizam koji web serveri i web pretraživači koriste da se utvrdi da li komponenta u kešu pretraživača odgovara poreklu servera sa kog je poslata.

		zahtevani broj čvorova fajla da bi konstruisali 'Etag' heder za odgovor. Iako sama po sebi nije ranjivost, ova informacija olakšava sprovođenje određenih NFS napada. „Running vulnerable HTTP service: Apache 2.2.9. http://172.23.202.124/1: „3e008-d7-47c90fa668440““			
33.	Apache httpd Subrequest handling of request headers (mod_headers) (CVE-2010-0434) (http-apacherequest-header-info-disclosure)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Napadnuti deo je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_headers. Pregledajte konfiguraciju vašeg web servera radi validacije. Propust u jezgru "subrequest process code" može dovesti do greške tipa segmentation fault-a ili otkrivanja podataka iz nekog drugog zahteva na thread-ovima servera, kao što su worker ili winnt MPM-ovi. Zahvaljujući Philip Pickett-u iz Vmware ovaj propust je prijavljen i predložen je način ispravke.	BID 38494¹⁵¹⁸ CVE CVE-2010-0434¹⁵¹⁹ DEBIAN DSA-2035¹⁵²⁰ OVAL OVAL10358¹⁵²¹ OVAL OVAL8695¹⁵²² REDHAT RHSA-2010:0168¹⁵²³ REDHAT RHSA-2010:0175¹⁵²⁴ SECUNIA 39100¹⁵²⁵ SECUNIA 39115¹⁵²⁶ SECUNIA 39501¹⁵²⁷ SECUNIA 39628¹⁵²⁸ SECUNIA 39632¹⁵²⁹ SECUNIA 39656¹⁵³⁰ SECUNIA 40096¹⁵³¹ XF apache-http-rh-info-disclosure(56625)¹⁵³² URL1¹⁵³³	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz
34.	Apache Tomcat v4.x Example Scripts Information Leakage (http-tomcat-0005)	172.23.202.124:8080 172.23.202.220:8080 Sledeće skripte su navedene kao primeri koji dolaze sa Apache Tomcat-om v4.x, a koje napadači mogu da iskoriste da dobiju informacije o sistemu. Poznato je da su ove skripte ranjive na napad tipa "cross site scripting" (XSS): /examples/jsp/num/numguess.jsp /examples/jsp/dates/date.jsp /examples/jsp/snp/snoop.jsp /examples/jsp/error/error.html /examples/jsp/sessions/carts.html /examples/jsp/checkbox/check.html /examples/jsp/colors/colors.html /examples/jsp/cal/login.html /examples/jsp/include/include.jsp /examples/jsp/forward/forward.jsp /examples/jsp/plugin/plugin.jsp /examples/jsp/jsptoserv/jsptoservlet.jsp /examples/jsp/simpletag/foo.jsp		Kritičan	U potpunosti obrisati ove skripte. Primeri skripta nikad ne treba da budu instalirani na serverima koji su u produkciji.

¹⁵¹⁸ <http://www.securityfocus.com/bid/38494>¹⁵¹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0434>¹⁵²⁰ <http://www.debian.org/security/2010/dsa-2035>¹⁵²¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10358>¹⁵²² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8695>¹⁵²³ <http://rhn.redhat.com/errata/RHSA-2010-0168.html>¹⁵²⁴ <http://rhn.redhat.com/errata/RHSA-2010-0175.html>¹⁵²⁵ <http://secunia.com/advisories/39100/>¹⁵²⁶ <http://secunia.com/advisories/39115/>¹⁵²⁷ <http://secunia.com/advisories/39501/>¹⁵²⁸ <http://secunia.com/advisories/39628/>¹⁵²⁹ <http://secunia.com/advisories/39632/>¹⁵³⁰ <http://secunia.com/advisories/39656/>¹⁵³¹ <http://secunia.com/advisories/40096/>¹⁵³² <http://xforce.iss.net/xforce/xfdb/56625>¹⁵³³ http://httpd.apache.org/security/vulnerabilities_22.html

		/examples/jsp/mail/sendmail.jsp /examples/servlet/HelloWorldExample /examples/servlet/RequestInfoExample /examples/servlet/RequestHeaderExample /examples/servlet/RequestParamExample /examples/servlet/CookieExample /examples/servlet/IndiServlet /examples/servlet/SessionExample /tomcat-docs/appdev/sample/web/hello.jsp			
35.	OpenSSH CBC Mode Information Disclosure Vulnerability (ssh-openssh-cbc-mode-info-disclosure)	172.23.202.124:22 172.23.202.220:22 Određene verzije OpenSSH-a poseduju ranjivu implementaciju bloka šifarskog algoritma u CBC modu (Cipher Block Chaining). Ovo bi udaljenom napadaču moglo omogućiti da preko nepoznatih vektora pridobije određene podatke u vidu običnog teksta iz proizvoljnog bloka šifrovanog teksta u SSH sesiji.	BID 32319 ¹⁵³⁴ CVE CVE-2008-5161 ¹⁵³⁵ SECUNIA 32760 ¹⁵³⁶ URL1 ¹⁵³⁷ URL2 ¹⁵³⁸	Ozbiljan	Uraditi download a zatim instalirati: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-5.2p1.tar.gz Verzija 5.2 OpenSSH-a je puštena u promet 22. februara 2009.
36.	Self-signed TLS/SSL certificate (ssl-self-signed-certificate)	172.23.202.124:443 172.23.202.220:443 TLS/SSL-a sertifikat servera je samopotpisan. Samopotpisani sertifikati po defaultu nisu od poverenja, naročito zato što napadi na TLS/SSL preko posrednika obično koriste samopotpisane sertifikate da prisluškuju TLS/SSL veze.		Ozbiljan	Nabaviti novi TLS/SSL serverov sertifikat koji NIJE samopotpisan i instalirati ga na server. Precizna uputstva za dobijanje novog sertifikata zavise od zahteva organizacije. Uopšteno, treba napraviti zahtev za sertifikat i taj zahtev sačuvati kao fajl. Ovaj fajl se zatim šalje Certificate Authority-ju (CA) na obradu. Organizacija možda poseduje sopstveni interni Certificate Authority. U suprotnom, potrebno je platiti sertifikat iz spoljnog poverljivog Certificate Authority-ja, kao što su Thawte ¹⁵³⁹ , Verisign ¹⁵⁴⁰ .
37.	Autocomplete enabled for sensitive HTML form fields (spider-sensitive-form-data-autocomplete-enabled)	172.23.202.124:8080 172.23.202.220:8080 Web forma sadrži lozinke i druge rubrike sa osetljivim tekstom za koje je otvorena mogućnost auto-complete od strane web pretraživača. Funkcija auto-complete skladišti forme popunjenih rubrika i lozinke lokalno, na web pretraživaču, tako da se ove rubrike automatski popunjavaju kada korisnik ponovo poseti sajt. Osetljivi podaci i lozinke mogu biti ukradeni ako je korisnikov sistem kompromitovan.		Umeren	Za svaku osetljivu rubriku u HTML, stavku „autocomplete“ potrebno je podesiti na „off“. Na primer: <input type=“password“ autocomplete=“off“ name=“pw“> Ako ima previše rubrika, možda je brže podesiti stavku „autocomplete“ na „off“ u spoljnom tagu <form>. Na primer: <form action=“/login.jsp“ autocomplete=“off“

¹⁵³⁴ <http://www.securityfocus.com/bid/32319>¹⁵³⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-5161>¹⁵³⁶ <http://secunia.com/advisories/32760/>¹⁵³⁷ http://www.cpni.gov.uk/Docs/Vulnerability_Advisory_SSH.txt, pristupljeno 20.12.2011¹⁵³⁸ <http://www.openssh.com/txt/cbc.adv>¹⁵³⁹ <http://www.thawte.com/>¹⁵⁴⁰ <http://www.verisign.com/>

		Međutim, treba imati u vidu da forma auto-complete nije standardna i da je to karakteristika web pretraživača koju svaki web pretraživač tretira na različit način. Na primer Opera zanemaruje ovu opciju i zahteva od korisnika da unese poverljive podatke svaki put kada posećuje određeni web sajt.			name="pw"> <input type="password" name="pw"> </form>
38.	Apache Tomcat default installation/welcome page installed (http-tomcat-default-install-page)	172.23.202.124:8080 172.23.202.220:8080 Tomcat difoltna instalacija ili „Welcome“ stranica je instalirana na serveru. To obično ukazuje na novoinstalirani server. U mnogim slučajevima, Tomcat se instalira zajedno sa drugim aplikacijama i korisnik možda nije svestan da je web server pokrenut. Ovakvi serveri se retko patch-uju i još rede nadgledaju, što zlonamernim napadačima postaje pogodna meta koja najverovatnije neće pokrenuti nikakvo upozorenje.		Umeren	Ako se od servera zahteva da obezbedi neophodnu funkcionalnost, onda difoltnu stranicu treba zameniti odgovarajućim sadržajem. U suprotnom, ovakav server treba ukloniti sa mreže, prateći bezbednosni princip minimalne složenosti (više složenosti = manja bezbednost). ¹⁵⁴¹
39.	Database Open Access (database-open-access)	172.23.202.124:3306 172.23.202.220:3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se ograničenje direktnog pristupa poverljivim sistemima jer mogu sadržavati osetljive podatke, a ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posjedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnim mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7.	URL ¹⁵⁴²	Umeren	Konfigurisati server baze podataka tako da omogući pristup samo proverenim sistemima. Na primer, PCI DSS standard zahteva da se postavi baza podataka na internu mrežu, odvojenu od DMZ.
40.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatišu slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	CVE CVE-1999-0524 ¹⁵⁴³ OSVDB 95 ¹⁵⁴⁴ XF icmp-netmask(306) ¹⁵⁴⁵ XF icmp-timestamp(322) ¹⁵⁴⁶	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost
41.	WebDAV Extensions are Enabled (http-	172.23.202.124:8080 172.23.202.220:8080		Umeren	Apache Onemogućiti WebDAV ¹⁵⁴⁷ za Apache

¹⁵⁴¹ Prema Bruce Schneier-u : "Budućnost digitalnih sistema jeste kompleksnost, a kompleksnost je najgori neprijatelj bezbednosti." Preuzeto iz <http://www.mccabe.com/pdf/More%20Complex%20Equals%20Less%20Secure-McCabe.pdf> , pristupljeno 10.10.2012.

¹⁵⁴² https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf

¹⁵⁴³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>

¹⁵⁴⁴ <http://www.osvdb.org/95>

¹⁵⁴⁵ <http://xforce.iss.net/xforce/xfdb/306>

¹⁵⁴⁶ <http://xforce.iss.net/xforce/xfdb/322>

	generic-webdav-enabled)	WebDAV je skup ekstenzija za HTTP protokol koji omogućava korisnicima da zajednički edituju i obrađuju fajlove na udaljenim web serverima. Mnogi web serveri po defaultu omogućavaju WebDAV ekstenzije, čak i kada nisu potrebne. S obzirom na dodatnu složenost, dosadašnja praksa je pokazala da treba onemogućiti WebDAV ukoliko se trenutno ne koristi.			Proverite da li je mod_dav modul isključen ili utvrdite da postoji zahtev za autentifikaciju na direktorijumima na kojima se zahteva DAV. Apache Tomcat, Tomcat, Tomcat Web Server Onemogućite WebDAV za Apache Tomcat Isključite WebDAV Servlet ¹⁵⁴⁸ za sve web aplikacije koje se nalaze na web serveru. To se može uraditi tako što se ukloni definicija servlet-a za WebDAV (kategorija org.apache.catalina.servlets.WebdavServlet) i uklone sve servlet mape koje se pozivaju na WebDAV servlet.
42.	Apache HTTPD: CRLF injection in mod_negotiation when untrusted uploads are supported	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_negotiation. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Moguće je ubaciti CRLF (Carriage Return and Line Feed) koji omogućava CRLF Injection napade (poznatih kao HTTP Response Splitting) za sajtove koji koriste mod_negotiation, omogućavajući neproverene aploudove na lokacije na kojima je omogućen MultiViews (višestruko pregledanje).	APPLE APPLE-SA-2009-05-12 ¹⁵⁴⁹ BID 27409 ¹⁵⁵⁰ CERT TA09-133A ¹⁵⁵¹ CVE CVE-2008-0456 ¹⁵⁵² SECUNIA 29348 ¹⁵⁵³ SECUNIA 35074 ¹⁵⁵⁴ URL1 ¹⁵⁵⁵	Umeren	Apache HTTPD >= 2.2 and < 2.2.12 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz
43	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom se koristi za procenu vremena neprekidnog rada udaljenog hosta (što zlonamerni napadač može iskoristiti pri planiranju daljih napada). Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1 ¹⁵⁵⁶ URL2 ¹⁵⁵⁷ URL3 ¹⁵⁵⁸	Umeren	Onemogućiti TCP vremenske pečate na Linux-u. Podesiti vrednost net.ipv4.tcp_timestamps na 0 pokretanjem sledeće komande: sysctl -w net.ipv4.tcp_timestamps=0 Uz to, sledeću vrednost staviti u defaultni sysctl konfiguracioni fajl,

¹⁵⁴⁷ WebDAV je otvoreni standar za nabavku i prenos podataka putem računarskih mreža. Pri tome korisnici vizuelno dolaze do podataka kao da su na sopstvenom računaru. Preuzeto iz : <http://sr.wikipedia.org/sr/WebDAV> , 12.09.2012.

¹⁵⁴⁸ Servlet je objekat programskog jezika Java koji dinamički obrađuje zahteve i konstruiše odgovor na zahtev. Java servlet API omogućava Java programerima da dodaju dinamički sadržaj Web serveru korišćenjem Java platforme. Servlet najčešće generiše HTML kod, ali to može biti i XML ili nešto slično. Preuzeto iz : <http://sr.wikipedia.org/sr/Servlet>

¹⁵⁴⁹ <http://lists.apple.com/archives/security-announce/2009/May/msg00001.html>

¹⁵⁵⁰ <http://www.securityfocus.com/bid/27409>

¹⁵⁵¹ <http://www.us-cert.gov/ncas/alerts/ta09-133a>

¹⁵⁵² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0456>

¹⁵⁵³ <http://secunia.com/advisories/29348/>

¹⁵⁵⁴ <http://secunia.com/advisories/35074/>

¹⁵⁵⁵ http://httpd.apache.org/security/vulnerabilities_22.html

¹⁵⁵⁶ http://www.forensicswiki.org/wiki/TCP_timestamps

¹⁵⁵⁷ <http://www.ietf.org/rfc/rfc1323.txt>

¹⁵⁵⁸ <http://uptime.netcraft.com/>

					uopšteno sysctl.conf: net.ipv4.tcp_timestamps=0

Tabela 69. Linux OS – Pronađeni servisi na IP adresi 172.23.202.124 (2011. godina)

SERVISI	CIFS¹⁵⁵⁹, CIFS Name Service¹⁵⁶⁰ : advertised-name-1: mandriva52enx86 (Computer Name) FTP 172.23.202.124 tcp 21 : vsFTPD 2.2.2, ftp.banner: 220 (vsFTPD 2.2.2) HTTP 172.23.202.124 tcp 80 Apache 2.2.9 http.banner: Apache/2.2.9 (Mandriva Linux/PREFORK-12.10mdvmes5.1) 172.23.202.124 tcp 8080 Apache Tomcat 5.5.28 HTTPS 172.23.202.124 tcp 443 Apache 2.2.9 http.banner: Apache/2.2.9 (Mandriva Linux/PREFORK-12.10mdvmes5.1) IBM AS400 Management Central 172.23.202.124 tcp 5555 MySQL 172.23.202.124 tcp 3306 SSH 172.23.202.124 tcp 22 OpenSSH 5.1 ssh.banner: SSH-2.0-OpenSSH_5.1
Spidered Web site	http://172.23.202.124:80 Common Default URLs: <i>Access Error (403)</i> addon-modules cgi-bin error icons login.cgi Guessed URLs <i>Access Error (403)</i> addon-modules %3f.jsp .svn entries ?P=+Adw-script+AD4-alert(42)+Adwscript+AD4-script+AD4-script+AD4-script+AD4-Adw-script AD4-alert(42) Adwscript AD4- CVS Entries Root

¹⁵⁵⁹ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

¹⁵⁶⁰ Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	DEADJOE Trace.axd WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config cgi-bin error icons index.CGI index.cgi index.cgi. index.cgi.bak index.cgi.old index.cgi.tmp info2www.cgi login.CGI login.cgi. login.cgi.bak login.cgi.old login.cgi.tmp <i>Successful (200)</i> ?P=+Adw-script+AD4-alert(42)+Adwscript+AD4-index.html http://172.23.202.124:8080 Common Default URLs The following URLs were guessed. They are often included with default web server or web server add-on installations. <i>Successful (200)</i> admin tomcat-docs Guessed URLs The following URLs were guessed using various tricks based on the discovered web site content. <i>Error (400)</i> index.jsp%00 index.jsp%5C jsp-examples cal cal1.jsp%00 cal1.jsp%00 cal1.jsp%5C cal1.jsp%5C checkbox checkresult.jsp%00 checkresult.jsp%00 checkresult.jsp%5C checkresult.jsp%5C colors colrs.jsp%00 colrs.jsp%00 colrs.jsp%5C colrs.jsp%5C dates date.jsp%00 date.jsp%00 date.jsp%5C jsp-examples cal cal1.jsp%00 cal1.jsp%00

	cal1.jsp%5C cal1.jsp%5C checkbox checkresult.jsp%00 checkresult.jsp%00 checkresult.jsp%5C checkresult.jsp%5C colors colrs.jsp%00 colrs.jsp%00 colrs.jsp%5C colrs.jsp%5C dates date.jsp%00 date.jsp%00 date.jsp%5C date.jsp%5C error err.jsp%00 err.jsp%00 err.jsp%5C err.jsp%5C errorpge.jsp%00 errorpge.jsp%5C forward forward.jsp%00 forward.jsp%00 forward.jsp%5C forward.jsp%5C include foo.jsp%00 foo.jsp%5C include.jsp%00 include.jsp%00 book.jsp%00 book.jsp%5C book.jsp%5C hello.jsp%00 hello.jsp%00 hello.jsp%5C hello.jsp%5C repeat.jsp%00 repeat.jsp%00 repeat.jsp%5C repeat.jsp%5C foo.jsp%00 foo.jsp%00 foo.jsp%5C foo.jsp%5C tagfiles hello.jsp%00 hello.jsp%00 hello.jsp%5C hello.jsp%5C panel.jsp%00 panel.jsp%00 panel.jsp%5C panel.jsp%5C products.jsp%00 products.jsp%00 products.jsp%5C products.jsp%5C xml xml.jsp%00 xml.jsp%00 xml.jsp%5C xml.jsp%5C

	<i>Requires Authentication (401)</i> manager jmxproxy %3f.jsp .svn entries ?P=+Adw-script+AD4-alert(42)+Adwscript+AD4- Adw-script AD4-alert(42) Adwscript AD4- CVS Entries Root DEADJOE Trace.axd WS_FTP.LOG <i>Successful (200)</i> ?P=+Adw-script+AD4-alert(42)+Adwscript+AD4- script+AD4- script+AD4- script+AD4- script+AD4- script+AD4- script+AD4- script+AD4- script+AD4- admin %3f.jsp default.html default.jsp error.jsp index.html index.jsp login.jsp index.jsp jsp-examples forward two.html two.html include foo.jsp foo.jsp index.html index.html security protected %3f.jsp svn entries Adw-script AD4-alert(42) Adwscript AD4- CVS Entries Root DEADJOE README README.TXT Trace.axd WEB-INF WS_FTP.LOG Web.sitemap _vti_bin _vti_bot _vti_cnf

	_vti_log _vti_pvt default.aspx default.htm default.html default.jsp default.php default.shtml default.wml index.asp index.aspx index.bak index.cfm index.cgi index.shtml servlets-examples index.html tomcat-docs appdev printer sample index.html architecture printer https://172.23.202.124:443 Common Default URLs The following URLs were guessed. They are often included with default web server or web server add-on installations. <i>Access Error (403)</i> cgi-bin error icons login.cgi Guessed URLs The following URLs were guessed using various tricks based on the discovered web site content. <i>Access Error (403)</i> cgi-bin ?P=+Adw-script+AD4-alert(42)+Adwscript+ AD4- script+AD4- script+AD4- error icons index.CGI index.cgi index.cgi. index.cgi.bak index.cgi.old cgi.tmp info2www.cgi login.CGI login.cgi. login.cgi.bak login.cgi.old login.cgi.tmp Linked URLs The following URLs were found as links in the content of other web pages. <i>Redirect (302)</i> admin balancer

	BlahBlah?paramName=paramValue News manager tomcat-docs Successful (200) ?P=+Adw-script+AD4-alert(42)+Adwscript+AD4-index.html

Tabela 70. Linux OS – Pronađeni servisi na IP adresi 172.23.202.220 (2011. godina)

SERVISI	CIFS¹⁵⁶¹, CIFS Name Service¹⁵⁶² : advertised-name-1: mandriva52enx64 (Computer Name) FTP 172.23.202.220 tcp 21 : vsFTPD 2.2.2, ftp.banner: 220 (vsFTPD 2.2.2) HTTP 172.23.202.220 tcp 80 Apache 2.2.9 http.banner: Apache/2.2.9 (Mandriva Linux/PREFORK-12.10mdvmes5.1) 172.23.202.220 tcp 8080 Apache Tomcat 5.5.28 HTTPS 172.23.202.220 tcp 443 Apache 2.2.9 http.banner: Apache/2.2.9 (Mandriva Linux/PREFORK-12.10mdvmes5.1) IBM AS400 Management Central 172.23.202.220 tcp 5555 MySQL 172.23.202.220 tcp 3306 SSH 172.23.202.220 tcp 22 OpenSSH 5.1 ssh.banner: SSH-2.0-OpenSSH_5.1
Spidered Web site	http://172.23.202.220:80 Common Default URLs: Access Error (403) addon-modules cgi-bin error icons login.cgi Guessed URLs Access Error (403) addon-modules %3f.jsp .svn entries ?P=+Adw-script+AD4-alert(42)+Adwscript+AD4-script+AD4-script+AD4-

¹⁵⁶¹ CIFS ili Common Internet File System definisan je od strane Microsoft-a da obezbedi servis deljenja datoteka preko Interneta. Proširuje SMB ili Server Message Block protokol dizajniran od strane IBM-a. CIFS obezbeđuje mehanizam za deljenje resursa (fajlova, štampača i dr.) i izvršava pozive udaljenih procedura (RPC).

¹⁵⁶² Ovaj servis se koristi za obradu zahteva za CIFS pretraživanja (imena). Odgovori sadrže imena i vrste usluge kojima se može pristupiti preko CIFS-a.

	script+AD4- Adw-script AD4-alert(42) Adwscript AD4- CVS Entries Root DEADJOE Trace.axd WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config cgi-bin error icons index.CGI index.cgi index.cgi. index.cgi.bak index.cgi.old index.cgi.tmp info2www.cgi login.CGI login.cgi. login.cgi.bak login.cgi.old login.cgi.tmp Successful (200) ?P=+Adw-script+AD4-alert(42)+Adwscript+ AD4- index.html http://172.23.202.220:8080 Common Default URLs The following URLs were guessed. They are often included with default web server or web server add-on installations. Successful (200) admin tomcat-docs Guessed URLs The following URLs were guessed using various tricks based on the discovered web site content. Error (400) index.jsp%00 index.jsp%5C jsp-examples cal cal1.jsp%00 cal1.jsp%00 cal1.jsp%5C cal1.jsp%5C checkbox checkresult.jsp%00 checkresult.jsp%00 checkresult.jsp%5C checkresult.jsp%5C colors colrs.jsp%00 colrs.jsp%00 colrs.jsp%5C colrs.jsp%5C dates date.jsp%00

	date.jsp%00 date.jsp%5C jsp-examples cal cal1.jsp%00 cal1.jsp%00 cal1.jsp%5C cal1.jsp%5C checkbox checkresult.jsp%00 checkresult.jsp%00 checkresult.jsp%5C checkresult.jsp%5C colors colrs.jsp%00 colrs.jsp%00 colrs.jsp%5C colrs.jsp%5C dates date.jsp%00 date.jsp%00 date.jsp%5C date.jsp%5C error err.jsp%00 err.jsp%00 err.jsp%5C err.jsp%5C errorpge.jsp%00 errorpge.jsp%5C forward forward.jsp%00 forward.jsp%00 forward.jsp%5C forward.jsp%5C include foo.jsp%00 foo.jsp%5C include.jsp%00 include.jsp%00 book.jsp%00 book.jsp%5C book.jsp%5C hello.jsp%00 hello.jsp%00 hello.jsp%5C hello.jsp%5C repeat.jsp%00 repeat.jsp%00 repeat.jsp%5C repeat.jsp%5C foo.jsp%00 foo.jsp%00 foo.jsp%5C foo.jsp%5C tagfiles hello.jsp%00 hello.jsp%00 hello.jsp%5C hello.jsp%5C panel.jsp%00 panel.jsp%00 panel.jsp%5C panel.jsp%5C products.jsp%00 products.jsp%00 products.jsp%5C

	products.jsp%5C xml xml.jsp%00 xml.jsp%00 xml.jsp%5C xml.jsp%5C <i>Requires Authentication (401)</i> manager jmxproxy %3f.jsp .svn entries ?P=+Adw-script+AD4-alert(42)+Adwscript+AD4- Adw-script AD4-alert(42) Adwscript AD4- CVS Entries Root DEADJOE Trace.axd WS_FTP.LOG <i>Successful (200)</i> ?P=+Adw-script+AD4-alert(42)+Adwscript+AD4- script+AD4- script+AD4- script+AD4- script+AD4- script+AD4- script+AD4- script+AD4- script+AD4- script+AD4- admin %3f.jsp default.html default.jsp error.jsp index.html index.jsp login.jsp index.jsp jsp-examples forward two.html two.html include foo.jsp foo.jsp index.html index.html security protected %3f.jsp svn entries Adw-script AD4-alert(42) Adwscript AD4- CVS Entries Root DEADJOE README README.TXT

	Trace.axd WEB-INF WS_FTP.LOG Web.sitemap _vti_bin _vti_bot _vti_cnf _vti_log _vti_pvt default.aspx default.htm default.html default.jsp default.php default.shtml default.wml index.asp index.aspx index.bak index.cfm index.cgi index.shtml servlets-examples index.html tomcat-docs appdev printer sample index.html architecture printer https://172.23.202.220:443 Common Default URLs The following URLs were guessed. They are often included with default web server or web server add-on installations. <i>Access Error (403)</i> cgi-bin error icons login.cgi Guessed URLs The following URLs were guessed using various tricks based on the discovered web site content. <i>Access Error (403)</i> cgi-bin ?P=+Adw-script+AD4-alert(42)+Adwscript+AD4-script+AD4-script+AD4-error icons index.CGI index.cgi index.cgi. index.cgi.bak index.cgi.old cgi.tmp info2www.cgi login.CGI login.cgi. login.cgi.bak login.cgi.old

	login.cgi.tmp Linked URLs The following URLs were found as links in the content of other web pages. Redirect (302) admin balancer BlahBlah?paramName=paramValue News manager tomcat-docs Successful (200) ?P=+Adw-script+AD4-alert(42)+Adwscript+AD4-index.html

Tabela 71. Linux OS sa IP adresama 172.23.202.126, 172.23.202.225 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.126		OS: Red Hat Enterprise Linux 4.8 AS x64, rhel48asx64			50
IP adresa: 172.23.202.225		OS: Red Hat Enterprise Linux 4.8 AS x86, rhel48asx86			50
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Apache httpd APR apr_palloc heap overflow (CVE-2009-2412) (apache-httpd-cve-2009-2412)	172.23.202.126:80 172.23.202.225:80 U modulu apr_palloc() je pronađen propust u sklopu APR-a, koji može prouzrokovati velika preopterećenja u programima koji pokušaju da kontrolišu apr_palloc() veličinu zadatu od strane korisnika. Sam Apache HTTP server ne dopušta prolaz ka ovoj funkciji neproverenim veličinama koje zadaje korisnik, tako da se on može pokrenuti samo preko neke druge aplikacije koja koristi apr_palloc() na ranjiv način.	APPLE APPLE-SA-2009-11-09 ¹⁵⁶³ BID 35949 ¹⁵⁶⁴ CVE CVE-2009-2412 ¹⁵⁶⁵ OSVDB 56765 ¹⁵⁶⁶ OSVDB 56766 ¹⁵⁶⁷ OVAL OVAL8394 ¹⁵⁶⁸ OVAL OVAL9958 ¹⁵⁶⁹ SECUNIA 36138 ¹⁵⁷⁰ SECUNIA 36140 ¹⁵⁷¹ SECUNIA 36166 ¹⁵⁷² SECUNIA 36233 ¹⁵⁷³ SECUNIA 37152 ¹⁵⁷⁴ SECUNIA 37221 ¹⁵⁷⁵ SUSE SA:2009:050 ¹⁵⁷⁶ URL1 ¹⁵⁷⁷	Kritičan	Apache >= 2.0 and < 2.1 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
2.	Apache httpd mod_isapi module unload flaw (CVE-2010-0425) (http-	172.23.202.126:80 172.23.202.225:80 U modulu mod_isapi je pronađen	BID 38494 ¹⁵⁷⁸ CERT-VN 280613 ¹⁵⁷⁹ CVE CVE-2010-0425 ¹⁵⁸⁰	Kritičan	Apache >= 2.0 and < 2.1 Uradi download a zatim instalirati:

¹⁵⁶³ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>¹⁵⁶⁴ <http://www.securityfocus.com/bid/35949>¹⁵⁶⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2412>¹⁵⁶⁶ <http://osvdb.org/56765>¹⁵⁶⁷ <http://osvdb.org/56766>¹⁵⁶⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8394>¹⁵⁶⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9958>¹⁵⁷⁰ <http://secunia.com/advisories/36138/>¹⁵⁷¹ <http://secunia.com/advisories/36140/>¹⁵⁷² <http://secunia.com/advisories/36166/>¹⁵⁷³ <http://secunia.com/advisories/36233/>¹⁵⁷⁴ <http://secunia.com/advisories/37152/>¹⁵⁷⁵ <http://secunia.com/advisories/37221/>¹⁵⁷⁶ <https://www.suse.com/support/security/advisories/>¹⁵⁷⁷ http://httpd.apache.org/security/vulnerabilities_20.html¹⁵⁷⁸ <http://www.securityfocus.com/bid/38494>¹⁵⁷⁹ <http://www.kb.cert.org/vuls/id/280613>¹⁵⁸⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0425>

	apache-mod_isapi-module-unload-flaw)	propust koji će pokušati da ukloni ISAPI dll kada naide na greške. To može ostaviti povratne pozive u nedefinisanoj stanju greške i kao posledica može da se javi segmentation fault. Na Windows platformama koje koriste mod_isapi, udaljeni napadač bi mogao da pošalje zlonameran zahtev da pokrene ovaj problem, a kako win32 MPM pokreće samo jedan proces, to bi kao ishod imalo odbijanje servisa i potencijalno dozvolilo da se pokrene proizvoljan kôd. Napomena: Zahvaljujući Brett Gervasoni-ju iz "Sense of Security" ovaj problem je prijavljen i za njega je predložena zakrpa.	OVAL OVAL8439¹⁵⁸¹ SECUNIA 38978¹⁵⁸² SECUNIA 39628¹⁵⁸³ XF apache-http-modisapi-ocp- unspecified(56624)¹⁵⁸⁴ URL1¹⁵⁸⁵		http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
3.	Apache httpd SSLVerifyClient bypass (CVE-2005-2700) (http-mod_ssl-client-auth-bypass)	172.23.202.126:80 172.23.202.225:80 Pronađen je servis koji ima propust u mod_ssl obradi direktive „SSLVerifyClient“. Ranjivost će se pojaviti ako je virtuelan host konfigurisan korišćenjem „SSLVerifyClient optional“ i dodatno ako je direktiva „SSLVerifyClient required“ podešena za specifičnu lokaciju. Za servere konfigurisane na ovaj način, napadač bi mogao da pristupi izvorima koji bi inače bili zaštićeni, jer se prilikom povezivanja ne traži klijentski sertifikat.	BID 14721¹⁵⁸⁶ CERT-VN 744929¹⁵⁸⁷ CVE CVE-2005-2700¹⁵⁸⁸ OSVDB 19188¹⁵⁸⁹ OVAL OVAL10416¹⁵⁹⁰ REDHAT RHSA-2005:608¹⁵⁹¹ REDHAT RHSA-2005:773¹⁵⁹² REDHAT RHSA-2005:816¹⁵⁹³ SECUNIA 16700¹⁵⁹⁴ SECUNIA 16705¹⁵⁹⁵ SECUNIA 16714¹⁵⁹⁶ SECUNIA 16743¹⁵⁹⁷ SECUNIA 16746¹⁵⁹⁸ SECUNIA 16748¹⁵⁹⁹ SECUNIA 16753¹⁶⁰⁰ SECUNIA 16754¹⁶⁰¹ SECUNIA 16769¹⁶⁰² SECUNIA 16771¹⁶⁰³ SECUNIA 16789¹⁶⁰⁴ SECUNIA 16864¹⁶⁰⁵ SECUNIA 16956¹⁶⁰⁶ SECUNIA 17088¹⁶⁰⁷	Kritičan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.55.tar.gz

¹⁵⁸¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8439>

¹⁵⁸² <http://secunia.com/advisories/38978/>

¹⁵⁸³ <http://secunia.com/advisories/39628/>

¹⁵⁸⁴ <http://xforce.iss.net/xforce/xfdb/56624>

¹⁵⁸⁵ http://httpd.apache.org/security/vulnerabilities_20.html

¹⁵⁸⁶ <http://www.securityfocus.com/bid/14721>

¹⁵⁸⁷ <http://www.kb.cert.org/vuls/id/744929>

¹⁵⁸⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2700>

¹⁵⁸⁹ <http://www.osvdb.org/19188>

¹⁵⁹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10416>

¹⁵⁹¹ <http://rhn.redhat.com/errata/RHSA-2005-608.html>

¹⁵⁹² <http://rhn.redhat.com/errata/RHSA-2005-773.html>

¹⁵⁹³ <http://rhn.redhat.com/errata/RHSA-2005-816.html>

¹⁵⁹⁴ <http://secunia.com/advisories/16700/>

¹⁵⁹⁵ <http://secunia.com/advisories/16705/>

¹⁵⁹⁶ <http://secunia.com/advisories/16714/>

¹⁵⁹⁷ <http://secunia.com/advisories/16743/>

¹⁵⁹⁸ <http://secunia.com/advisories/16746/>

¹⁵⁹⁹ <http://secunia.com/advisories/16748/>

¹⁶⁰⁰ <http://secunia.com/advisories/16753/>

¹⁶⁰¹ <http://secunia.com/advisories/16754/>

¹⁶⁰² <http://secunia.com/advisories/16769/>

¹⁶⁰³ <http://secunia.com/advisories/16771/>

¹⁶⁰⁴ <http://secunia.com/advisories/16789/>

¹⁶⁰⁵ <http://secunia.com/advisories/16864/>

¹⁶⁰⁶ <http://secunia.com/advisories/16956/>

¹⁶⁰⁷ <http://secunia.com/advisories/17088/>

			SECUNIA 17288 ¹⁶⁰⁸ SECUNIA 17311 ¹⁶⁰⁹ SECUNIA 17813 ¹⁶¹⁰ SECUNIA 19072 ¹⁶¹¹ SECUNIA 19073 ¹⁶¹² SECUNIA 21848 ¹⁶¹³ SECUNIA 22523 ¹⁶¹⁴ SUSE SA:2005:051 ¹⁶¹⁵ SUSE SA:2005:052 ¹⁶¹⁶ SUSE SA:2006:051 ¹⁶¹⁷ SUSE SA:2006:051 ¹⁶¹⁸ URL1 ¹⁶¹⁹		
4.	Apache httpd mod_proxy_ftp FTP command injection (CVE-2009-3095) (apache-httpd- 2_0_xmod_ proxy_ftp-ftp- command-injection- cve-2009-3095)	172.23.202.126:80 172.23.202.225:80 U modulu mod_proxy_ftp je pronađen propust. U reverznoj proxy konfiguraciji, udaljeni napadač bi mogao da iskoristi ovaj defekt da zaobide uobičajenu zabranu pristupa tako što bi kreirao pažljivo izrađen HTTP Authorization heder, koji omogućava napadaču da šalje proizvoljne komande FTP serveru.	APPLE APPLE-SA- 2010-03-29 ¹⁶²⁰ CVE CVE-2009-3095 ¹⁶²¹ DEBIAN DSA-1934 ¹⁶²² OVAL OVAL8662 ¹⁶²³ OVAL OVAL9363 ¹⁶²⁴ SECUNIA 37152 ¹⁶²⁵ SUSE SA:2009:050 ¹⁶²⁶ URL1 ¹⁶²⁷	Kritičan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
5.	Apache httpd mod_rewrite off-by-one error (CVE-2006-3747) (http-apache-mod- rewrite-bof)	172.23.202.126:80 172.23.202.225:80 Propust prepunjavanja bafera off-by- one je otkriven u modulu mod_rewrite. U zavisnosti od toga na koji je način kompajliran Apache httpd, ovaj propust softvera može dovesti do ranjivosti koja bi, u kombinaciji sa određenim tipovima pravila Rewrite-a u konfiguracionim fajlovima web servera, mogla biti	APPLE APPLE-SA- 2008-03-18 ¹⁶²⁸ BID 19204 ¹⁶²⁹ CERT TA08-150A ¹⁶³⁰ CERT-VN 395412 ¹⁶³¹ CVE CVE-2006-3747 ¹⁶³² DEBIAN DSA-1131 ¹⁶³³ DEBIAN DSA-1132 ¹⁶³⁴ OSVDB 27588 ¹⁶³⁵ SECUNIA 21197 ¹⁶³⁶ SECUNIA 21241 ¹⁶³⁷ SECUNIA 21245 ¹⁶³⁸	Kritičan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.59.tar.gz

¹⁶⁰⁸ <http://secunia.com/advisories/17288/>¹⁶⁰⁹ <http://secunia.com/advisories/17311/>¹⁶¹⁰ <http://secunia.com/advisories/17813/>¹⁶¹¹ <http://secunia.com/advisories/19072/>¹⁶¹² <http://secunia.com/advisories/19073/>¹⁶¹³ <http://secunia.com/advisories/21848/>¹⁶¹⁴ <http://secunia.com/advisories/22523/>¹⁶¹⁵ <https://www.suse.com/support/security/advisories/>¹⁶¹⁶ <https://www.suse.com/support/security/advisories/>¹⁶¹⁷ <https://www.suse.com/support/security/advisories/>¹⁶¹⁸ <https://www.suse.com/support/security/advisories/>¹⁶¹⁹ http://httpd.apache.org/security/vulnerabilities_20.html¹⁶²⁰ <http://lists.apple.com/archives/security-announce/2010/Mar/msg00001.html>¹⁶²¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3095>¹⁶²² <http://www.debian.org/security/2009/dsa-1934>¹⁶²³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8662>¹⁶²⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9363>¹⁶²⁵ <http://secunia.com/advisories/37152/>¹⁶²⁶ <https://www.suse.com/support/security/advisories/>¹⁶²⁷ http://httpd.apache.org/security/vulnerabilities_20.html¹⁶²⁸ <http://lists.apple.com/archives/security-announce/2008/Mar/msg00000.html>¹⁶²⁹ <http://www.securityfocus.com/bid/19204>¹⁶³⁰ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>¹⁶³¹ <http://www.kb.cert.org/vuls/id/395412>¹⁶³² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-3747>¹⁶³³ <http://lists.debian.org/debian-security-announce/2006/msg00219.html>¹⁶³⁴ <http://lists.debian.org/debian-security/2006/08/msg00000.html>¹⁶³⁵ <http://www.osvdb.org/27588>¹⁶³⁶ <http://secunia.com/advisories/21197/>¹⁶³⁷ <http://secunia.com/advisories/21241/>

		aktivirana iz daleka. Posledice ove od ranjivosti bi mogle uključivati odbijanje servisa (obaranje procesa web servera) ili potencijalno omogućavanje pokretanja proizvoljnog kôda.	SECUNIA 21247 ¹⁶³⁹ SECUNIA 21266 ¹⁶⁴⁰ SECUNIA 21273 ¹⁶⁴¹ SECUNIA 21284 ¹⁶⁴² SECUNIA 21307 ¹⁶⁴³ SECUNIA 21313 ¹⁶⁴⁴ SECUNIA 21315 ¹⁶⁴⁵ SECUNIA 21346 ¹⁶⁴⁶ SECUNIA 21478 ¹⁶⁴⁷ SECUNIA 21509 ¹⁶⁴⁸ SECUNIA 22262 ¹⁶⁴⁹ SECUNIA 22368 ¹⁶⁵⁰ SECUNIA 22388 ¹⁶⁵¹ SECUNIA 22523 ¹⁶⁵² SECUNIA 23028 ¹⁶⁵³ SECUNIA 23260 ¹⁶⁵⁴ SECUNIA 26329 ¹⁶⁵⁵ SECUNIA 29420 ¹⁶⁵⁶ SECUNIA 29849 ¹⁶⁵⁷ SECUNIA 30430 ¹⁶⁵⁸ SUSE SUSE-SA:2006:043 ¹⁶⁵⁹ XF apache-modrewrite-offbyone-bo(28063) ¹⁶⁶⁰ URL1 ¹⁶⁶¹		
6.	Apache httpd SSLCipherSuite bypass (CVE-2004-0885) (http://apache2-mod-ssl-ciphersuite-bypass)	172.23.202.126:80 172.23.202.225:80 Problem je otkriven u modulu mod_ssl ukoliko je konfigurisan tako da koristi „SSLCipherSuite“ direktivu u kontekstu direktorijuma ili lokacije. Ako je određena lokacija konfigurisana tako da zahteva određene skupove šifara, onda će klijent biti u mogućnosti da pristupi toj lokaciji koristeći bilo koji skup šifara koji dozvoljava virtuelna konfiguracija host-a.	BID 11360 ¹⁶⁶² CVE CVE-2004-0885 ¹⁶⁶³ OVAL OVAL10384 ¹⁶⁶⁴ REDHAT RHSA-2004:562 ¹⁶⁶⁵ REDHAT RHSA-2004:600 ¹⁶⁶⁶ REDHAT RHSA-2005:816 ¹⁶⁶⁷ REDHAT RHSA-2008:0261 ¹⁶⁶⁸ SECUNIA 19072 ¹⁶⁶⁹ XF apache-sslciphersuite-	Kritičan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.53.tar.gz

¹⁶³⁸ <http://secunia.com/advisories/21245/>¹⁶³⁹ <http://secunia.com/advisories/21247/>¹⁶⁴⁰ <http://secunia.com/advisories/21266/>¹⁶⁴¹ <http://secunia.com/advisories/21273/>¹⁶⁴² <http://secunia.com/advisories/21284/>¹⁶⁴³ <http://secunia.com/advisories/21307/>¹⁶⁴⁴ <http://secunia.com/advisories/21313/>¹⁶⁴⁵ <http://secunia.com/advisories/21315/>¹⁶⁴⁶ <http://secunia.com/advisories/21346/>¹⁶⁴⁷ <http://secunia.com/advisories/21478/>¹⁶⁴⁸ <http://secunia.com/advisories/21509/>¹⁶⁴⁹ <http://secunia.com/advisories/22262/>¹⁶⁵⁰ <http://secunia.com/advisories/22368/>¹⁶⁵¹ <http://secunia.com/advisories/22388/>¹⁶⁵² <http://secunia.com/advisories/22523/>¹⁶⁵³ <http://secunia.com/advisories/23028/>¹⁶⁵⁴ <http://secunia.com/advisories/23260/>¹⁶⁵⁵ <http://secunia.com/advisories/26329/>¹⁶⁵⁶ <http://secunia.com/advisories/29420/>¹⁶⁵⁷ <http://secunia.com/advisories/29849/>¹⁶⁵⁸ <http://secunia.com/advisories/30430/>¹⁶⁵⁹ <https://www.suse.com/support/security/advisories/>¹⁶⁶⁰ <http://xforce.iss.net/xforce/xfdb/28063>¹⁶⁶¹ http://httpd.apache.org/security/vulnerabilities_20.html¹⁶⁶² <http://www.securityfocus.com/bid/11360>¹⁶⁶³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0885>¹⁶⁶⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10384>¹⁶⁶⁵ <http://rhn.redhat.com/errata/RHSA-2004-562.html>¹⁶⁶⁶ <http://rhn.redhat.com/errata/RHSA-2004-600.html>¹⁶⁶⁷ <http://rhn.redhat.com/errata/RHSA-2005-816.html>¹⁶⁶⁸ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>¹⁶⁶⁹ <http://secunia.com/advisories/19072/>

			restriction-bypass(17671) ¹⁶⁷⁰ URL ¹⁶⁷¹		
7.	Apache httpd PCRE overflow (CVE-2005-2491) (http-apache2-pcre-bof)	172.23.202.126:80 172.23.202.225:80 Ranjivost tipa "Integer Overflow" je otkriven u PCRE (Perl compatible regular expression) biblioteci uključenoj u httpd. Lokalni korisnik koji ima mogućnost da kreira .htaccess fajlove mogao bi da kreira zlonamerno izrađen regularan izraz tako da dobije privilegije nad child procesima httpd servisa.	BID 14620 ¹⁶⁷² BID 15647 ¹⁶⁷³ CVE CVE-2005-2491 ¹⁶⁷⁴ DEBIAN DSA-800 ¹⁶⁷⁵ DEBIAN DSA-817 ¹⁶⁷⁶ DEBIAN DSA-819 ¹⁶⁷⁷ DEBIAN DSA-821 ¹⁶⁷⁸ OVAL OVAL11516 ¹⁶⁷⁹ OVAL OVAL1496 ¹⁶⁸⁰ OVAL OVAL1659 ¹⁶⁸¹ OVAL OVAL735 ¹⁶⁸² REDHAT RHSA-2005:358 ¹⁶⁸³ REDHAT RHSA-2005:761 ¹⁶⁸⁴ REDHAT RHSA-2006:0197 ¹⁶⁸⁵ SECUNIA 16502 ¹⁶⁸⁶ SECUNIA 16679 ¹⁶⁸⁷ SECUNIA 17252 ¹⁶⁸⁸ SECUNIA 17813 ¹⁶⁸⁹ SECUNIA 19072 ¹⁶⁹⁰ SECUNIA 19193 ¹⁶⁹¹ SECUNIA 19532 ¹⁶⁹² SECUNIA 21522 ¹⁶⁹³ SECUNIA 22691 ¹⁶⁹⁴ SECUNIA 22875 ¹⁶⁹⁵ SGI 20060401-01-U ¹⁶⁹⁶ SUSE SUSE-SA:2005:048 ¹⁶⁹⁷ SUSE SUSE-SA:2005:049 ¹⁶⁹⁸ SUSE SUSE-SA:2005:051 ¹⁶⁹⁹ SUSE SUSE-SA:2005:052 ¹⁷⁰⁰	Kritičan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.55.tar.gz

¹⁶⁷⁰ <http://xforce.iss.net/xforce/xfdb/17671>¹⁶⁷¹ http://httpd.apache.org/security/vulnerabilities_20.html¹⁶⁷² <http://www.securityfocus.com/bid/14620> pristupljeno 18.12.2011.¹⁶⁷³ <http://www.securityfocus.com/bid/15647> pristupljeno 18.12.2011.¹⁶⁷⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2491>¹⁶⁷⁵ <http://www.debian.org/security/DSA-/DSA-800> pristupljeno 18.12.2011.¹⁶⁷⁶ <http://www.debian.org/security/DSA-/DSA-817> pristupljeno 18.12.2011.¹⁶⁷⁷ <http://www.debian.org/security/DSA-/DSA-819> pristupljeno 18.12.2011.¹⁶⁷⁸ <http://www.debian.org/security/DSA-/DSA-821> pristupljeno 18.12.2011.¹⁶⁷⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11516>¹⁶⁸⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1496>¹⁶⁸¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1659>¹⁶⁸² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:735>¹⁶⁸³ <http://rhn.redhat.com/errata/RHSA-2005-358.html>¹⁶⁸⁴ <http://rhn.redhat.com/errata/RHSA-2005-761.html>¹⁶⁸⁵ <http://rhn.redhat.com/errata/RHSA-2006-0197.html>¹⁶⁸⁶ <http://secunia.com/advisories/16502/>¹⁶⁸⁷ <http://secunia.com/advisories/16679/>¹⁶⁸⁸ <http://secunia.com/advisories/17252/>¹⁶⁸⁹ <http://secunia.com/advisories/17813/>¹⁶⁹⁰ <http://secunia.com/advisories/19072/>¹⁶⁹¹ <http://secunia.com/advisories/19193/>¹⁶⁹² <http://secunia.com/advisories/19532/>¹⁶⁹³ <http://secunia.com/advisories/21522/>¹⁶⁹⁴ <http://secunia.com/advisories/22691/>¹⁶⁹⁵ <http://secunia.com/advisories/22875/>¹⁶⁹⁶ <ftp://patches.sgi.com/support/free/security/advisories/20060401-01-U> pristupljeno 18.12.2011¹⁶⁹⁷ <https://www.suse.com/support/security/advisories/>¹⁶⁹⁸ <https://www.suse.com/support/security/advisories/>¹⁶⁹⁹ <https://www.suse.com/support/security/advisories/>¹⁷⁰⁰ <https://www.suse.com/support/security/advisories/>

			URL1 ¹⁷⁰¹		
8.	OpenSSH X11 Cookie Local Authentication Bypass Vulnerability (openssh-x11-cookie-auth-bypass)	172.23.202.126:22 172.23.202.225:22 Pre verzije 4.7, OpenSSH nije adekvatno radio kada nepoverljivi kolačić (cookie) nije mogao biti kreiran. Umesto njega, koristi se poverljivi X11 kolačić. To omogućava napadačima da naruše ciljanu polisu i dobiju privilegije korisnika, što za posledicu servis tretira X klijenta kao poverljivog.	CVE CVE-2007-4752 ¹⁷⁰² BID 25628 ¹⁷⁰³ XF openssh-x11cookie-privilege-escalation(36637) ¹⁷⁰⁴	Kritičan	Uraditi download a zatim instalirati: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-4.7p1.tar.gz Verzija 4.7 of OpenSSH je puštena u promet 4. septembra 2007.
9.	OpenSSH GSSAPI Credentials Leak (ssh-openssh-gssapi-credentials-leak)	172.23.202.126:22 172.23.202.225:22 Odredene verzije OpenSSH greškom prosleđuju Kerberos poverljive podatke udaljenom host-u čak i kada se korisnička autentifikacija proverava drugim mehanizmima. Tako ako korisnik ima konfigurisanu GSSAPI autentifikaciju sa omogućenom opcijom GSSAPIDelegateCredentials, udaljeni napadač bi verovatno mogao da dođe do korisnikovih poverljivih podataka.	CVE CVE-2005-2798 ¹⁷⁰⁵ BID 14729 ¹⁷⁰⁶	Kritičan	Nadograditi na najnoviju verziju OpenSSH-a. Najnovija verzija OpenSSH-a je 5.2 (OpenBSD izvor) i 5.2p1 (prenosivi izvor).
10.	Apache httpd mod_deflate DoS (CVE-2009-1891) (apache-httpd-cve-2009-1891)	172.23.202.126:80 172.23.202.225:80 Ranjivost na DOS napad otkrivena je modulu mod_deflate. Ovaj modul nastavlja da kompresuje velike fajlove sve dok se kompresija ne završi, čak i kada je mrežna konekcija koja je zahtevala taj sadržaj prekinuta pre nego što je kompresija završena. To dovodi do toga da mod_deflate zauzima veliku količinu CPU-a ukoliko je mod_deflate bio omogućen za velike fajlove.	APPLE APPLE-SA-2009-11-09 ¹⁷⁰⁷ CVE CVE-2009-1891 ¹⁷⁰⁸ DEBIAN DSA-1834 ¹⁷⁰⁹ OSVDB 55782 ¹⁷¹⁰ OVAL OVAL8632 ¹⁷¹¹ OVAL OVAL9248 ¹⁷¹² REDHAT RHSA-2009:1148 ¹⁷¹³ REDHAT RHSA-2009:1156 ¹⁷¹⁴ SECUNIA 35721 ¹⁷¹⁵ SECUNIA 35781 ¹⁷¹⁶ SECUNIA 35793 ¹⁷¹⁷ SECUNIA 35865 ¹⁷¹⁸ SECUNIA 37152 ¹⁷¹⁹ SECUNIA 37221 ¹⁷²⁰ SUSE SA:2009:050 ¹⁷²¹ URL1 ¹⁷²²	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz

¹⁷⁰¹ http://httpd.apache.org/security/vulnerabilities_20.html¹⁷⁰² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-4752>¹⁷⁰³ <http://www.securityfocus.com/bid/25628>¹⁷⁰⁴ <http://xforce.iss.net/xforce/xfdb/36637>¹⁷⁰⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2798>¹⁷⁰⁶ <http://www.securityfocus.com/bid/14729>¹⁷⁰⁷ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>¹⁷⁰⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1891>¹⁷⁰⁹ <http://www.debian.org/security/DSA-/DSA-1834> pristupljeno 18.12.2011¹⁷¹⁰ <http://osvdb.org/55782>¹⁷¹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8632>¹⁷¹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9248>¹⁷¹³ <http://rhn.redhat.com/errata/RHSA-2009-1148.html>¹⁷¹⁴ <http://rhn.redhat.com/errata/RHSA-2009-1156.html>¹⁷¹⁵ <http://secunia.com/advisories/35721/>¹⁷¹⁶ <http://secunia.com/advisories/35781/>¹⁷¹⁷ <http://secunia.com/advisories/35793/>¹⁷¹⁸ <http://secunia.com/advisories/35865/>¹⁷¹⁹ <http://secunia.com/advisories/37152/>¹⁷²⁰ <http://secunia.com/advisories/37221/>¹⁷²¹ <https://www.suse.com/support/security/advisories/>¹⁷²² http://httpd.apache.org/security/vulnerabilities_20.html

11.	OpenSSH X11 Forwarding Information Disclosure Vulnerability (ssh-openssh-x11-fowarding-info-disclosure)	172.23.202.126:22 172.23.202.225:22 Određene verzije OpenSSH-a ne povezuju ispravno TCP portove na lokalnom IPv6 interfejsu ako se koriste zahtevani IPv4 portovi. Ovo bi loklanom napadaču moglo da omogući da preuzme prosleđenu X11 sesiju putem otvaranja TCP port-a 6010 (IPv4).	BID 28444 ¹⁷²³ CVE CVE-2008-1483 ¹⁷²⁴ SECUNIA 29522 ¹⁷²⁵ URL1 ¹⁷²⁶	Ozbiljan	Nadograditi na najnoviju verziju OpenSSH-a. Najnovija verzija OpenSSH-a je 5.2 (OpenBSD izvor) i 5.2p1 (portable izvor).
12.	Apache httpd expat DoS (CVE-2009-3560) (apache-httpd-2_0_x-cve-2009-3560)	172.23.202.126:80 172.23.202.225:80 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepoverljivi XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	BID 37203 ¹⁷²⁷ CVE CVE-2009-3560 ¹⁷²⁸ DEBIAN DSA-1953 ¹⁷²⁹ OVAL OVAL10613 ¹⁷³⁰ OVAL OVAL6883 ¹⁷³¹ SECUNIA 37537 ¹⁷³² SECUNIA 38231 ¹⁷³³ SECUNIA 38794 ¹⁷³⁴ SECUNIA 38832 ¹⁷³⁵ SECUNIA 38834 ¹⁷³⁶ SECUNIA 39478 ¹⁷³⁷ SECUNIA 41701 ¹⁷³⁸ SECUNIA 43300 ¹⁷³⁹ URL1 ¹⁷⁴⁰	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
13.	Apache httpd expat DoS (CVE-2009-3720) (apache-httpd-2_0_x-cve-2009-3720)	172.23.202.126:80 172.23.202.225:80 Skenirani servis je osjetljiv na ovu ranjivost SAMO ako je napadač u mogućnosti da dovede do toga da Apache parsira nepoverljivi XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer	CVE CVE-2009-3720 ¹⁷⁴¹ OVAL OVAL11019 ¹⁷⁴² OVAL OVAL7112 ¹⁷⁴³ REDHAT RHSA-2010:0002 ¹⁷⁴⁴ SECUNIA 37324 ¹⁷⁴⁵ SECUNIA 37537 ¹⁷⁴⁶ SECUNIA 37925 ¹⁷⁴⁷ SECUNIA 38050 ¹⁷⁴⁸ SECUNIA 38231 ¹⁷⁴⁹ SECUNIA 38794 ¹⁷⁵⁰	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz

¹⁷²³ <http://www.securityfocus.com/bid/28444>¹⁷²⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-1483>¹⁷²⁵ <http://secunia.com/advisories/29522/>¹⁷²⁶ <http://www.openssh.org/txt/release-5.0>¹⁷²⁷ <http://www.securityfocus.com/bid/37203>¹⁷²⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3560>¹⁷²⁹ <http://www.debian.org/security/DSA-/DSA-1953> pristupljeno dana 18.12.2011¹⁷³⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10613>¹⁷³¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6883>¹⁷³² <http://secunia.com/advisories/37537/>¹⁷³³ <http://secunia.com/advisories/38231/>¹⁷³⁴ <http://secunia.com/advisories/38794/>¹⁷³⁵ <http://secunia.com/advisories/38832/>¹⁷³⁶ <http://secunia.com/advisories/38834/>¹⁷³⁷ <http://secunia.com/advisories/39478/>¹⁷³⁸ <http://secunia.com/advisories/41701/>¹⁷³⁹ <http://secunia.com/advisories/43300/>¹⁷⁴⁰ http://httpd.apache.org/security/vulnerabilities_20.html¹⁷⁴¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3720>¹⁷⁴² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11019>¹⁷⁴³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7112>¹⁷⁴⁴ <http://rhn.redhat.com/errata/RHSA-2010-0002.html>¹⁷⁴⁵ <http://secunia.com/advisories/37324/>¹⁷⁴⁶ <http://secunia.com/advisories/37537/>¹⁷⁴⁷ <http://secunia.com/advisories/37925/>¹⁷⁴⁸ <http://secunia.com/advisories/38050/>¹⁷⁴⁹ <http://secunia.com/advisories/38231/>¹⁷⁵⁰ <http://secunia.com/advisories/38794/>

		over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	SECUNIA 38832 ¹⁷⁵¹ SECUNIA 38834 ¹⁷⁵² SECUNIA 39478 ¹⁷⁵³ SECUNIA 41701 ¹⁷⁵⁴ SECUNIA 43300 ¹⁷⁵⁵ URL1 ¹⁷⁵⁶		
14.	Apache httpd mod_dav DoS (CVE-2010-1452) (apache-httpd-2_0_x-cve-2010-1452)	172.23.202.126:80 172.23.202.225:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako web server izvršava jedan od sledećih modula: mod_dav. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u obradi zahteva od strane modula mod_dav. Zlonameran udaljeni napadač bi mogao da pošalje pažljivo izrađen zahtev i prouzrokuje da httpd child proces krahira. Ovakvo krahiranje bi se manifestovalo samo kao odbijanje servisa ako se koristi Worker MPM. Ovaj problem se dalje može ublažiti ako na mod_dav samo utiču zahtevi za koje postoji mogućnost autentifikovanja. Ovaj problem je prijavio Mark Drayton.	APPLE APPLE-SA-2011-03-21 ¹⁷⁵⁷ CVE CVE-2010-1452 ¹⁷⁵⁸ OVAL OVAL11683 ¹⁷⁵⁹ REDHAT RHSA-2010:0659 ¹⁷⁶⁰ SECUNIA 42367 ¹⁷⁶¹ URL1 ¹⁷⁶²	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
15.	Apache httpd apr_bridage_split_line DoS (CVE-2010-1623) (apache-httpd-2_0_x-cve-2010-1623)	172.23.202.126:80 172.23.202.225:80 Defekt je otkriven u funkciji apr_bridage_split_line() u sklopu APR-util library, upotrebljen da procesira ne-SSL zahteve. Udaljeni napadač bi mogao da šalje zahteve, pažljivo izrađujući tajming za pojedinačne bajtove, što bi polako zauzimalo memoriju i potencijalno dovelo do odbijanja servisa.	BID 43673 ¹⁷⁶³ CVE CVE-2010-1623 ¹⁷⁶⁴ REDHAT RHSA-2010:0950 ¹⁷⁶⁵ SECUNIA 41701 ¹⁷⁶⁶ SECUNIA 42015 ¹⁷⁶⁷ SECUNIA 42361 ¹⁷⁶⁸ SECUNIA 42367 ¹⁷⁶⁹ SECUNIA 42403 ¹⁷⁷⁰ SECUNIA 42537 ¹⁷⁷¹ SECUNIA 43211 ¹⁷⁷² SECUNIA 43285 ¹⁷⁷³ URL1 ¹⁷⁷⁴	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz

¹⁷⁵¹ <http://secunia.com/advisories/38832/>¹⁷⁵² <http://secunia.com/advisories/38834/>¹⁷⁵³ <http://secunia.com/advisories/39478/>¹⁷⁵⁴ <http://secunia.com/advisories/41701/>¹⁷⁵⁵ <http://secunia.com/advisories/43300/>¹⁷⁵⁶ http://httpd.apache.org/security/vulnerabilities_20.html¹⁷⁵⁷ <http://lists.apple.com/archives/security-announce/2011/Mar/msg00006.html>¹⁷⁵⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1452>¹⁷⁵⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11683>¹⁷⁶⁰ <http://rhn.redhat.com/errata/RHSA-2010-0659.html>¹⁷⁶¹ <http://secunia.com/advisories/42367/>¹⁷⁶² http://httpd.apache.org/security/vulnerabilities_20.html¹⁷⁶³ <http://www.securityfocus.com/bid/43673>¹⁷⁶⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1623>¹⁷⁶⁵ <http://rhn.redhat.com/errata/RHSA-2010-0950.html>¹⁷⁶⁶ <http://secunia.com/advisories/41701/>¹⁷⁶⁷ <http://secunia.com/advisories/42015/>¹⁷⁶⁸ <http://secunia.com/advisories/42361/>¹⁷⁶⁹ <http://secunia.com/advisories/42367/>¹⁷⁷⁰ <http://secunia.com/advisories/42403/>¹⁷⁷¹ <http://secunia.com/advisories/42537/>¹⁷⁷² <http://secunia.com/advisories/43211/>¹⁷⁷³ <http://secunia.com/advisories/43285/>¹⁷⁷⁴ http://httpd.apache.org/security/vulnerabilities_20.html

16.	Apache httpd mod_cache proxy DoS (CVE-2007-1863) (apache-httpd-2_0_x-mod_cache-proxy-dos-cve-2007-1863)	172.23.202.126:80 172.23.202.225:80 Propust je otkriven u modulu mod_cache. Na sajtovima na kojima je omogućeno keširanje, udaljeni napadač bi mogao da pošalje pažljivo izrađen zahtev koji bi doveo do toga da child proces Apache-a koji to obrađuje krahira. To može dovesti samo do odbijanja servisa ako se koristi threaded MPM.	BID 24649 ¹⁷⁷⁵ CERT TA08-150A ¹⁷⁷⁶ CVE CVE-2007-1863 ¹⁷⁷⁷ OVAL OVAL9824 ¹⁷⁷⁸ REDHAT RHSA-2007:0533 ¹⁷⁷⁹ REDHAT RHSA-2007:0534 ¹⁷⁸⁰ REDHAT RHSA-2007:0556 ¹⁷⁸¹ REDHAT RHSA-2007:0557 ¹⁷⁸² SECUNIA 25830 ¹⁷⁸³ SECUNIA 25873 ¹⁷⁸⁴ SECUNIA 25920 ¹⁷⁸⁵ SECUNIA 26273 ¹⁷⁸⁶ SECUNIA 26443 ¹⁷⁸⁷ SECUNIA 26508 ¹⁷⁸⁸ SECUNIA 26822 ¹⁷⁸⁹ SECUNIA 26842 ¹⁷⁹⁰ SECUNIA 26993 ¹⁷⁹¹ SECUNIA 27037 ¹⁷⁹² SECUNIA 27563 ¹⁷⁹³ SECUNIA 27732 ¹⁷⁹⁴ SECUNIA 28606 ¹⁷⁹⁵ SECUNIA 30430 ¹⁷⁹⁶ SUSE SA:2007:061 ¹⁷⁹⁷ URL1 ¹⁷⁹⁸	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.61.tar.gz
17.	Apache httpd mod_proxy_ftp DoS (CVE-2009-3094) (apache-httpd-2_0_x-mod_proxy_ftp-dos-cve-2009-3094)	172.23.202.126:80 172.23.202.225:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ftp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust NULL pointer dereference (pointer sa NULL vrednošću	CVE CVE-2009-3094 ¹⁷⁹⁹ DEBIAN DSA-1934 ¹⁸⁰⁰ OVAL OVAL10981 ¹⁸⁰¹ OVAL OVAL8087 ¹⁸⁰² SECUNIA 36549 ¹⁸⁰³ SECUNIA 37152 ¹⁸⁰⁴ SUSE SA:2009:050 ¹⁸⁰⁵ URL1 ¹⁸⁰⁶	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz

¹⁷⁷⁵ <http://www.securityfocus.com/bid/24649>¹⁷⁷⁶ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>¹⁷⁷⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-1863>¹⁷⁷⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9824>¹⁷⁷⁹ <http://rhn.redhat.com/errata/RHSA-2007-0533.html>¹⁷⁸⁰ <http://rhn.redhat.com/errata/RHSA-2007-0534.html>¹⁷⁸¹ <http://rhn.redhat.com/errata/RHSA-2007-0556.html>¹⁷⁸² <http://rhn.redhat.com/errata/RHSA-2007-0557.html>¹⁷⁸³ <http://secunia.com/advisories/25830/>¹⁷⁸⁴ <http://secunia.com/advisories/25873/>¹⁷⁸⁵ <http://secunia.com/advisories/25920/>¹⁷⁸⁶ <http://secunia.com/advisories/26273/>¹⁷⁸⁷ <http://secunia.com/advisories/26443/>¹⁷⁸⁸ <http://secunia.com/advisories/26508/>¹⁷⁸⁹ <http://secunia.com/advisories/26822/>¹⁷⁹⁰ <http://secunia.com/advisories/26842/>¹⁷⁹¹ <http://secunia.com/advisories/26993/>¹⁷⁹² <http://secunia.com/advisories/27037/>¹⁷⁹³ <http://secunia.com/advisories/27563/>¹⁷⁹⁴ <http://secunia.com/advisories/27732/>¹⁷⁹⁵ <http://secunia.com/advisories/28606/>¹⁷⁹⁶ <http://secunia.com/advisories/30430/>¹⁷⁹⁷ <https://www.suse.com/support/security/advisories/>¹⁷⁹⁸ http://httpd.apache.org/security/vulnerabilities_20.html¹⁷⁹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3094>¹⁸⁰⁰ <http://www.debian.org/security/DSA-/DSA-1934> pristupljeno dana 18.12.2011¹⁸⁰¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10981>¹⁸⁰² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8087>¹⁸⁰³ <http://secunia.com/advisories/36549/>¹⁸⁰⁴ <http://secunia.com/advisories/37152/>¹⁸⁰⁵ <https://www.suse.com/support/security/advisories/>

		upotrebljen kao da ukazuje na validnu memorijsku oblast) otkriven je u modulu mod_proxy_ftp. Zlonamerni FTP server, kojem su zahtevi proksirani, mogao bi da iskoristi ovaj propust u smislu obaranja http child procesa uz pomoć namerno izmenjenog odgovora EPSV ili PASV komandi, što bi dovelo do delimičnog odbijanja servisa.			
18.	Apache httpd mod_proxy_http DoS (CVE-2008-2364) (apache-httpd-2_0_x-mod_proxy_http-dos-cve-2008-2364)	172.23.202.126:80 172.23.202.225:80 Otkriven je propust prilikom obrade prekomernih privremenih odgovora sa glavnog servera kada se koristi mod_proxy_http. Udaljeni napadač bi mogao da izazove odbijanje servisa ili preopterećenje memorije.	BID 29653 ¹⁸⁰⁷ BID 31681 ¹⁸⁰⁸ CVE CVE-2008-2364 ¹⁸⁰⁹ OVAL OVAL11713 ¹⁸¹⁰ OVAL OVAL6084 ¹⁸¹¹ OVAL OVAL9577 ¹⁸¹² REDHAT RHSA-2008:0966 ¹⁸¹³ REDHAT RHSA-2008:0967 ¹⁸¹⁴ SECUNIA 30621 ¹⁸¹⁵ SECUNIA 31026 ¹⁸¹⁶ SECUNIA 31404 ¹⁸¹⁷ SECUNIA 31416 ¹⁸¹⁸ SECUNIA 31651 ¹⁸¹⁹ SECUNIA 31904 ¹⁸²⁰ SECUNIA 32222 ¹⁸²¹ SECUNIA 32685 ¹⁸²² SECUNIA 32838 ¹⁸²³ SECUNIA 33156 ¹⁸²⁴ SECUNIA 33797 ¹⁸²⁵ SECUNIA 34219 ¹⁸²⁶ SECUNIA 34259 ¹⁸²⁷ SECUNIA 34418 ¹⁸²⁸ XF apache-modproxy-module-dos(42987) ¹⁸²⁹ URL1 ¹⁸³⁰	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
19.	Apache httpd mod_ssl access control DoS (CVE-2005-3357) (apache-httpd-2_0_x-	172.23.202.126:80 172.23.202.225:80 Propust NULL pointer dereference	BID 16152 ¹⁸³¹ CERT TA08-150A ¹⁸³² CVE CVE-2005-3357 ¹⁸³³ OVAL OVAL11467 ¹⁸³⁴	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dis

¹⁸⁰⁶ http://httpd.apache.org/security/vulnerabilities_20.html¹⁸⁰⁷ <http://www.securityfocus.com/bid/29653>¹⁸⁰⁸ <http://www.securityfocus.com/bid/31681>¹⁸⁰⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-2364>¹⁸¹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11713>¹⁸¹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6084>¹⁸¹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9577>¹⁸¹³ <http://rhn.redhat.com/errata/RHSA-2008-0966.html>¹⁸¹⁴ <http://rhn.redhat.com/errata/RHSA-2008-0967.html>¹⁸¹⁵ <http://secunia.com/advisories/30621/>¹⁸¹⁶ <http://secunia.com/advisories/31026/>¹⁸¹⁷ <http://secunia.com/advisories/31404/>¹⁸¹⁸ <http://secunia.com/advisories/31416/>¹⁸¹⁹ <http://secunia.com/advisories/31651/>¹⁸²⁰ <http://secunia.com/advisories/31904/>¹⁸²¹ <http://secunia.com/advisories/32222/>¹⁸²² <http://secunia.com/advisories/32685/>¹⁸²³ <http://secunia.com/advisories/32838/>¹⁸²⁴ <http://secunia.com/advisories/33156/>¹⁸²⁵ <http://secunia.com/advisories/33797/>¹⁸²⁶ <http://secunia.com/advisories/34219/>¹⁸²⁷ <http://secunia.com/advisories/34259/>¹⁸²⁸ <http://secunia.com/advisories/34418/>¹⁸²⁹ <http://xforce.iss.net/xforce/xfdb/42987>¹⁸³⁰ http://httpd.apache.org/security/vulnerabilities_20.html¹⁸³¹ <http://www.securityfocus.com/bid/16152>¹⁸³² <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>¹⁸³³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-3357>

	mod_ssl-access-controlldos-cve-2005-3357)	(pointer sa NULL vrednošću upotrebljen kao da ukazuje na validnu memorijsku oblast) otkriven je u modulu mod_ssl. To je slučaj kada je server na kojem je virtuelan host SSL konfigurisan sa kontrolom pristupa i uobičajenim dokumentom za prikaz greške (tip 400). Udaljeni napadač bi mogao da pošalje posebno kreiran zahtev da pokrene ovaj problem koji bi doveo do upada. Ovakav upad bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM.	REDHAT ¹⁸³⁵ RHSA-2006:0159 ¹⁸³⁵ SECUNIA ¹⁸³⁶ 18307 ¹⁸³⁶ SECUNIA ¹⁸³⁷ 18333 ¹⁸³⁷ SECUNIA ¹⁸³⁸ 18339 ¹⁸³⁸ SECUNIA ¹⁸³⁹ 18340 ¹⁸³⁹ SECUNIA ¹⁸⁴⁰ 18429 ¹⁸⁴⁰ SECUNIA ¹⁸⁴¹ 18517 ¹⁸⁴¹ SECUNIA ¹⁸⁴² 18585 ¹⁸⁴² SECUNIA ¹⁸⁴³ 18743 ¹⁸⁴³ SECUNIA ¹⁸⁴⁴ 19012 ¹⁸⁴⁴ SECUNIA ¹⁸⁴⁵ 21848 ¹⁸⁴⁵ SECUNIA ¹⁸⁴⁶ 22233 ¹⁸⁴⁶ SECUNIA ¹⁸⁴⁷ 22368 ¹⁸⁴⁷ SECUNIA ¹⁸⁴⁸ 22523 ¹⁸⁴⁸ SECUNIA ¹⁸⁴⁹ 22669 ¹⁸⁴⁹ SECUNIA ¹⁸⁵⁰ 22992 ¹⁸⁵⁰ SECUNIA ¹⁸⁵¹ 23260 ¹⁸⁵¹ SECUNIA ¹⁸⁵² 29849 ¹⁸⁵² SECUNIA ¹⁸⁵³ 30430 ¹⁸⁵³ SGI ¹⁸⁵⁴ 20060101-01-U ¹⁸⁵⁴ SUSE ¹⁸⁵⁵ SA:2006:051 ¹⁸⁵⁵ SUSE ¹⁸⁵⁶ SA:2006:051 ¹⁸⁵⁶ URL1 ¹⁸⁵⁷		t/httpd/httpd-2.0.58.tar.gz
20.	Apache httpd Signals to arbitrary processes (CVE-2007-3304) (apache-httpd-2_0_x-signals-to-arbitraryprocesses-cve-2007-3304)	172.23.202.126:80 172.23.202.225:80 Pre nego što mu je poslao signale, Apache HTTP server nije overio da li proces potiče od Apache čajlda. Lokalni napadač koji ima mogućnost da pokreće skripta na HTTP serveru, mogao bi da manipuliše semaforom za signale i da prouzrokuje okončanje proizvoljnog procesa, što bi moglo da dovede do odbijanja servisa.	BID ¹⁸⁵⁸ 24215 ¹⁸⁵⁸ CVE ¹⁸⁵⁹ CVE-2007-3304 ¹⁸⁵⁹ OVAL ¹⁸⁶⁰ OVAL11589 ¹⁸⁶⁰ REDHAT ¹⁸⁶¹ RHSA-2007:0532 ¹⁸⁶¹ REDHAT ¹⁸⁶² RHSA-2007:0556 ¹⁸⁶² REDHAT ¹⁸⁶³ RHSA-2007:0557 ¹⁸⁶³ REDHAT ¹⁸⁶⁴ RHSA-2007:0662 ¹⁸⁶⁴ REDHAT ¹⁸⁶⁵ RHSA-2008:0261 ¹⁸⁶⁵	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.61.tar.gz

¹⁸³⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11467>¹⁸³⁵ <http://rhn.redhat.com/errata/RHSA-2006-0159.html>¹⁸³⁶ <http://secunia.com/advisories/18307/>¹⁸³⁷ <http://secunia.com/advisories/18333/>¹⁸³⁸ <http://secunia.com/advisories/18339/>¹⁸³⁹ <http://secunia.com/advisories/18340/>¹⁸⁴⁰ <http://secunia.com/advisories/18429/>¹⁸⁴¹ <http://secunia.com/advisories/18517/>¹⁸⁴² <http://secunia.com/advisories/18585/>¹⁸⁴³ <http://secunia.com/advisories/18743/>¹⁸⁴⁴ <http://secunia.com/advisories/19012/>¹⁸⁴⁵ <http://secunia.com/advisories/21848/>¹⁸⁴⁶ <http://secunia.com/advisories/22233/>¹⁸⁴⁷ <http://secunia.com/advisories/22368/>¹⁸⁴⁸ <http://secunia.com/advisories/22523/>¹⁸⁴⁹ <http://secunia.com/advisories/22669/>¹⁸⁵⁰ <http://secunia.com/advisories/22992/>¹⁸⁵¹ <http://secunia.com/advisories/23260/>¹⁸⁵² <http://secunia.com/advisories/29849/>¹⁸⁵³ <http://secunia.com/advisories/30430/>¹⁸⁵⁴ <ftp://patches.sgi.com/support/free/security/advisories/20060101-01-U> pristupljeno 18.12.2011¹⁸⁵⁵ <https://www.suse.com/support/security/advisories/>¹⁸⁵⁶ <https://www.suse.com/support/security/advisories/>¹⁸⁵⁷ http://httpd.apache.org/security/vulnerabilities_20.html¹⁸⁵⁸ <http://www.securityfocus.com/bid/24215>¹⁸⁵⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3304>¹⁸⁶⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11589>¹⁸⁶¹ <http://rhn.redhat.com/errata/RHSA-2007-0532.html>¹⁸⁶² <http://rhn.redhat.com/errata/RHSA-2007-0556.html>¹⁸⁶³ <http://rhn.redhat.com/errata/RHSA-2007-0557.html>¹⁸⁶⁴ <http://rhn.redhat.com/errata/RHSA-2007-0662.html>

			SECUNIA 25827¹⁸⁶⁶ SECUNIA 25830¹⁸⁶⁷ SECUNIA 25920¹⁸⁶⁸ SECUNIA 26211¹⁸⁶⁹ SECUNIA 26273¹⁸⁷⁰ SECUNIA 26443¹⁸⁷¹ SECUNIA 26508¹⁸⁷² SECUNIA 26611¹⁸⁷³ SECUNIA 26759¹⁸⁷⁴ SECUNIA 26790¹⁸⁷⁵ SECUNIA 26822¹⁸⁷⁶ SECUNIA 26842¹⁸⁷⁷ SECUNIA 26993¹⁸⁷⁸ SECUNIA 27121¹⁸⁷⁹ SECUNIA 27209¹⁸⁸⁰ SECUNIA 27563¹⁸⁸¹ SECUNIA 27732¹⁸⁸² SECUNIA 28212¹⁸⁸³ SECUNIA 28224¹⁸⁸⁴ SECUNIA 28606¹⁸⁸⁵ SGI 20070701-01-P¹⁸⁸⁶ SUSE SA:2007:061¹⁸⁸⁷ XF apache-child-process-dos(35095)¹⁸⁸⁸ URL1¹⁸⁸⁹		
21.	FTP access with ftp account (ftp-generic-0001)	172.23.202.126:21 172.23.202.225:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisnikovim ID-jem (identifikacijom) „ftp“ i šifrom „ftp“. Dosadašnja praksa je pokazala da je najbolje ukloniti difoltni naloge, ukoliko je to moguće. Za naloge koje sistem zahteva treba izmeniti difoltnu šifru.	CVE CVE-1999-0497¹⁸⁹⁰	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko on nije kritičan za dalje funkcionisanje sistema. U suprotnom, treba promeniti šifru u nedifoltnu vrednost.
22.	FTP access with anonymous account (ftp-generic-0002)	172.23.202.126:21 172.23.202.225:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisnikovim ID-jem	CVE CVE-1999-0497¹⁸⁹¹	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko on nije kritičan za dalje funkcionisanje sistema. U suprotnom, treba promeniti

¹⁸⁶⁵ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>¹⁸⁶⁶ <http://secunia.com/advisories/25827/>¹⁸⁶⁷ <http://secunia.com/advisories/25830/>¹⁸⁶⁸ <http://secunia.com/advisories/25920/>¹⁸⁶⁹ <http://secunia.com/advisories/26211/>¹⁸⁷⁰ <http://secunia.com/advisories/26273/>¹⁸⁷¹ <http://secunia.com/advisories/26443/>¹⁸⁷² <http://secunia.com/advisories/26508/>¹⁸⁷³ <http://secunia.com/advisories/26611/>¹⁸⁷⁴ <http://secunia.com/advisories/26759/>¹⁸⁷⁵ <http://secunia.com/advisories/26790/>¹⁸⁷⁶ <http://secunia.com/advisories/26822/>¹⁸⁷⁷ <http://secunia.com/advisories/26842/>¹⁸⁷⁸ <http://secunia.com/advisories/26993/>¹⁸⁷⁹ <http://secunia.com/advisories/27121/>¹⁸⁸⁰ <http://secunia.com/advisories/27209/>¹⁸⁸¹ <http://secunia.com/advisories/27563/>¹⁸⁸² <http://secunia.com/advisories/27732/>¹⁸⁸³ <http://secunia.com/advisories/28212/>¹⁸⁸⁴ <http://secunia.com/advisories/28224/>¹⁸⁸⁵ <http://secunia.com/advisories/28606/>¹⁸⁸⁶ <ftp://patches.sgi.com/support/free/security/advisories/20070701-01-P> pristupljeno 18.12.2011¹⁸⁸⁷ <https://www.suse.com/support/security/advisories/>¹⁸⁸⁸ <http://xforce.iss.net/xforce/xfdb/35095>¹⁸⁸⁹ http://httpd.apache.org/security/vulnerabilities_20.html¹⁸⁹⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>¹⁸⁹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>

		(identifikacijom) „anonymous“ i šifrom „ftp@“. Dosadašnja praksa je pokazala da je najbolje ukloniti difoltne naloge, ukoliko je to moguće. Za naloge koje sistem zahteva treba izmeniti difoltnu šifru.			šifru u nedifoltnu vrednost.
23.	FTP server does not support AUTH command (ftp-generic-0007)	172.23.202.126:21 172.23.202.225:21 FTP klijenti po difoltu šalju FTP server-u poverljive podatke (korisnički ID i šifru) u vidu čitkog teksta. Ova okolnost dozvoljava zlonamernim korisnicima da presreću poverljive podatke ukoliko prisluškuju vezu. Noviji FTP serveri podržavaju AUTH komandu, koja omogućava dodatne opcije autentifikacije, kao što su TLS, Kerberos, GSSAPI itd. Ona se može koristiti za sprečavanje prisluškivanja na FTP vezama.		Ozbiljan	Ažurirati/preći na FTP server koji podržava AUTH komandu.
24.	Apache httpd mod_proxy crash (CVE-2007-3847) (http://apache-mod_proxy-date-parsing-dos)	172.23.202.126:80 172.23.202.225:80 Propust je otkriven u Apache-ovom HTTP Server modulu mod_proxy. Na sajtovima na kojima je konfigurisan "reverse proxy", udaljeni napadač bi mogao da pošalje pažljivo izrađen zahtev koji bi mogao da prouzrokuje pad child procesa Apache-a koji taj zahtev obrađuje. Na sajtovima na kojima je konfigurisan "forward proxy", napadač bi mogao da prouzrokuje sličan pad ako bi korisnik bio naveden da poseti zlonamerni sajt koji koristi taj proksi. Ovo bi moglo da dovede do odbijanja servisa ako se koristi threaded MPM.	BID 25489 ¹⁸⁹² CERT TA08-150A ¹⁸⁹³ CVE CVE-2007-3847 ¹⁸⁹⁴ OVAL OVAL10525 ¹⁸⁹⁵ REDHAT RHSA-2007:0746 ¹⁸⁹⁶ REDHAT RHSA-2007:0747 ¹⁸⁹⁷ REDHAT RHSA-2007:0911 ¹⁸⁹⁸ REDHAT RHSA-2008:0005 ¹⁸⁹⁹ SECUNIA 26636 ¹⁹⁰⁰ SECUNIA 26722 ¹⁹⁰¹ SECUNIA 26790 ¹⁹⁰² SECUNIA 26842 ¹⁹⁰³ SECUNIA 26952 ¹⁹⁰⁴ SECUNIA 26993 ¹⁹⁰⁵ SECUNIA 27209 ¹⁹⁰⁶ SECUNIA 27563 ¹⁹⁰⁷ SECUNIA 27593 ¹⁹⁰⁸ SECUNIA 27732 ¹⁹⁰⁹ SECUNIA 27882 ¹⁹¹⁰ SECUNIA 27971 ¹⁹¹¹ SECUNIA 28467 ¹⁹¹²	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.61.tar.gz

¹⁸⁹² <http://www.securityfocus.com/bid/25489> pristupljeno 18.12.2011¹⁸⁹³ <http://www.cert.org/advisories/TA08-150A.html> pristupljeno 18.12.2011¹⁸⁹⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3847>¹⁸⁹⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10525>¹⁸⁹⁶ <http://rhn.redhat.com/errata/RHSA-2007-0746.html>¹⁸⁹⁷ <http://rhn.redhat.com/errata/RHSA-2007-0747.html>¹⁸⁹⁸ <http://rhn.redhat.com/errata/RHSA-2007-0911.html>¹⁸⁹⁹ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>¹⁹⁰⁰ <http://secunia.com/advisories/26636/>¹⁹⁰¹ <http://secunia.com/advisories/26722/>¹⁹⁰² <http://secunia.com/advisories/26790/>¹⁹⁰³ <http://secunia.com/advisories/26842/>¹⁹⁰⁴ <http://secunia.com/advisories/26952/>¹⁹⁰⁵ <http://secunia.com/advisories/26993/>¹⁹⁰⁶ <http://secunia.com/advisories/27209/>¹⁹⁰⁷ <http://secunia.com/advisories/27563/>¹⁹⁰⁸ <http://secunia.com/advisories/27593/>¹⁹⁰⁹ <http://secunia.com/advisories/27732/>¹⁹¹⁰ <http://secunia.com/advisories/27882/>¹⁹¹¹ <http://secunia.com/advisories/27971/>

			SECUNIA 28606 ¹⁹¹³ SECUNIA 28749 ¹⁹¹⁴ SECUNIA 28922 ¹⁹¹⁵ SECUNIA 29420 ¹⁹¹⁶ SECUNIA 30430 ¹⁹¹⁷ SUSE SA:2007:061 ¹⁹¹⁸ URL1 ¹⁹¹⁹		
25.	Apache httpd Worker MPM memory leak (CVE-2005-2970) (http://apache-worker-mpm-memleak)	172.23.202.126:80 172.23.202.225:80 Gubitak memorije u Worker MPM-u bi udaljenim napadačima omogućio da prouzrokuju odbijanje servisa (zauzimanje memorije) preko prekinutih veza, što onemogućava da se memorija iz transakcionih pool-ova ponovo koristi za druge veze.	BID 15762 ¹⁹²⁰ CVE CVE-2005-2970 ¹⁹²¹ OVAL OVAL10043 ¹⁹²² REDHAT RHSA-2006:0159 ¹⁹²³ SECUNIA 16559 ¹⁹²⁴ SECUNIA 17923 ¹⁹²⁵ SECUNIA 18161 ¹⁹²⁶ SECUNIA 18333 ¹⁹²⁷ SECUNIA 18585 ¹⁹²⁸ URL1 ¹⁹²⁹	Ozbiljan	Apache >= 2.0 and < 2.1 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.55.tar.gz
26.	Apache httpd Memory consumption DoS (CVE-2004-0942) (http://apache2-long-header-dos)	172.23.202.126:80 172.23.202.225:80 Problem je otkriven tamo gde ograničenje dužine rubrike nije bilo primenjeno za određene zlonamerne zahteve. To bi udaljenom napadaču, koji je u mogućnosti da šalje velike količine podataka serveru, omogućilo child procesi Apache-a zauzmu srazmerno velike količine memorije, što bi dovelo do odbijanja servisa.	CVE CVE-2004-0942 ¹⁹³⁰ MANDRAKE MDKSA-2004:135 ¹⁹³¹ OVAL OVAL10962 ¹⁹³² REDHAT RHSA-2004:562 ¹⁹³³ SECUNIA 19072 ¹⁹³⁴ XF apache-http-get-dos(17930) ¹⁹³⁵ URL1 ¹⁹³⁶	Ozbiljan	Apache >= 2.0 and < 2.1 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.53.tar.gz
27.	Apache httpd ByteRange filter DoS (CVE-2005-2728) (http://apache2-reverse-proxy-memory-leak)	172.23.202.126:80 172.23.202.225:80 Propust u Apache-ovom filteru opsega bajtova može da dovede do toga da se određeni odgovori baferuju u memoriju. Ako server poseduje dinamički izvor, kao što je CGI	BID 14660 ¹⁹³⁷ CVE CVE-2005-2728 ¹⁹³⁸ DEBIAN DSA-805 ¹⁹³⁹ OVAL OVAL10017 ¹⁹⁴⁰ OVAL OVAL1246 ¹⁹⁴¹ OVAL OVAL1727 ¹⁹⁴² OVAL OVAL760 ¹⁹⁴³	Ozbiljan	Apache >= 2.0 and < 2.1 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.55.tar.gz

¹⁹¹² <http://secunia.com/advisories/28467/>¹⁹¹³ <http://secunia.com/advisories/28606/>¹⁹¹⁴ <http://secunia.com/advisories/28749/>¹⁹¹⁵ <http://secunia.com/advisories/28922/>¹⁹¹⁶ <http://secunia.com/advisories/29420/>¹⁹¹⁷ <http://secunia.com/advisories/30430/>¹⁹¹⁸ <https://www.suse.com/support/security/advisories/>¹⁹¹⁹ http://httpd.apache.org/security/vulnerabilities_20.html¹⁹²⁰ <http://www.securityfocus.com/bid/15762>¹⁹²¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2970>¹⁹²² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10043>¹⁹²³ <http://rhn.redhat.com/errata/RHSA-2006-0159.html>¹⁹²⁴ <http://secunia.com/advisories/16559/>¹⁹²⁵ <http://secunia.com/advisories/17923/>¹⁹²⁶ <http://secunia.com/advisories/18161/>¹⁹²⁷ <http://secunia.com/advisories/18333/>¹⁹²⁸ <http://secunia.com/advisories/18585/>¹⁹²⁹ http://httpd.apache.org/security/vulnerabilities_20.html¹⁹³⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0942>¹⁹³¹ <http://www.mandriva.com/en/support/security/advisories/advisory/MDKSA-2004:135/?name=MDKSA-2004:135>¹⁹³² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10962>¹⁹³³ <http://rhn.redhat.com/errata/RHSA-2004-562.html>¹⁹³⁴ <http://secunia.com/advisories/19072/>¹⁹³⁵ <http://xforce.iss.net/xforce/xfdb/17930>¹⁹³⁶ http://httpd.apache.org/security/vulnerabilities_20.html¹⁹³⁷ <http://www.securityfocus.com/bid/14660>¹⁹³⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2728>¹⁹³⁹ <https://security-tracker.debian.org/tracker/DSA-805-1>¹⁹⁴⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10017>¹⁹⁴¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1246>¹⁹⁴² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1727>¹⁹⁴³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:760>

		skripte ili PHP skripte, koje obrađuju velike količine podataka, napadač bi mogao da pošalje pažljivo izrađen zahtev sa ciljem iskorišćavanja resursa, što može da dovede do odbijanja servisa.	REDHAT ¹⁹⁴⁴ RHSA-2005:608 SECUNIA ¹⁹⁴⁵ 16559 SECUNIA ¹⁹⁴⁶ 16705 SECUNIA ¹⁹⁴⁷ 16714 SECUNIA ¹⁹⁴⁸ 16743 SECUNIA ¹⁹⁴⁹ 16746 SECUNIA ¹⁹⁵⁰ 16753 SECUNIA ¹⁹⁵¹ 16754 SECUNIA ¹⁹⁵² 16769 SECUNIA ¹⁹⁵³ 16789 SECUNIA ¹⁹⁵⁴ 16956 SECUNIA ¹⁹⁵⁵ 17036 SECUNIA ¹⁹⁵⁶ 17288 SECUNIA ¹⁹⁵⁷ 17600 SECUNIA ¹⁹⁵⁸ 17831 SECUNIA ¹⁹⁵⁹ 17923 SECUNIA ¹⁹⁶⁰ 18161 SECUNIA ¹⁹⁶¹ 18333 SECUNIA ¹⁹⁶² 18517 SECUNIA ¹⁹⁶³ 19072 SGI ¹⁹⁶⁴ 20060101-01-U SUSE ¹⁹⁶⁵ SA:2005:051 SUSE ¹⁹⁶⁶ SA:2005:052 XF ¹⁹⁶⁷ apache-byterange-dos(22006) URL1		
28.	Apache httpd Malicious CRL off-by-one (CVE-2005-1268) (http://apache2-ssl-crl-verify-bof)	172.23.202.126:80 172.23.202.225:80 Ranjivost tipa "off-by-one stack overflow" je otkrivena u mod_ssl CRL pri overi povratnog poziva. Da bi sprečio ovaj problem, Apache server treba da bude konfigurisan tako da koristi listu opozvanih	BID ¹⁹⁶⁸ 14366 CVE ¹⁹⁶⁹ CVE-2005-1268 DEBIAN ¹⁹⁷⁰ DSA-805 MANDRAKE ¹⁹⁷¹ MDKSA-2005:129 OVAL ¹⁹⁷² OVAL1346 OVAL ¹⁹⁷³ OVAL1714 OVAL ¹⁹⁷⁴ OVAL1747 OVAL ¹⁹⁷⁵ OVAL9589	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.55.tar.gz

¹⁹⁴⁴ <http://rhn.redhat.com/errata/RHSA-2005-608.html>¹⁹⁴⁵ <http://secunia.com/advisories/16559/>¹⁹⁴⁶ <http://secunia.com/advisories/16705/>¹⁹⁴⁷ <http://secunia.com/advisories/16714/>¹⁹⁴⁸ <http://secunia.com/advisories/16743/>¹⁹⁴⁹ <http://secunia.com/advisories/16746/>¹⁹⁵⁰ <http://secunia.com/advisories/16753/>¹⁹⁵¹ <http://secunia.com/advisories/16754/>¹⁹⁵² <http://secunia.com/advisories/16769/>¹⁹⁵³ <http://secunia.com/advisories/16789/>¹⁹⁵⁴ <http://secunia.com/advisories/16956/>¹⁹⁵⁵ <http://secunia.com/advisories/17036/>¹⁹⁵⁶ <http://secunia.com/advisories/17288/>¹⁹⁵⁷ <http://secunia.com/advisories/17600/>¹⁹⁵⁸ <http://secunia.com/advisories/17831/>¹⁹⁵⁹ <http://secunia.com/advisories/17923/>¹⁹⁶⁰ <http://secunia.com/advisories/18161/>¹⁹⁶¹ <http://secunia.com/advisories/18333/>¹⁹⁶² <http://secunia.com/advisories/18517/>¹⁹⁶³ <http://secunia.com/advisories/19072/>¹⁹⁶⁴ <ftp://patches.sgi.com/support/free/security/advisories/20060101-01-U> pristupljeno 18.12.2011¹⁹⁶⁵ <https://www.suse.com/support/security/advisories/>¹⁹⁶⁶ <https://www.suse.com/support/security/advisories/>¹⁹⁶⁷ http://httpd.apache.org/security/vulnerabilities_20.html¹⁹⁶⁸ <http://www.securityfocus.com/bid/14366>¹⁹⁶⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-1268>¹⁹⁷⁰ <https://security-tracker.debian.org/tracker/DSA-805-1>¹⁹⁷¹ <http://www.mandriva.com/en/support/security/advisories/advisory/MDKSA-2005:129/?name=MDKSA-2005:129>¹⁹⁷² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1346>¹⁹⁷³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1714>¹⁹⁷⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1747>¹⁹⁷⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9589>

		sertifikata (CRL).	REDHAT ¹⁹⁷⁶ RHSA-2005:582 SECUNIA ¹⁹⁷⁷ 19072 SECUNIA ¹⁹⁷⁸ 19185 SUSE ¹⁹⁷⁹ SUSE-SA:2005:046 URL ¹⁹⁸⁰ 1		
29.	Browsable web directory (http-generic-browsable-dir)	172.23.202.126:8080 172.23.202.225:8080 Otkriven je direktorijum na web serveru koji može biti pretraživan, što znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice - spajdering (prateći hiperlinkove), ili -kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute-force napadom na liste uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skriven“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice. Primer: http://172.23.202.126:8080/webdav/ 1: <html> 2: <head> 3: <title>Directory Listing For </title>		Ozbiljan	Za Apache: onemogućiti pretraživanje direktorijuma mreže za sve direktorijume i poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim ako je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i brisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume. Za Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote: Onemogućiti pretraživanje direktorijuma mreže za sve direktorijume i poddirektorijume. Uključiti Tomcat-ov web.xml file. U odeljku „default“, promeniti parametar „listings“ iz „true“ u „false“. Restartovati server. Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume.

¹⁹⁷⁶ <http://rhn.redhat.com/errata/RHSA-2005-582.html>¹⁹⁷⁷ <http://secunia.com/advisories/19072/>¹⁹⁷⁸ <http://secunia.com/advisories/19185/>¹⁹⁷⁹ <https://www.suse.com/support/security/advisories/>¹⁹⁸⁰ http://httpd.apache.org/security/vulnerabilities_20.html

30.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	172.23.202.126:3306 172.23.202.225:3306: Kada se kod TCP-a paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183 ¹⁹⁸¹ CERT-VN: 415294 ¹⁹⁸² CVE CVE-2004-0230 ¹⁹⁸³ MS: MS05-019 ¹⁹⁸⁴ MS: MS06-064 ¹⁹⁸⁵ NETBSD: NetBSD-SA2004-006 ¹⁹⁸⁶ OVAL: OVAL2689 ¹⁹⁸⁷ OVAL: OVAL270 ¹⁹⁸⁸ OVAL OVAL3508 ¹⁹⁸⁹ OVAL OVAL4791 ¹⁹⁹⁰ OVAL OVAL5711 ¹⁹⁹¹ SECUNIA: 11440 ¹⁹⁹² SECUNIA 11458 ¹⁹⁹³ SECUNIA: 22341 ¹⁹⁹⁴ SGI 20040403-01-A ¹⁹⁹⁵ XF tcp-rst-dos(15886) ¹⁹⁹⁶ URL1 ¹⁹⁹⁷ URL2 ¹⁹⁹⁸	Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC 2385. ¹⁹⁹⁹ Cilj je da se smanji opasnost od određenih napada na BGP, kao što su TCP reseti.
31.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podesi na jedinstvenu vrednost i da se koristi u rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da fingerprint-uje operativni sistem.	BID 4314 ²⁰⁰⁰ CVE CVE-2002-0510 ²⁰⁰¹ XF linux-udp-fingerprint(8588) ²⁰⁰²	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili čak ranjivost koju treba popravljati, tako da ne postoje rešenja koja se mogu kupiti. Jedino se može postaviti fajervol ili neki drugi oblik zaštite sa kojim se vrši filtriranje između napadnutog sistema i zlonamernog napada kojem je cilj randomizovanje IP ID-jeva.
32.	Apache httpd mod_imap XSS (CVE-2007-5000) (apache-httpd-2_0_x-mod_imagemap-xss-cve-2007-5000)	172.23.202.126:80 172.23.202.225:80 Propust je otkriven u modulu mod_imap. Na sajtovim na kojima je omogućen mod_imap i fajl imagemap je javno dostupan, moguće je izvesti napad tipa "crossite scripting attack".	BID 26838 ²⁰⁰³ CERT TA08-150A ²⁰⁰⁴ CVE CVE-2007-5000 ²⁰⁰⁵ OSVDB 39134 ²⁰⁰⁶ OVAL OVAL9539 ²⁰⁰⁷ REDHAT RHSA-2008:0004 ²⁰⁰⁸ REDHAT RHSA-2008:0005 ²⁰⁰⁹	Ozbiljan	Apache >= 2.0 and < 2.1 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.63.tar.gz

¹⁹⁸¹ <http://www.securityfocus.com/bid/10183>¹⁹⁸² <http://www.kb.cert.org/vuls/id/415294>¹⁹⁸³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>¹⁹⁸⁴ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>¹⁹⁸⁵ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>¹⁹⁸⁶ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>¹⁹⁸⁷ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:2689>¹⁹⁸⁸ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:270>¹⁹⁸⁹ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:3508>¹⁹⁹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:4791>¹⁹⁹¹ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:5711>¹⁹⁹² <http://secunia.com/advisories/11440/>¹⁹⁹³ <http://secunia.com/advisories/11458/>¹⁹⁹⁴ <http://secunia.com/advisories/22341/>¹⁹⁹⁵ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>¹⁹⁹⁶ <http://xforce.iss.net/xforce/xfdb/15886>¹⁹⁹⁷ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>¹⁹⁹⁸ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>¹⁹⁹⁹ <http://www.ietf.org/rfc/rfc2385.txt>²⁰⁰⁰ <http://www.securityfocus.com/bid/4314>²⁰⁰¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>²⁰⁰² <http://xforce.iss.net/xforce/xfdb/8588>²⁰⁰³ <http://www.securityfocus.com/bid/26838>²⁰⁰⁴ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>²⁰⁰⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-5000>²⁰⁰⁶ <http://www.osvdb.org/39134>²⁰⁰⁷ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:9539>²⁰⁰⁸ <http://rhn.redhat.com/errata/RHSA-2008-0004.html>

			REDHAT RHSA- 2008:0006 ²⁰¹⁰ REDHAT RHSA- 2008:0007 ²⁰¹¹ REDHAT RHSA- 2008:0008 ²⁰¹² REDHAT RHSA- 2008:0009 ²⁰¹³ REDHAT RHSA- 2008:0261 ²⁰¹⁴ SECUNIA 28046 ²⁰¹⁵ SECUNIA 28073 ²⁰¹⁶ SECUNIA 28081 ²⁰¹⁷ SECUNIA 28196 ²⁰¹⁸ SECUNIA 28375 ²⁰¹⁹ SECUNIA 28467 ²⁰²⁰ SECUNIA 28471 ²⁰²¹ SECUNIA 28525 ²⁰²² SECUNIA 28526 ²⁰²³ SECUNIA 28607 ²⁰²⁴ SECUNIA 28749 ²⁰²⁵ SECUNIA 28750 ²⁰²⁶ SECUNIA 28922 ²⁰²⁷ SECUNIA 28977 ²⁰²⁸ SECUNIA 29420 ²⁰²⁹ SECUNIA 29640 ²⁰³⁰ SECUNIA 29806 ²⁰³¹ SECUNIA 29988 ²⁰³² SECUNIA 30356 ²⁰³³ SECUNIA 30430 ²⁰³⁴ SECUNIA 30732 ²⁰³⁵ SECUNIA 31142 ²⁰³⁶ SUSE SUSE- SA:2008:021 ²⁰³⁷ URL1 ²⁰³⁸		
33.	Apache HTTP Method 413 Error Response Cross-Site Scripting	172.23.202.126:80 172.23.202.225:80	APPLE APPLE-SA- 2008-03-18 ²⁰³⁹ BID 26663 ²⁰⁴⁰	Ozbiljan	Apache >= 2.0 and < 2.1 Ažurirati na Apache verziju 2.0.63

²⁰⁰⁹ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>²⁰¹⁰ <http://rhn.redhat.com/errata/RHSA-2008-0006.html>²⁰¹¹ <http://rhn.redhat.com/errata/RHSA-2008-0007.html>²⁰¹² <http://rhn.redhat.com/errata/RHSA-2008-0008.html>²⁰¹³ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>²⁰¹⁴ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>²⁰¹⁵ <http://secunia.com/advisories/28046/>²⁰¹⁶ <http://secunia.com/advisories/28073/>²⁰¹⁷ <http://secunia.com/advisories/28081/>²⁰¹⁸ <http://secunia.com/advisories/28196/>²⁰¹⁹ <http://secunia.com/advisories/28375/>²⁰²⁰ <http://secunia.com/advisories/28467/>²⁰²¹ <http://secunia.com/advisories/28471/>²⁰²² <http://secunia.com/advisories/28525/>²⁰²³ <http://secunia.com/advisories/28526/>²⁰²⁴ <http://secunia.com/advisories/28607/>²⁰²⁵ <http://secunia.com/advisories/28749/>²⁰²⁶ <http://secunia.com/advisories/28750/>²⁰²⁷ <http://secunia.com/advisories/28922/>²⁰²⁸ <http://secunia.com/advisories/28977/>²⁰²⁹ <http://secunia.com/advisories/29420/>²⁰³⁰ <http://secunia.com/advisories/29640/>²⁰³¹ <http://secunia.com/advisories/29806/>²⁰³² <http://secunia.com/advisories/29988/>²⁰³³ <http://secunia.com/advisories/30356/>²⁰³⁴ <http://secunia.com/advisories/30430/>²⁰³⁵ <http://secunia.com/advisories/30732/>²⁰³⁶ <http://secunia.com/advisories/31142/>²⁰³⁷ <https://www.suse.com/support/security/advisories/>²⁰³⁸ http://httpd.apache.org/security/vulnerabilities_20.html²⁰³⁹ <http://lists.apple.com/archives/security-announce/2008/Mar/msg00000.html>²⁰⁴⁰ <http://www.securityfocus.com/bid/26663>

	Vulnerability (http-apache-malformed-413-response-xss)	Određene verzije Apache web servera ne saniraju na odgovarajući način metodu zahteva na 413 stranici sa pogrešnim odgovorom koja je uzvrćena kad je zlonameran zahtev sa velikom vrednošću za dužinu sadržaja (Content-Length) poslat serveru. Nedostatak izlaza uzrokuje ranjivost na XSS napade na serveru. Ova ranjivost se može iskoristiti samo ako napadnuti HTTP klijent bude primoran da pošalje HTTP zahtev sa nevalidnim imenom metoda.	CVE CVE-2007-6203²⁰⁴¹ SECUNIA 27906²⁰⁴² SECUNIA 28196²⁰⁴³ SECUNIA 29348²⁰⁴⁴ SECUNIA 29420²⁰⁴⁵ SECUNIA 29640²⁰⁴⁶ SECUNIA 30356²⁰⁴⁷ SECUNIA 30732²⁰⁴⁸ SECUNIA 33105²⁰⁴⁹ SECUNIA 34219²⁰⁵⁰ XF apache-413error-xss(38800)²⁰⁵¹ URL1²⁰⁵² URL2²⁰⁵³ URL3²⁰⁵⁴ URL4²⁰⁵⁵		Apache 2.0.62 nikada nije pušten u opticaj usled problema u kvalitetu koji su otkriveni u tarbolima pre puštanja u promet. Umesto toga, ažurirati na Apache verziju 2.0.63. Apache >= 2.1 and < 2.3 Ažurirajte na Apache verziju 2.2.7 Apache 2.2.7 nikada nije pušten u opticaj usled problema u kvalitetu koji su otkriveni u tarbolima pre puštanja u promet. Umesto toga, ažurirati na Apache 2.2.8.
34.	Apache httpd mod_status cross-site scripting (CVE-2006-5752) (apache-httpd-2_0_x-mod_status-crosssite-scripting-cve-2006-5752)	172.23.202.126:80 172.23.202.225:80 Propust je otkriven u modulu mod_status. Na sajtovima na kojima je status servera javno dostupan i omogućen je ExtendedStatus, postoji mogućnost XSS napada. Stranica sa statusom servera nije po difoltu omogućena, a dosadašnja praksa je pokazala da je najbolje da ona ne bude javno dostupna.	BID 24645²⁰⁵⁶ CVE CVE-2006-5752²⁰⁵⁷ OVAL OVAL10154²⁰⁵⁸ REDHAT RHSA-2007:0532²⁰⁵⁹ REDHAT RHSA-2007:0533²⁰⁶⁰ REDHAT RHSA-2007:0534²⁰⁶¹ REDHAT RHSA-2007:0556²⁰⁶² REDHAT RHSA-2007:0557²⁰⁶³ REDHAT RHSA-2008:0261²⁰⁶⁴ SECUNIA 25827²⁰⁶⁵ SECUNIA 25830²⁰⁶⁶ SECUNIA 25873²⁰⁶⁷ SECUNIA 25920²⁰⁶⁸ SECUNIA 26273²⁰⁶⁹ SECUNIA 26443²⁰⁷⁰ SECUNIA 26458²⁰⁷¹	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.61.tar.gz

²⁰⁴¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6203>

²⁰⁴² <http://secunia.com/advisories/27906/>

²⁰⁴³ <http://secunia.com/advisories/28196/>

²⁰⁴⁴ <http://secunia.com/advisories/29348/>

²⁰⁴⁵ <http://secunia.com/advisories/29420/>

²⁰⁴⁶ <http://secunia.com/advisories/29640/>

²⁰⁴⁷ <http://secunia.com/advisories/30356/>

²⁰⁴⁸ <http://secunia.com/advisories/30732/>

²⁰⁴⁹ <http://secunia.com/advisories/33105/>

²⁰⁵⁰ <http://secunia.com/advisories/34219/>

²⁰⁵¹ <http://xforce.iss.net/xforce/xfdb/38800>

²⁰⁵² http://procheckup.com/Vulnerability_PR07-37.php

²⁰⁵³ <http://svn.apache.org/viewvc?revision=600645&view=revision>

²⁰⁵⁴ <http://svn.apache.org/viewvc?revision=602473&view=revision>

²⁰⁵⁵ <http://svn.apache.org/viewvc?revision=604425&view=revision>

²⁰⁵⁶ <http://www.securityfocus.com/bid/24645>

²⁰⁵⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-5752>

²⁰⁵⁸ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval:def:10154>

²⁰⁵⁹ <http://rhn.redhat.com/errata/RHSA-2007-0532.html>

²⁰⁶⁰ <http://rhn.redhat.com/errata/RHSA-2007-0533.html>

²⁰⁶¹ <http://rhn.redhat.com/errata/RHSA-2007-0534.html>

²⁰⁶² <http://rhn.redhat.com/errata/RHSA-2007-0556.html>

²⁰⁶³ <http://rhn.redhat.com/errata/RHSA-2007-0557.html>

²⁰⁶⁴ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>

²⁰⁶⁵ <http://secunia.com/advisories/25827/>

²⁰⁶⁶ <http://secunia.com/advisories/25830/>

²⁰⁶⁷ <http://secunia.com/advisories/25873/>

²⁰⁶⁸ <http://secunia.com/advisories/25920/>

²⁰⁶⁹ <http://secunia.com/advisories/26273/>

²⁰⁷⁰ <http://secunia.com/advisories/26443/>

²⁰⁷¹ <http://secunia.com/advisories/26458/>

			SECUNIA 26508 ²⁰⁷² SECUNIA 26822 ²⁰⁷³ SECUNIA 26842 ²⁰⁷⁴ SECUNIA 26993 ²⁰⁷⁵ SECUNIA 27037 ²⁰⁷⁶ SECUNIA 27563 ²⁰⁷⁷ SECUNIA 27732 ²⁰⁷⁸ SECUNIA 28212 ²⁰⁷⁹ SECUNIA 28224 ²⁰⁸⁰ SECUNIA 28606 ²⁰⁸¹ SUSE SA:2007:061 ²⁰⁸² XF apache-modstatus- xss(35097) URL1 ²⁰⁸³		
35.	Apache httpd Subrequest handling of request headers (mod_headers) (CVE- 2010-0434) (apache- httpd- 2_0_x-subrequest- handling-of-request- headers-mod_headers- cve-2010-0434)	172.23.202.126:80 172.23.202.225:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_headers. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust u jezgru "subrequest process code" može dovesti do greške tipa segmentation fault-a ili do otkrivanja podataka iz nekog drugog zahteva na thread-ovima servera, kao što su worker ili winnt MPM-ovi. Zahvaljujući Philip Pickett-u iz Vmware, ovaj propust je prijavljen i predložen je način ispravke.	APPLE APPLE-SA- 2010-11-10 ²⁰⁸⁴ BID 38494 ²⁰⁸⁵ CVE CVE-2010-0434 ²⁰⁸⁶ DEBIAN DSA-2035 ²⁰⁸⁷ OVAL OVAL10358 ²⁰⁸⁸ OVAL OVAL8695 ²⁰⁸⁹ REDHAT RHSA- 2010:0168 ²⁰⁹⁰ REDHAT RHSA- 2010:0175 ²⁰⁹¹ SECUNIA 39100 ²⁰⁹² SECUNIA 39115 ²⁰⁹³ SECUNIA 39501 ²⁰⁹⁴ SECUNIA 39628 ²⁰⁹⁵ SECUNIA 39632 ²⁰⁹⁶ SECUNIA 39656 ²⁰⁹⁷ SECUNIA 40096 ²⁰⁹⁸ XF apache-http-rh-info- disclosure(56625) ²⁰⁹⁹ URL1 ²¹⁰⁰	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/ httpd/httpd-2.0.64.tar.gz
36.	Apache httpd mod_proxy_ftp globbing XSS (CVE-	172.23.202.126:80 172.23.202.225:80 Skenirani servis je osetljiv na ovu	BID 30560 ²¹⁰¹ CERT TA09-133A ²¹⁰² CERT-VN 663763 ²¹⁰³	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati:

²⁰⁷² <http://secunia.com/advisories/26508/>²⁰⁷³ <http://secunia.com/advisories/26822/>²⁰⁷⁴ <http://secunia.com/advisories/26842/>²⁰⁷⁵ <http://secunia.com/advisories/26993/>²⁰⁷⁶ <http://secunia.com/advisories/27037/>²⁰⁷⁷ <http://secunia.com/advisories/27563/>²⁰⁷⁸ <http://secunia.com/advisories/27732/>²⁰⁷⁹ <http://secunia.com/advisories/28212/>²⁰⁸⁰ <http://secunia.com/advisories/28224/>²⁰⁸¹ <http://secunia.com/advisories/28606/>²⁰⁸² <https://www.suse.com/support/security/advisories/>²⁰⁸³ http://httpd.apache.org/security/vulnerabilities_20.html²⁰⁸⁴ <http://support.apple.com/kb/ht4435>²⁰⁸⁵ <http://www.securityfocus.com/bid/38494>²⁰⁸⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0434>²⁰⁸⁷ <http://www.debian.org/security/2010/dsa-2035>²⁰⁸⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10358>²⁰⁸⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8695>²⁰⁹⁰ <http://rhn.redhat.com/errata/RHSA-2010-0168.html>²⁰⁹¹ <http://rhn.redhat.com/errata/RHSA-2010-0175.html>²⁰⁹² <http://secunia.com/advisories/39100/>²⁰⁹³ <http://secunia.com/advisories/39115/>²⁰⁹⁴ <http://secunia.com/advisories/39501/>²⁰⁹⁵ <http://secunia.com/advisories/39628/>²⁰⁹⁶ <http://secunia.com/advisories/39632/>²⁰⁹⁷ <http://secunia.com/advisories/39656/>²⁰⁹⁸ <http://secunia.com/advisories/40096/>²⁰⁹⁹ <http://xforce.iss.net/xforce/xfdb/56625>²¹⁰⁰ http://httpd.apache.org/security/vulnerabilities_20.html²¹⁰¹ <http://www.securityfocus.com/bid/30560>²¹⁰² <http://www.us-cert.gov/ncas/alerts/TA09-133A>

	2008-2939) (http-apache-mod-proxy-ftp-wildcard-xss)	ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ftp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u modulu mod_proxy_ftp prilikom obrade "wildcard"-a ukoliko se on nađe na putanji FTP URL. Ukoliko je mod_proxy_ftp omogućen da podržava FTP-over-HTTP, zahtevi koji sadrže specijalne karaktere mogu da dovedu do cross-site scripting napada (XSS).	CVE CVE-2008-2939 ²¹⁰⁴ OVAL OVAL11316 ²¹⁰⁵ OVAL OVAL7716 ²¹⁰⁶ REDHAT RHSA-2008:0966 ²¹⁰⁷ REDHAT RHSA-2008:0967 ²¹⁰⁸ SECUNIA 31384 ²¹⁰⁹ SECUNIA 31673 ²¹¹⁰ SECUNIA 32685 ²¹¹¹ SECUNIA 32838 ²¹¹² SECUNIA 33156 ²¹¹³ SECUNIA 33797 ²¹¹⁴ SECUNIA 34219 ²¹¹⁵ SECUNIA 35074 ²¹¹⁶ XF apache-modproxyftp-xss(44223). ²¹¹⁷ URL1 ²¹¹⁸		http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
37.	Apache httpd mod_imap Referer Cross-Site Scripting (CVE-2005-3352) (http-apache-mod_imap-xss)	172.23.202.126:80 172.23.202.225:80 Propust u modulu mod_imap prilikom upotrebe direktiva Referer sa mapama slika (eng. imagemaps). U određenim konfiguracijama sajtova, udaljeni napadač bi mogao da izvrši napad unakrsnog skriptovanja, ako bi korisnik bio naveden da poseti zlonamerni URL koristeći određene web pretraživače.	BID 15834 ²¹¹⁹ CERT TA08-150A ²¹²⁰ CVE CVE-2005-3352 ²¹²¹ DEBIAN DSA-1167 ²¹²² OVAL OVAL10480 ²¹²³ REDHAT RHSA-2006:0158 ²¹²⁴ REDHAT RHSA-2006:0159 ²¹²⁵ REDHAT RHSA-2006:0692 ²¹²⁶ SECUNIA 17319 ²¹²⁷ SECUNIA 18008 ²¹²⁸ SECUNIA 18333 ²¹²⁹ SECUNIA 18339 ²¹³⁰ SECUNIA 18340 ²¹³¹ SECUNIA 18429 ²¹³² SECUNIA 18517 ²¹³³ SECUNIA 18526 ²¹³⁴ SECUNIA 18585 ²¹³⁵	Ozbiljan	Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.58.tar.gz

²¹⁰³ <http://www.kb.cert.org/vuls/id/663763>²¹⁰⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-2939>²¹⁰⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11316>²¹⁰⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7716>²¹⁰⁷ <http://rhn.redhat.com/errata/RHSA-2008-0966.html>²¹⁰⁸ <http://rhn.redhat.com/errata/RHSA-2008-0967.html>²¹⁰⁹ <http://secunia.com/advisories/31384/>²¹¹⁰ <http://secunia.com/advisories/31673/>²¹¹¹ <http://secunia.com/advisories/32685/>²¹¹² <http://secunia.com/advisories/32838/>²¹¹³ <http://secunia.com/advisories/33156/>²¹¹⁴ <http://secunia.com/advisories/33797/>²¹¹⁵ <http://secunia.com/advisories/34219/>²¹¹⁶ <http://secunia.com/advisories/35074/>²¹¹⁷ <http://xforce.iss.net/xforce/xfdb/44223>²¹¹⁸ http://httpd.apache.org/security/vulnerabilities_20.html²¹¹⁹ <http://www.securityfocus.com/bid/15834>²¹²⁰ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>²¹²¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-3352>²¹²² <http://lists.debian.org/debian-security-announce/2006/msg00257.html>²¹²³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10480>²¹²⁴ <http://rhn.redhat.com/errata/RHSA-2006-0158.html>²¹²⁵ <http://rhn.redhat.com/errata/RHSA-2006-0159.html>²¹²⁶ <http://rhn.redhat.com/errata/RHSA-2006-0692.html>²¹²⁷ <http://secunia.com/advisories/17319/>²¹²⁸ <http://secunia.com/advisories/18008/>²¹²⁹ <http://secunia.com/advisories/18333/>²¹³⁰ <http://secunia.com/advisories/18339/>²¹³¹ <http://secunia.com/advisories/18340/>²¹³² <http://secunia.com/advisories/18429/>²¹³³ <http://secunia.com/advisories/18517/>²¹³⁴ <http://secunia.com/advisories/18526/>

			SECUNIA 18743 ²¹³⁶ SECUNIA 19012 ²¹³⁷ SECUNIA 20046 ²¹³⁸ SECUNIA 20670 ²¹³⁹ SECUNIA 21744 ²¹⁴⁰ SECUNIA 22140 ²¹⁴¹ SECUNIA 22368 ²¹⁴² SECUNIA 22388 ²¹⁴³ SECUNIA 22669 ²¹⁴⁴ SECUNIA 23260 ²¹⁴⁵ SECUNIA 25239 ²¹⁴⁶ SECUNIA 29420 ²¹⁴⁷ SECUNIA 29849 ²¹⁴⁸ SECUNIA 30430 ²¹⁴⁹ SGI 20060101-01-U ²¹⁵⁰ SUSE SUSE-SA:2006:043 ²¹⁵¹ URL1 ²¹⁵²		
38.	Apache httpd mod_proxy_ftp UTF-7 XSS (CVE-2008-0005) (http-apache-mod_proxy_ftp-utf7-xss)	172.23.202.126:80 172.23.202.225:80 U modul mod_proxy_ftp je dodata zaobilaznica. Na sajtovima na kojima je omogućen mod_proxy_ftp i konfigurisan je forward tip proxy-ja, moguće je izvesti napad XSS na Web pretraživače koji ne prepoznaju određeni character set prema pravilima iz dokumenta RFC 2616.	BID 27234 ²¹⁵³ CVE CVE-2008-0005 ²¹⁵⁴ OVAL OVAL10812 ²¹⁵⁵ REDHAT RHSA-2008:0004 ²¹⁵⁶ REDHAT RHSA-2008:0005 ²¹⁵⁷ REDHAT RHSA-2008:0006 ²¹⁵⁸ REDHAT RHSA-2008:0007 ²¹⁵⁹ REDHAT RHSA-2008:0008 ²¹⁶⁰ REDHAT RHSA-2008:0009 ²¹⁶¹ SECUNIA 28467 ²¹⁶² SECUNIA 28471 ²¹⁶³ SECUNIA 28526 ²¹⁶⁴ SECUNIA 28607 ²¹⁶⁵ SECUNIA 28749 ²¹⁶⁶	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.63.tar.gz

²¹³⁵ <http://secunia.com/advisories/18585/>²¹³⁶ <http://secunia.com/advisories/18743/>²¹³⁷ <http://secunia.com/advisories/19012/>²¹³⁸ <http://secunia.com/advisories/20046/>²¹³⁹ <http://secunia.com/advisories/20670/>²¹⁴⁰ <http://secunia.com/advisories/21744/>²¹⁴¹ <http://secunia.com/advisories/22140/>²¹⁴² <http://secunia.com/advisories/22368/>²¹⁴³ <http://secunia.com/advisories/22388/>²¹⁴⁴ <http://secunia.com/advisories/22669/>²¹⁴⁵ <http://secunia.com/advisories/23260/>²¹⁴⁶ <http://secunia.com/advisories/25239/>²¹⁴⁷ <http://secunia.com/advisories/29420/>²¹⁴⁸ <http://secunia.com/advisories/29849/>²¹⁴⁹ <http://secunia.com/advisories/30430/>²¹⁵⁰ <ftp://patches.sgi.com/support/free/security/advisories/20060101-01-U> pristupljeno 18.12.2011²¹⁵¹ <https://www.suse.com/support/security/advisories/>²¹⁵² http://httpd.apache.org/security/vulnerabilities_20.html²¹⁵³ <http://www.securityfocus.com/bid/27234>²¹⁵⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0005>²¹⁵⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10812>²¹⁵⁶ <http://rhn.redhat.com/errata/RHSA-2008-0004.html>²¹⁵⁷ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>²¹⁵⁸ <http://rhn.redhat.com/errata/RHSA-2008-0006.html>²¹⁵⁹ <http://rhn.redhat.com/errata/RHSA-2008-0007.html>²¹⁶⁰ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>²¹⁶¹ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>²¹⁶² <http://secunia.com/advisories/28467/>²¹⁶³ <http://secunia.com/advisories/28471/>²¹⁶⁴ <http://secunia.com/advisories/28526/>²¹⁶⁵ <http://secunia.com/advisories/28607/>²¹⁶⁶ <http://secunia.com/advisories/28749/>

			SECUNIA 28977 ²¹⁶⁷ SECUNIA 29348 ²¹⁶⁸ SECUNIA 29420 ²¹⁶⁹ SECUNIA 29640 ²¹⁷⁰ SECUNIA 30732 ²¹⁷¹ SECUNIA 35650 ²¹⁷² SUSE SUSE-SA:2008:021 ²¹⁷³ XF apache-modproxyftp-utf7-xss(39615) URL1 ²¹⁷⁴		
39.	Apache httpd mod_status XSS (CVE-2007-6388) (http://apache-mod_status-open-redirect)	172.23.202.126:80 172.23.202.225:80 Propust je otkriven u modulu mod_status. Na sajtovima na kojima je omogućen mod_status ukoliko su stranice statusa javno dostupne, postoji mogućnost XSS napada. Stranica sa statusom servera nije po defaultu omogućena, a dosadašnja praksa je pokazala da je najbolje da ona ne bude javno dostupna.	BID 27237 ²¹⁷⁵ CERT TA08-150A ²¹⁷⁶ CVE CVE-2007-6388 ²¹⁷⁷ OVAL OVAL10272 ²¹⁷⁸ REDHAT RHSA-2008:0004 ²¹⁷⁹ REDHAT RHSA-2008:0005 ²¹⁸⁰ REDHAT RHSA-2008:0006 ²¹⁸¹ REDHAT RHSA-2008:0007 ²¹⁸² REDHAT RHSA-2008:0008 ²¹⁸³ REDHAT RHSA-2008:0009 ²¹⁸⁴ REDHAT RHSA-2008:0261 ²¹⁸⁵ SECUNIA 28467 ²¹⁸⁶ SECUNIA 28471 ²¹⁸⁷ SECUNIA 28526 ²¹⁸⁸ SECUNIA 28607 ²¹⁸⁹ SECUNIA 28749 ²¹⁹⁰ SECUNIA 28922 ²¹⁹¹ SECUNIA 28965 ²¹⁹² SECUNIA 28977 ²¹⁹³ SECUNIA 29420 ²¹⁹⁴ SECUNIA 29504 ²¹⁹⁵ SECUNIA 29640 ²¹⁹⁶	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.63.tar.gz

²¹⁶⁷ <http://secunia.com/advisories/28977/>²¹⁶⁸ <http://secunia.com/advisories/29348/>²¹⁶⁹ <http://secunia.com/advisories/29420/>²¹⁷⁰ <http://secunia.com/advisories/29640/>²¹⁷¹ <http://secunia.com/advisories/30732/>²¹⁷² <http://secunia.com/advisories/35650/>²¹⁷³ <https://www.suse.com/support/security/advisories/>²¹⁷⁴ http://httpd.apache.org/security/vulnerabilities_20.html²¹⁷⁵ <http://www.securityfocus.com/bid/27237>²¹⁷⁶ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>²¹⁷⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6388>²¹⁷⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10272>²¹⁷⁹ <http://rhn.redhat.com/errata/RHSA-2008-0004.html>²¹⁸⁰ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>²¹⁸¹ <http://rhn.redhat.com/errata/RHSA-2008-0006.html>²¹⁸² <http://rhn.redhat.com/errata/RHSA-2008-0007.html>²¹⁸³ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>²¹⁸⁴ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>²¹⁸⁵ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>²¹⁸⁶ <http://secunia.com/advisories/28467/>²¹⁸⁷ <http://secunia.com/advisories/28471/>²¹⁸⁸ <http://secunia.com/advisories/28526/>²¹⁸⁹ <http://secunia.com/advisories/28607/>²¹⁹⁰ <http://secunia.com/advisories/28749/>²¹⁹¹ <http://secunia.com/advisories/28922/>²¹⁹² <http://secunia.com/advisories/28965/>²¹⁹³ <http://secunia.com/advisories/28977/>²¹⁹⁴ <http://secunia.com/advisories/29420/>²¹⁹⁵ <http://secunia.com/advisories/29504/>²¹⁹⁶ <http://secunia.com/advisories/29640/>

			SECUNIA 29806 ²¹⁹⁷ SECUNIA 29988 ²¹⁹⁸ SECUNIA 30356 ²¹⁹⁹ SECUNIA 30430 ²²⁰⁰ SECUNIA 30732 ²²⁰¹ SECUNIA 31142 ²²⁰² SECUNIA 33200 ²²⁰³ SUSE SA:2008:021 ²²⁰⁴ XF apache-status-page-xss(39472) ²²⁰⁵		
40.	Apache httpd HTTP Request Spoofing (CVE-2005-2088) (http://apache-request-smuggling-vuln)	172.23.202.126:80 172.23.202.225:80 Propust je otkriven prilikom upotrebe Apache servera kao HTTP proxy servera. Udaljeni napadač bi mogao da pošalje HTTP zahtev sa hederom „Transfer- Encoding: chunked“ i hederom Content-Length (dužina sadržaja), što bi dovelo do toga da Apache nepropisno obradi i prosledi sadržaj zahteva na način koji prouzrokuje da ga server koji ga prima obradi kao poseban HTTP zahtev. Ovo bi moglo da omogućiti zaobilaženje softverskog fajervola zaštite ili da dovede do XSS napada.	BID 14106 ²²⁰⁶ BID 15647 ²²⁰⁷ CVE CVE-2005-2088 ²²⁰⁸ DEBIAN DSA-803 ²²⁰⁹ DEBIAN DSA-805 ²²¹⁰ OVAL OVAL11452 ²²¹¹ OVAL OVAL1237 ²²¹² OVAL OVAL1526 ²²¹³ OVAL OVAL1629 ²²¹⁴ OVAL OVAL840 ²²¹⁵ REDHAT RHSA-2005:582 ²²¹⁶ SECUNIA 14530 ²²¹⁷ SECUNIA 17319 ²²¹⁸ SECUNIA 17487 ²²¹⁹ SECUNIA 17813 ²²²⁰ SECUNIA 19072 ²²²¹ SECUNIA 19073 ²²²² SECUNIA 19185 ²²²³ SECUNIA 19317 ²²²⁴ SECUNIA 23074 ²²²⁵ SUSE SA:2005:046 ²²²⁶	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.55.tar.gz
41.	OpenSSH CBC Mode Information Disclosure Vulnerability (ssh-)	172.23.202.126:22 172.23.202.225:22	BID 32319 ²²²⁷ CVE CVE-2008-5161 ²²²⁸ SECUNIA 32760 ²²²⁹	Ozbiljan	Uraditi download a zatim instalirati: ftp://ftp.openbsd.org/pub/O

²¹⁹⁷ <http://secunia.com/advisories/29806/>²¹⁹⁸ <http://secunia.com/advisories/29988/>²¹⁹⁹ <http://secunia.com/advisories/30356/>²²⁰⁰ <http://secunia.com/advisories/30430/>²²⁰¹ <http://secunia.com/advisories/30732/>²²⁰² <http://secunia.com/advisories/31142/>²²⁰³ <http://secunia.com/advisories/33200/>²²⁰⁴ <https://www.suse.com/support/security/advisories/>²²⁰⁵ <http://xforce.iss.net/xforce/xfdb/39472> pristupljeno 11.12.2011²²⁰⁶ <http://www.securityfocus.com/bid/14106>²²⁰⁷ <http://www.securityfocus.com/bid/15647>²²⁰⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2088>²²⁰⁹ <http://lists.debian.org/debian-security-announce/2005/msg00193.html>²²¹⁰ <https://security-tracker.debian.org/tracker/DSA-805-1>²²¹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11452>²²¹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1237>²²¹³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1526>²²¹⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1629>²²¹⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:840>²²¹⁶ <http://rhn.redhat.com/errata/RHSA-2005-582.html>²²¹⁷ <http://secunia.com/advisories/14530/>²²¹⁸ <http://secunia.com/advisories/17319/>²²¹⁹ <http://secunia.com/advisories/17487/>²²²⁰ <http://secunia.com/advisories/17813/>²²²¹ <http://secunia.com/advisories/19072/>²²²² <http://secunia.com/advisories/19073/>²²²³ <http://secunia.com/advisories/19185/>²²²⁴ <http://secunia.com/advisories/19317/>²²²⁵ <http://secunia.com/advisories/23074/>²²²⁶ <https://www.suse.com/support/security/advisories/>²²²⁷ <http://www.securityfocus.com/bid/32319>²²²⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-5161>²²²⁹ <http://secunia.com/advisories/32760/>

	openssh-cbc-mode-info-disclosure)	Određene verzije OpenSSH-a poseduju ranjivu implementaciju blok šifarskog algoritma u CBC (Cipher Block Chaining) modu. Ovo bi udaljenom napadaču moglo omogućiti da preko nepoznatih vektora pridobije određene podatke u vidu običnog teksta iz arbitrarnog bloka šifrovanog teksta u SSH sesiji.	URL1 ²²³⁰		penBSD/OpenSSH/portable/openssh-5.2p1.tar.gz Verzija 5.2 OpenSSH-a je puštena u promet 22. februara 2009.
42.	OpenSSH „known_hosts“ File Information Disclosure (ssh-openssh-known_hosts-file-info-leak)	172.23.202.126:22 172.23.202.225:22 Verzije OpenSSH pre 4.0 čuvale su imena hostova, IP adrese i oznake u običnom tekstu, u fajlu „known_hosts“. To može omogućiti napadaču koji poseduje kompromitovan nalog SSH korisnika da generiše listu dodatnih meta za koje postoji mogućnost da poseduju istu šifru ili ključ.	CVE CVE-2005-2666 ²²³¹	Ozbiljan	Uraditi download a zatim instalirati: http://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-4.0p1.tar.gz Verzija 4.0 OpenSSH-a je puštena u promet 22. februara 2009. Izvorni kôd za ovaj program se može preuzeti sa http://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-4.0p1.tar.gz .
43.	OpenSSH „X11UseLocalhost“ X11 Forwarding Session Hijacking Vulnerability (ssh-opensshx11uselocalhost - x11-forwarding-session-hijack)	172.23.202.126:22 172.23.202.225:22 Određene verzije OpenSSH-a podešavaju SO_REUSEADDR socket opciju kada je onemogućeno podešavanje X11UseLocalhost konfiguracije. Ovo bi lokalnom napadaču moglo da omogući da preuzme X11 port prosleđivanja preko veze ka pojedinačnoj IP adresi.	BID 30339 ²²³² CVE CVE-2008-3259 ²²³³ SECUNIA 31179 ²²³⁴	Ozbiljan	Uraditi download a zatim instalirati: http://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-5.1p1.tar.gz Verzija 5.1 OpenSSH-a je puštena u promet 21. jula 2008.
44.	SSH server supports SSH protocol v1 clients (ssh-v1-supported)	172.23.202.126:22 172.23.202.225:22 SSH server podržava klijente SSH verzije 1. Verzija 1 SSH protokola sadrži osnovne slabosti koje dovode do toga da su sesije ranjive na napade preko posrednika. S obzirom da su svi savremeni SSH klijenti podržavali SSH v2 tokom najmanje 5 godina, ne postoji potreba da se podržava SSHv1.	CERT-VN 13877 ²²³⁵ CERT-VN 315308 ²²³⁶ CVE CVE-2001-1473 ²²³⁷	Kritičan	Potrebno je konfigurisati SSH server tako da podržava samo protokol verziju 2. Za servere bazirane na OpenSSH, izmenite liniju „Protocol“ u fajlu sshd_config tako da piše: Protocol 2 Za sisteme koji nisu bazirani na OpenSSH, trebalo bi nadograditi verziju operativnog sistema tako da omogući SSHv2 podršku.
45.	Apache httpd mod_disk_cache stores sensitive headers (CVE-2004-1834) (apache-httpd-2.0_xmod_disk_cache-stores-	172.23.202.126:80 172.23.202.225:80 Eksperimentalan modul mod_disk_cache je sačuvao poverljive podatke klijenta za keširane objekte, kao što su poverljivi	BID 9933 ²²³⁸ CVE CVE-2004-1834 ²²³⁹ OSVDB 4446 ²²⁴⁰ OVAL OVAL11133 ²²⁴¹ REDHAT RHSA-2004:562 ²²⁴²	Umeren	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.53.tar.gz

²²³⁰ <http://www.openssh.com/txt/cbc.adv>²²³¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2666>²²³² <http://www.securityfocus.com/bid/30339>²²³³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-3259>²²³⁴ <http://secunia.com/advisories/31179/>²²³⁵ <http://www.kb.cert.org/vuls/id/13877>²²³⁶ <http://www.kb.cert.org/vuls/id/315308>²²³⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2001-1473>²²³⁸ <http://www.securityfocus.com/bid/9933>²²³⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-1834>²²⁴⁰ <http://www.osvdb.org/4446>²²⁴¹ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval:def:11133>²²⁴² <http://rhn.redhat.com/errata/RHSA-2004-562.html>

	sensitive-headers-cve-2004-1834)	podaci proxy autentifikacija i šifre osnovne autentifikacije na disku.	SECUNIA 11176 ²²⁴³ SECUNIA 19072 ²²⁴⁴ URL1 ²²⁴⁵		
46.	HTTP TRACE Method Enabled (http-trace-method-enabled)	172.23.202.126:80 172.23.202.225:80 HTTP TRACE metoda se obično koristi da uzvratni potpuni HTTP zahtev klijentu koji ga zahteva, u cilju debugovanja proxy servera. Napadač bi mogao da kreira web stranicu koristeći XMLHTTP, ActiveX ili XMLHttpRequest da natera klijenta da pošalje TRACE zahtev i da sačuva klijenove kolačiće. Kao posledica može da se javi XSS napad. Primer: 172.23.202.126:80 Running vulnerable HTTP service. http://172.23.202.126/ 1: TRACE / HTTP/1.1 2: Host: 172.23.202.126 3: Cookie: vulnerable=yes	CVE CVE-2004-2320 ²²⁴⁶ CVE CVE-2004-2763 ²²⁴⁷ CVE CVE-2005-3398 ²²⁴⁸ CVE CVE-2006-4683 ²²⁴⁹ CVE CVE-2007-3008 ²²⁵⁰ CVE CVE-2008-7253 ²²⁵¹ CVE CVE-2009-2823 ²²⁵² CVE CVE-2010-0386 ²²⁵³ OSVDB 877 ²²⁵⁴ SUN 50603 ²²⁵⁵ BID 9561 ²²⁵⁶ URL1 ²²⁵⁷ URL2 ²²⁵⁸	Ozbiljan	Apache Onemogućiti HTTP TRACE metodu za Apache. Novije verzije Apache-a (1.3.34 i 2.0.55 i novije) omogućuju konfiguracionu direktivu koja se zove TraceEnable. Da bi se odbili TRACE zahtevi, dodaje se sledeći red u konfiguraciju servera: TraceEnable off Za starije verzije Apache web servera, koristiti modul mod_rewrite da bi se odbili TRACE zahteve: RewriteEngine On RewriteCond %{REQUEST_METHOD} ^TRACE RewriteRule .* - [F]
47.	Database Open Access (database-open-access)	172.23.202.126:3306 172.23.202.225:3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićeni sigurnosnim mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7.	URL1 ²²⁵⁹	Umeren	Konfigurisati server baze podataka tako da dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.
48.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše	CVE CVE-1999-0524 ²²⁶⁰ OSVDB 95 ²²⁶¹ XF icmp-netmask(306) ²²⁶² XF icmp-timestamp(322) ²²⁶³	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola.

²²⁴³ <http://secunia.com/advisories/11176/>²²⁴⁴ <http://secunia.com/advisories/19072/>²²⁴⁵ http://httpd.apache.org/security/vulnerabilities_20.html²²⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2320>²²⁴⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2763>²²⁴⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-3398>²²⁴⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-4683>²²⁵⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3008>²²⁵¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-7253>²²⁵² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2823>²²⁵³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0386>²²⁵⁴ <http://osvdb.org/877>²²⁵⁵ <https://sunsolve.sun.com/search/document.do?assetkey=1-22-50603-1> pristupljeno 18.12.2011²²⁵⁶ <http://www.securityfocus.com/bid/9561>²²⁵⁷ <http://www.apacheweek.com/issues/03-01-24#news>²²⁵⁸ <http://www.kb.cert.org/vuls/id/867593>²²⁵⁹ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf²²⁶⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>²²⁶¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>²²⁶² <http://xforce.iss.net/xforce/xfdb/306>²²⁶³ <http://xforce.iss.net/xforce/xfdb/322>

		slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.			Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
49.	WebDAV Extensions are Enabled (http-generic-webdav-enabled)	172.23.202.126:8080 172.23.202.225:8080 WebDAV je skup ekstenzija za HTTP protokol koji omogućava korisnicima da zajednički edituju i obrađuju fajlove na udaljenim web serverima. Mnogi web serveri po defaultu omogućavaju WebDAV ekstenzije, čak i kada nisu potrebne. S obzirom na dodatnu složenost, dosadašnja praksa je pokazala da treba onemogućiti WebDAV ukoliko se trenutno ne koristi.		Umeren	Potrebno je onemogućiti WebDAV ²²⁶⁴ (eng. Web-based Distributed Authoring and Versioning) za Apache. Proveriti da li je mod_dav modul isključen ili utvrditi da postoji zahtev za autentifikaciju na direktorijumima na kojima se zahteva DAV. Apache Tomcat, Tomcat, Tomcat Web Server Onemogućiti WebDAV za Apache Tomcat Isključiti WebDAV Servlet ²²⁶⁵ za sve web aplikacije koje se nalaze na web serveru. To se može uraditi tako što se ukloni definicija servlet-a za WebDAV (kategorija org.apache.catalina.servlets.WebdavServlet) i uklone sve servlet mape koje se pozivaju na WebDAV servlet.
50.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta (što zlonamerni napadač može iskoristiti pri planiranju dlajih napada). Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1²²⁶⁶ URL2²²⁶⁷ URL3²²⁶⁸	Umeren	Onemogućiti TCP odgovore na vremenski pečat na Linux-u. Podesiti vrednost net.ipv4.tcp_timestamps na 0 pokretanjem sledeće komande: sysctl -w net.ipv4.tcp_timestamps=0 Dodatno, u defaultni sysctl konfiguracioni fajl uneti sledeću vrednost, uopšteno generally sysctl.conf: net.ipv4.tcp_timestamps=0

Tabela 72. Linux OS – Pronađeni servisi na IP adresi 172.23.202.126 (2011. godina)

SERVISI	
	FTP 172.23.202.126 tcp 21 1 vsFTPD 2.0.1 ftp.banner: 220 (vsFTPD 2.0.1) HTTP 172.23.202.126 tcp 80 7 Apache 2.0.52

²²⁶⁴ WebDAV je otvoreni standard za nabavku i prenos podataka putem računarskih mreža. Pri tome korisnici vizuelno dolaze do podataka kao da su na sopstvenom računaru. Preuzeto iz : <http://sr.wikipedia.org/sr/WebDAV> , 12.09.2012.

²²⁶⁵ Servlet je objekat programskog jezika Java koji dinamički obrađuje zahteve i konstruiše odgovor na zahtev. Java servlet API omogućava Java programerima da dodaju dinamički sadržaj Web serveru korišćenjem Java platforme. Servlet najčešće generiše HTML kod, ali to može biti i XML ili nešto slično. Preuzeto iz : <http://sr.wikipedia.org/sr/Servlet>

²²⁶⁶ http://www.forensicswiki.org/wiki/TCP_timestamps

²²⁶⁷ <http://www.ietf.org/rfc/rfc1323.txt>

²²⁶⁸ <http://uptime.netcraft.com/>

	WebDAV: http.banner: Apache/2.0.52 (Red Hat) http.banner.server: Apache/2.0.52 (Red Hat) MySQL 172.23.202.126 tcp 3306 SSH 172.23.202.126 tcp 22 3 OpenSSH 3.9p1 ssh.banner: SSH-1.99-OpenSSH_3.9p1 ssh.protocol.version: 1.99 Portmapper²²⁶⁹ : 172.23.202.126 tcp 111 0 program-number: 100000 program-version: 2 STATUS: 172.23.202.126 udp 936 0 program-number: 100024 program-version: 1 172.23.202.126 tcp 939 0 program-number: 100024 program-version: 1
Spidered Web site	http://172.23.202.126:80 Common Default URLs: <i>Access Error (403)</i> cgi-bin error <i>Successful (200)</i> Icons Guessed URLs <i>Access Error (403)</i> ?P=+Adw-script+AD4-alert(42)+Adw-script+AD4-script+AD4-script+AD4-cgi-bin-error <i>Redirect (301)</i> icons small <i>Successful (200)</i> icons ?P=+Adw-script+AD4-alert(42)+Adw-script+AD4-script+AD4-README-small-README Linked URLs <i>Access Error (403)</i> <i>Successful (200)</i> icons small

²²⁶⁹ Port mapper poziva udaljene procedure je servis koji mapira RPC programe ka specifičnim portovima i daje tu informaciju klijentskim programima. S obzirom da većina RPC programa nema dobro definisan broj portova, njima se dinamički dodeljuje broj porta kada prvi put budu pokrenuti. Bilo koji klijentski program koji poželi da koristi određeni RPC program najpre stupa u kontakt sa port mapperom da bi odredio port i protokol specifikovanog RPC programa. Nakon toga, klijent koristi tu informaciju da direktno stupi u kontakt sa RPC programom. Neke implementacije port mapera dodatno omogućavaju prolazak komandi ka RPC programima kroz port mapper.

Tabela 73. Linux OS – Pronađeni servisi na IP adresi 172.23.202.225 (2011. godina)

SERVISI	FTP 172.23.202.225 tcp 21 1 vsFTPD 2.0.1 ftp.banner: 220 (vsFTPD 2.0.1) HTTP 172.23.202.225 tcp 80 7 Apache 2.0.52 WebDAV: http.banner: Apache/2.0.52 (Red Hat) http.banner.server: Apache/2.0.52 (Red Hat) MySQL 172.23.202.225 tcp 3306 SSH 172.23.202.225 tcp 22 3 OpenSSH 3.9p1 ssh.banner: SSH-1.99-OpenSSH_3.9p1 ssh.protocol.version: 1.99 Portmapper²²⁷⁰ : 172.23.202.225 tcp 111 0 program-number: 100000 program-version: 2 STATUS: 172.23.202.225 udp 936 0 program-number: 100024 program-version: 1 172.23.202.225 tcp 939 0 program-number: 100024 program-version: 1
Spidered Web site	http://172.23.202.225:80 Common Default URLs: <i>Access Error (403)</i> cgi-bin error <i>Successful (200)</i> Icons Guessed URLs <i>Access Error (403)</i> ?P=+Adw-script+AD4-alert(42)+Adw script+AD4- script+AD4- script+AD4- cgi-bin error <i>Redirect (301)</i> icons small <i>Successful (200)</i> icons ?P=+Adw-script+AD4-alert(42)+Adw script+AD4- script+AD4- README small README

²²⁷⁰ Port mapper poziva udaljene procedure je servis koji mapira RPC programe ka specifičnim portovima i daje tu informaciju klijentskim programima. S obzirom da većina RPC programa nema dobro definisan broj portova, njima se dinamički dodeljuje broj porta kada prvi put budu pokrenuti. Bilo koji klijentski program koji poželi da koristi određeni RPC program najpre stupa u kontakt sa port mapperom da bi odredio port i protokol specifikovanog RPC programa. Nakon toga, klijent koristi tu informaciju da direktno stupi u kontakt sa RPC programom. Neke implementacije port mapera dodatno omogućavaju prolazak komandi ka RPC programima kroz port mapper.

	Linked URLs Access Error (403) Successful (200) icons small

Tabela 74. Linux OS sa IP adresama 172.23.202.193, 172.23.202.194, 172.23.202.226, 172.23.202.227 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.193		OS: Red Hat Enterprise Linux 5.1 x86, redhat51entx86			47
IP adresa: 172.23.202.227		OS: Red Hat Enterprise Linux 5.1 x64, redhat51entx64			47
IP adresa: 172.23.202.194		OS: Red Hat Enterprise Linux 5.2 x86, redhat52entx86			47
IP adresa: 172.23.202.226		OS: Red Hat Enterprise Linux 5.2 x64, redhat52entx64			47
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Apache httpd mod_isapi module unload flaw (CVE-2010-0425) (apache-httpd-2_2_x-mod_isapi-moduleunload-flaw-cve-2010-0425)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 U modulu mod_isapi je pronađen propust, koji će pokušati da ukloni ISAPI dll kada naiđe na greške. To može ostaviti povratne pozive u nedefinisanoj stanju greške i kao posledica može da se javi segmentation fault. Na Windows platformama koje koriste mod_isapi, udaljeni napadač bi mogao da pošalje zlonameran zahtev da pokrene ovaj problem, a kako win32 MPM pokreće samo jedan proces, to bi kao ishod imalo odbijanje servisa i potencijalno dozvolilo da se pokrene arbitraran kôd. Zahvaljujući Brett Gervasoni-ju iz "Sense of Security" ovaj problem je prijavljen i za njega je predložena zakrpa.	BID 38494 ²²⁷¹ CERT-VN 280613 ²²⁷² CVE CVE-2010-0425 ²²⁷³ OVAL OVAL8439 ²²⁷⁴ SECUNIA 38978 ²²⁷⁵ SECUNIA 39628 ²²⁷⁶ URL1 ²²⁷⁷ XF apache-http-modisapi-ocp- unspecified(56624) ²²⁷⁸	Kritičan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz
2.	Apache httpd APR apr_palloc heap overflow (CVE-2009-2412) (http-apache-apr_palloc-heap-overflow-cve-2009-2412)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 U modulu apr_palloc() je pronađen propust u sklopu APR-a, koji može	APPLE APPLE-SA-2009-11-09 ²²⁷⁹ BID 35949 ²²⁸⁰ CVE CVE-2009-2412 ²²⁸¹ OSVDB 56765 ²²⁸² OSVDB 56766 ²²⁸³	Kritičan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.13.tar.gz

²²⁷¹ <http://www.securityfocus.com/bid/38494>

²²⁷² <http://www.kb.cert.org/vuls/id/280613>

²²⁷³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0425>

²²⁷⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8439>

²²⁷⁵ <http://secunia.com/advisories/38978/>

²²⁷⁶ <http://secunia.com/advisories/39628/>

²²⁷⁷ http://httpd.apache.org/security/vulnerabilities_22.html

²²⁷⁸ <http://xforce.iss.net/xforce/xfdb/56624>

²²⁷⁹ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>

²²⁸⁰ <http://www.securityfocus.com/bid/35949>

²²⁸¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2412>

²²⁸² <http://osvdb.org/56765>

	overflow)	prouzrokovati velika preopterećenja u programima koji pokušaju da kontrolišu apr_palloc() veličinu zadatu od strane korisnika. Sam Apache HTTP server ne dopušta prolaz ka ovoj funkciji neproverenim veličinama koje zadaje korisnik, tako da se on može pokrenuti samo preko neke druge aplikacije koja koristi apr_palloc() na ranjiv način.	OVAL OVAL8394 ²²⁸⁴ OVAL OVAL9958 ²²⁸⁵ SECUNIA 36138 ²²⁸⁶ SECUNIA 36140 ²²⁸⁷ SECUNIA 36166 ²²⁸⁸ SECUNIA 36233 ²²⁸⁹ SECUNIA 37152 ²²⁹⁰ SECUNIA 37221 ²²⁹¹ SUSE SA:2009:050 ²²⁹² URL1 2293		
3.	Apache httpd mod_proxy_ftp FTP command injection (CVE-2009-3095) (apache-httpd-2_2_xmod_proxy_ftp-ftp-command-injection-cve-2009-3095)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 U modulu mod_proxy_ftp je pronađen propust. U reverznoj proxy konfiguraciji, udaljeni napadač bi mogao da iskoristi ovaj defekt da zaobiđe uobičajenu zabranu pristupa tako što bi kreirao pažljivo izrađen HTTP Authorization heder, koji omogućava napadaču da šalje proizvoljne komande FTP serveru.	APPLE APPLE-SA-2010-03-29 ²²⁹⁴ CVE CVE-2009-3095 ²²⁹⁵ DEBIAN DSA-1934 ²²⁹⁶ OVAL OVAL8662 ²²⁹⁷ OVAL OVAL9363 ²²⁹⁸ SECUNIA 37152 ²²⁹⁹ SUSE SA:2009:050 ²³⁰⁰ URL1 2301	Kritičan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.gz
4.	Apache httpd APR-util XML DoS (CVE-2009-1955) (http-apache-apr-util-xml-dos)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Ranjivost na DOS napad otkriva je u sklopu kopije kompleta APR-util library Extensible Markup Language (XML) prevodioca (eng. parser). Udaljeni napadač bi mogao da kreira posebno izrađen XML dokument koji bi prouzrokovao ogromno zauzeće memorije kada ga procesira XML decoding engine.	APPLE APPLE-SA-2009-11-09 ²³⁰² BID 35253 ²³⁰³ CVE CVE-2009-1955 ²³⁰⁴ DEBIAN DSA-1812 ²³⁰⁵ OVAL OVAL10270 ²³⁰⁶ REDHAT RHSA-2009:1107 ²³⁰⁷ REDHAT RHSA-2009:1108 ²³⁰⁸ SECUNIA 34724 ²³⁰⁹ SECUNIA 35284 ²³¹⁰ SECUNIA 35360 ²³¹¹ SECUNIA 35395 ²³¹²	Kritičan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

²²⁸³ <http://osvdb.org/56766>²²⁸⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8394>²²⁸⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9958>²²⁸⁶ <http://secunia.com/advisories/36138/>²²⁸⁷ <http://secunia.com/advisories/36140/>²²⁸⁸ <http://secunia.com/advisories/36166/>²²⁸⁹ <http://secunia.com/advisories/36233/>²²⁹⁰ <http://secunia.com/advisories/37152/>²²⁹¹ <http://secunia.com/advisories/37221/>²²⁹² <https://www.suse.com/support/security/advisories/>²²⁹³ http://httpd.apache.org/security/vulnerabilities_22.html²²⁹⁴ <http://lists.apple.com/archives/security-announce/2010/Mar/msg00001.html>²²⁹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3095>²²⁹⁶ <http://www.debian.org/security/DSA-/DSA-1934>²²⁹⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8662>²²⁹⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9363>²²⁹⁹ <http://secunia.com/advisories/37152/>²³⁰⁰ <https://www.suse.com/support/security/advisories/>²³⁰¹ http://httpd.apache.org/security/vulnerabilities_22.html²³⁰² <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>²³⁰³ <http://www.securityfocus.com/bid/35253>²³⁰⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1955>²³⁰⁵ <http://lists.debian.org/debian-security-announce/2009/msg00124.html>²³⁰⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10270>²³⁰⁷ <http://rhn.redhat.com/errata/RHSA-2009-1107.html>²³⁰⁸ <http://rhn.redhat.com/errata/RHSA-2009-1108.html>²³⁰⁹ <http://secunia.com/advisories/34724/>²³¹⁰ <http://secunia.com/advisories/35284/>²³¹¹ <http://secunia.com/advisories/35360/>²³¹² <http://secunia.com/advisories/35395/>

			SECUNIA 35444 ²³¹³ SECUNIA 35487 ²³¹⁴ SECUNIA 35565 ²³¹⁵ SECUNIA 35710 ²³¹⁶ SECUNIA 35797 ²³¹⁷ SECUNIA 35843 ²³¹⁸ SECUNIA 36473 ²³¹⁹ SECUNIA 37221 ²³²⁰ URL1 ²³²¹		
5.	OpenSSH X11 Cookie Local Authentication Bypass Vulnerability (openssh-x11-cookie-auth-bypass)	172.23.202.193:22 172.23.202.194:22 172.23.202.226:22 172.23.202.227:22 Pre verzije 4.7, OpenSSH nije adekvatno radio kada nepoverljivi kolačić (cookie) nije mogao biti kreiran. Umesto njega, koristi se poverljivi X11 kolačić. To omogućava napadačima da naruše ciljanu polisu i dobiju privilegije korisnika, a kao posledica servis tretira X-klijenta kao poverljivog.	CVE CVE-2007-4752 ²³²² BID 25628 ²³²³ XF openssh-x11cookie-privilege-escalation(36637) ²³²⁴	Kritičan	Uraditi download a zatim instalirati: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-4.7p1.tar.gz Verzija 4.7 OpenSSH-a je puštena u promet 4. septembra 2007.
6.	Apache httpd mod_deflate DoS (CVE-2009-1891) (apache-httpd-cve-2009-1891)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Ranjivost na DOS napad otkrivena je u modulu mod_deflate. Ovaj modul nastavlja da kompresuje velike fajlove sve dok se kompresija ne završi, čak i kada je mrežna konekcija koja je zahtevala taj sadržaj prekinuta pre nego što je kompresija završena. To dovodi do toga da mod_deflate zauzima veliku količinu CPU-a ukoliko je mod_deflate bio onemogućen za velike fajlove.	APPLE APPLE-SA-2009-11-09 ²³²⁵ CVE CVE-2009-1891 ²³²⁶ DEBIAN DSA-1834 ²³²⁷ OSVDB 55782 ²³²⁸ OVAL OVAL8632 ²³²⁹ OVAL OVAL9248 ²³³⁰ REDHAT RHSA-2009:1148 ²³³¹ REDHAT RHSA-2009:1156 ²³³² SECUNIA 35721 ²³³³ SECUNIA 35781 ²³³⁴ SECUNIA 35793 ²³³⁵ SECUNIA 35865 ²³³⁶ SECUNIA 37152 ²³³⁷ SECUNIA 37221 ²³³⁸ SUSE SUSE-SA:2009:050 ²³³⁹	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz

²³¹³ <http://secunia.com/advisories/35444/>
²³¹⁴ <http://secunia.com/advisories/35487/>
²³¹⁵ <http://secunia.com/advisories/35565/>
²³¹⁶ <http://secunia.com/advisories/35710/>
²³¹⁷ <http://secunia.com/advisories/35797/>
²³¹⁸ <http://secunia.com/advisories/35843/>
²³¹⁹ <http://secunia.com/advisories/36473/>
²³²⁰ <http://secunia.com/advisories/37221/>
²³²¹ http://httpd.apache.org/security/vulnerabilities_22.html
²³²² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-4752>
²³²³ <http://www.securityfocus.com/bid/25628>
²³²⁴ <http://xforce.iss.net/xforce/xfdb/36637>
²³²⁵ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>
²³²⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1891>
²³²⁷ <http://www.debian.org/security/DSA-/DSA-1834> pristupljeno 18.12.2011
²³²⁸ <http://osvdb.org/55782>
²³²⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8632>
²³³⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9248>
²³³¹ <http://rhn.redhat.com/errata/RHSA-2009-1148.html>
²³³² <http://rhn.redhat.com/errata/RHSA-2009-1156.html>
²³³³ <http://secunia.com/advisories/35721/>
²³³⁴ <http://secunia.com/advisories/35781/>
²³³⁵ <http://secunia.com/advisories/35793/>
²³³⁶ <http://secunia.com/advisories/35865/>
²³³⁷ <http://secunia.com/advisories/37152/>
²³³⁸ <http://secunia.com/advisories/37221/>
²³³⁹ <https://www.suse.com/support/security/advisories/>

			URL ²³⁴⁰		
7.	Apache httpd mod_proxy reverse proxy DoS (CVE-2009-1890) (http-apache-mod_proxy-reverse-proxy-dos)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja prisustva mod_proxy modula. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy. Zlonamerni napadač bi mogao da iskoristi ovaj propust na takav način da primora proxy proces da zauzme veliku količinu CPU vremena.	APPLE APPLE-SA-2009-11-09 ²³⁴¹ CVE CVE-2009-1890 ²³⁴² DEBIAN DSA-1834 ²³⁴³ OSVDB 55553 ²³⁴⁴ OVAL OVAL8616 ²³⁴⁵ OVAL OVAL9403 ²³⁴⁶ REDHAT RHSA-2009:1148 ²³⁴⁷ REDHAT RHSA-2009:1156 ²³⁴⁸ SECUNIA 35691 ²³⁴⁹ SECUNIA 35721 ²³⁵⁰ SECUNIA 35793 ²³⁵¹ SECUNIA 35865 ²³⁵² SECUNIA 37152 ²³⁵³ SECUNIA 37221 ²³⁵⁴ SUSE SUSE-SA:2009:050 ²³⁵⁵ URL ²³⁵⁶	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz
8.	Apache httpd APR-util off-by-one overflow (CVE-2009-1956) (http-apache-apr-util-off-by-one-overflow)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Propust prepunjavanja bafera "off-by-one" je otkriven u načinu na koji APR-util library komplet procesira promenljivu listu argumenata. Napadač bi mogao da kreira posebno izrađen string input za već formatiranu output rutu konverzije, koja bi, na velikim platformama, potencijalno mogla da dovede do otkrivanja povreljivih informacija ili do odbijanja servisa.	APPLE APPLE-SA-2009-11-09 ²³⁵⁷ BID 35251 ²³⁵⁸ CVE CVE-2009-1956 ²³⁵⁹ OVAL OVAL11567 ²³⁶⁰ REDHAT RHSA-2009:1107 ²³⁶¹ REDHAT RHSA-2009:1108 ²³⁶² SECUNIA 34724 ²³⁶³ SECUNIA 35284 ²³⁶⁴ SECUNIA 35395 ²³⁶⁵ SECUNIA 35487 ²³⁶⁶ SECUNIA 35565 ²³⁶⁷ SECUNIA 35710 ²³⁶⁸ SECUNIA 35797 ²³⁶⁹ SECUNIA 35843 ²³⁷⁰	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

²³⁴⁰ http://httpd.apache.org/security/vulnerabilities_20.html²³⁴¹ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>²³⁴² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1890>²³⁴³ <http://www.debian.org/security/2009/dsa-1834>²³⁴⁴ <http://osvdb.org/55553>²³⁴⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8616>²³⁴⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9403>²³⁴⁷ <http://rhn.redhat.com/errata/RHSA-2009-1148.html>²³⁴⁸ <http://rhn.redhat.com/errata/RHSA-2009-1156.html>²³⁴⁹ <http://secunia.com/advisories/35691/>²³⁵⁰ <http://secunia.com/advisories/35721/>²³⁵¹ <http://secunia.com/advisories/35793/>²³⁵² <http://secunia.com/advisories/35865/>²³⁵³ <http://secunia.com/advisories/37152/>²³⁵⁴ <http://secunia.com/advisories/37221/>²³⁵⁵ <https://www.suse.com/support/security/advisories/>²³⁵⁶ http://httpd.apache.org/security/vulnerabilities_22.html²³⁵⁷ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>²³⁵⁸ <http://www.securityfocus.com/bid/35251>²³⁵⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1956>²³⁶⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11567>²³⁶¹ <http://rhn.redhat.com/errata/RHSA-2009-1107.html>²³⁶² <http://rhn.redhat.com/errata/RHSA-2009-1108.html>²³⁶³ <http://secunia.com/advisories/34724/>²³⁶⁴ <http://secunia.com/advisories/35284/>²³⁶⁵ <http://secunia.com/advisories/35395/>²³⁶⁶ <http://secunia.com/advisories/35487/>²³⁶⁷ <http://secunia.com/advisories/35565/>²³⁶⁸ <http://secunia.com/advisories/35710/>²³⁶⁹ <http://secunia.com/advisories/35797/>

			SECUNIA 37221 ²³⁷¹ URL1 ²³⁷²		
9.	OpenSSH X11 Forwarding Information Disclosure Vulnerability (ssh-openssh-x11-fowarding-info-disclosure)	172.23.202.193:22 172.23.202.194:22 172.23.202.226:22 172.23.202.227:22 Određene verzije OpenSSH-a ne povezuju ispravno TCP portove na lokalnom IPv6 interfejsu ako se koriste zahtevani IPv4 portovi. Ovo bi loklanom napadaču moglo da omogući da preuzme prosledenu X11 sesiju putem otvaranja TCP port-a 6010 (IPv4).	BID 28444 ²³⁷³ CVE CVE-2008-1483 ²³⁷⁴ SECUNIA 29522 ²³⁷⁵ URL1 ²³⁷⁶	Ozbiljan	Nadogradite na najnoviju verziju OpenSSH-a. Najnovija verzija OpenSSH-a je 5.2 (OpenBSD izvor) i 5.2p1 (prenosivi izvor).
10.	Apache httpd expat DoS (CVE-2009-3560) (apache-httpd-2_2_x-cve-2009-3560)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je rannjiv samo ukoliko je zlonamerni napadač u mogućnosti da dovede do toga da Apache parsira nepoverljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument (na primer kroz mod dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	BID 37203 ²³⁷⁷ CVE CVE-2009-3560 ²³⁷⁸ DEBIAN DSA-1953 ²³⁷⁹ OVAL OVAL10613 ²³⁸⁰ OVAL OVAL6883 ²³⁸¹ SECUNIA 37537 ²³⁸² SECUNIA 38231 ²³⁸³ SECUNIA 38794 ²³⁸⁴ SECUNIA 38832 ²³⁸⁵ SECUNIA 38834 ²³⁸⁶ SECUNIA 39478 ²³⁸⁷ SECUNIA 41701 ²³⁸⁸ SECUNIA 43300 ²³⁸⁹ URL1 ²³⁹⁰	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
11.	Apache httpd expat DoS (CVE-2009-3720) (apache-httpd-2_2_x-cve-2009-3720)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako je napadač u	CVE CVE-2009-3720 ²³⁹¹ OVAL OVAL11019 ²³⁹² OVAL OVAL7112 ²³⁹³ REDHAT RHSA-2010:0002 ²³⁹⁴ SECUNIA 37324 ²³⁹⁵	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz

²³⁷⁰ <http://secunia.com/advisories/35843/>²³⁷¹ <http://secunia.com/advisories/37221/>²³⁷² http://httpd.apache.org/security/vulnerabilities_22.html²³⁷³ <http://www.securityfocus.com/bid/28444>²³⁷⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-1483>²³⁷⁵ <http://secunia.com/advisories/29522/>²³⁷⁶ <http://www.openssh.org/txt/release-5.0>²³⁷⁷ <http://www.securityfocus.com/bid/37203>²³⁷⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3560>²³⁷⁹ <http://www.debian.org/security/2009/dsa-1953>²³⁸⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10613>²³⁸¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6883>²³⁸² <http://secunia.com/advisories/37537/>²³⁸³ <http://secunia.com/advisories/38231/>²³⁸⁴ <http://secunia.com/advisories/38794/>²³⁸⁵ <http://secunia.com/advisories/38832/>²³⁸⁶ <http://secunia.com/advisories/38834/>²³⁸⁷ <http://secunia.com/advisories/39478/>²³⁸⁸ <http://secunia.com/advisories/41701/>²³⁸⁹ <http://secunia.com/advisories/43300/>²³⁹⁰ http://httpd.apache.org/security/vulnerabilities_22.html²³⁹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3720>²³⁹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11019>²³⁹³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7112>²³⁹⁴ <http://rhn.redhat.com/errata/RHSA-2010-0002.html>²³⁹⁵ <http://secunia.com/advisories/37324/>

		moгуćnosti da dovede do toga da Apache parsira nepoverljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove moгуćnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u moгуćnosti da dovede do toga da Apache parsira nepovreljiv XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	SECUNIA 37537²³⁹⁶ SECUNIA 37925²³⁹⁷ SECUNIA 38050²³⁹⁸ SECUNIA 38231²³⁹⁹ SECUNIA 38794²⁴⁰⁰ SECUNIA 38832²⁴⁰¹ SECUNIA 38834²⁴⁰² SECUNIA 39478²⁴⁰³ SECUNIA 41701²⁴⁰⁴ SECUNIA 43300²⁴⁰⁵ URL1²⁴⁰⁶		
12.	Apache httpd apr_bridage_split_line DoS (CVE-2010-1623) (apache-httpd-2_2_x-cve-2010-1623)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako Apache procesira ne-SSL zahteve. Proveriti konfiguraciju web servera radi utvrđivanja ove moгуćnosti. Propust je otkriven u funkciji apr_brigade_split_line() u sklopu kompleta APR-util library, koji se koristi za procesiranje ne-SSL zahteva. Udaljeni napadač bi mogao da šalje zahteve, pažljivo izrađujući tajming za pojedinačne bajtove, što bi polako zauzimalo memoriju i potencijalno dovelo do odbijanja servisa.	BID 43673²⁴⁰⁷ CVE CVE-2010-1623²⁴⁰⁸ REDHAT RHSA-2010:0950²⁴⁰⁹ SECUNIA 41701²⁴¹⁰ SECUNIA 42015²⁴¹¹ SECUNIA 42361²⁴¹² SECUNIA 42367²⁴¹³ SECUNIA 42403²⁴¹⁴ SECUNIA 42537²⁴¹⁵ SECUNIA 43211²⁴¹⁶ SECUNIA 43285²⁴¹⁷ URL1²⁴¹⁸	Ozbiljan	Apache >= 2.2 and < 2.3 Uradiiti download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
13.	Apache httpd mod_cache and mod_dav DoS (CVE-2010-1452) (apache-httpd-2_2_x-mod_cache-andmod_	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako web server izvršava jedan od sledećih modula:	APPLE APPLE-SA-2011-03-21²⁴¹⁹ CVE CVE-2010-1452²⁴²⁰ OVAL OVAL11683²⁴²¹ REDHAT RHSA-2010:0659²⁴²² SECUNIA 42367²⁴²³	Ozbiljan	Apache >= 2.2 and < 2.3 Uradiiti download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.16.tar.gz

²³⁹⁶ <http://secunia.com/advisories/37537/>²³⁹⁷ <http://secunia.com/advisories/37925/>²³⁹⁸ <http://secunia.com/advisories/38050/>²³⁹⁹ <http://secunia.com/advisories/38231/>²⁴⁰⁰ <http://secunia.com/advisories/38794/>²⁴⁰¹ <http://secunia.com/advisories/38832/>²⁴⁰² <http://secunia.com/advisories/38834/>²⁴⁰³ <http://secunia.com/advisories/39478/>²⁴⁰⁴ <http://secunia.com/advisories/41701/>²⁴⁰⁵ <http://secunia.com/advisories/43300/>²⁴⁰⁶ http://httpd.apache.org/security/vulnerabilities_22.html²⁴⁰⁷ <http://www.securityfocus.com/bid/43673>²⁴⁰⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1623>²⁴⁰⁹ <http://rhn.redhat.com/errata/RHSA-2010-0950.html>²⁴¹⁰ <http://secunia.com/advisories/41701/>²⁴¹¹ <http://secunia.com/advisories/42015/>²⁴¹² <http://secunia.com/advisories/42361/>²⁴¹³ <http://secunia.com/advisories/42367/>²⁴¹⁴ <http://secunia.com/advisories/42403/>²⁴¹⁵ <http://secunia.com/advisories/42537/>²⁴¹⁶ <http://secunia.com/advisories/43211/>²⁴¹⁷ <http://secunia.com/advisories/43285/>²⁴¹⁸ http://httpd.apache.org/security/vulnerabilities_22.html²⁴¹⁹ <http://lists.apple.com/archives/security-announce/2011/Mar/msg00006.html>²⁴²⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1452>²⁴²¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11683>²⁴²² <http://rhn.redhat.com/errata/RHSA-2010-0659.html>²⁴²³ <http://secunia.com/advisories/42367/>

	dav-dos-cve-2010-1452)	mod_cache, mod_dav. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u obradi zahteva od strane mod_cache i mod_dav. Zlonameran udaljeni napadač bi mogao da pošalje pažljivo izrađen zahtev i prouzrokuje da httpd child proces krahira. Ovakvo krahiranje bi se manifestovalo samo kao odbijanje servisa ako se koristi Worker MPM. Ovaj problem se dalje može ublažiti ako na mod_dav samo utiču zahtevi za koje postoji mogućnost autentifikovanja, a mod_cache je pod uticajem samo ako se koristi neuobičajena „CacheIgnoreURLSessionIdentifiers“ direktiva, uvedena u verziji 2.2.14. Ovaj problem je prijavio Mark Drayton.	URL1 ²⁴²⁴		
14.	Apache httpd mod_proxy crash (CVE-2007-3847) (apache-httpd-2_2_x-mod_proxy-crash-cve-2007-3847)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Propust je otkriven u Apache-ovom HTTP Server modulu mod_proxy. Na sajtovima na kojima je konfigurisan "reverse proxy", udaljeni napadač bi mogao da pošalje pažljivo izrađen zahtev koji bi mogao da prouzrokuje pad child procesa Apache-a koji taj zahtev obrađuje. Na sajtovima na kojima je konfigurisan "forward proxy", napadač bi mogao da prouzrokuje sličan pad ako bi korisnik bio naveden da poseti zlonameran sajt koji koristi taj proksi. Ovo bi moglo da dovede do odbijanja servisa ako se koristi threaded MPM.	APPLE APPLE-SA-2008-03-18 ²⁴²⁵ APPLE APPLE-SA-2008-05-28 ²⁴²⁶ CERT 25489 ²⁴²⁷ CERT TA08-150A ²⁴²⁸ CVE CVE-2007-3847 ²⁴²⁹ OVAL OVAL10525 ²⁴³⁰ REDHAT RHSA-2007:0746 ²⁴³¹ REDHAT RHSA-2007:0747 ²⁴³² REDHAT RHSA-2007:0911 ²⁴³³ REDHAT RHSA-2008:0005 ²⁴³⁴ SECUNIA 26636 ²⁴³⁵ SECUNIA 26722 ²⁴³⁶ SECUNIA 26790 ²⁴³⁷ SECUNIA 26842 ²⁴³⁸ SECUNIA 26952 ²⁴³⁹ SECUNIA 26993 ²⁴⁴⁰ SECUNIA 27209 ²⁴⁴¹ SECUNIA 27563 ²⁴⁴² SECUNIA 27593 ²⁴⁴³ SECUNIA 27732 ²⁴⁴⁴ SECUNIA 27882 ²⁴⁴⁵	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz

²⁴²⁴ http://httpd.apache.org/security/vulnerabilities_22.html²⁴²⁵ <http://lists.apple.com/archives/security-announce/2008/Mar/msg00000.html>²⁴²⁶ <http://lists.apple.com/archives/security-announce/2008/May/msg00001.html>²⁴²⁷ <http://www.securityfocus.com/bid/25489> pristupljeno 11.12.2011²⁴²⁸ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>²⁴²⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3847>²⁴³⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10525>²⁴³¹ <http://rhn.redhat.com/errata/RHSA-2007-0746.html>²⁴³² <http://rhn.redhat.com/errata/RHSA-2007-0747.html>²⁴³³ <http://rhn.redhat.com/errata/RHSA-2007-0911.html>²⁴³⁴ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>²⁴³⁵ <http://secunia.com/advisories/26636/>²⁴³⁶ <http://secunia.com/advisories/26722/>²⁴³⁷ <http://secunia.com/advisories/26790/>²⁴³⁸ <http://secunia.com/advisories/26842/>²⁴³⁹ <http://secunia.com/advisories/26952/>²⁴⁴⁰ <http://secunia.com/advisories/26993/>²⁴⁴¹ <http://secunia.com/advisories/27209/>²⁴⁴² <http://secunia.com/advisories/27563/>²⁴⁴³ <http://secunia.com/advisories/27593/>²⁴⁴⁴ <http://secunia.com/advisories/27732/>

			SECUNIA 27971 ²⁴⁴⁶ SECUNIA 28467 ²⁴⁴⁷ SECUNIA 28606 ²⁴⁴⁸ SECUNIA 28749 ²⁴⁴⁹ SECUNIA 28922 ²⁴⁵⁰ SECUNIA 29420 ²⁴⁵¹ SECUNIA 30430 ²⁴⁵² SUSE SA:2007:061 ²⁴⁵³ URL1 ²⁴⁵⁴		
15.	Apache httpd mod_proxy_http DoS (CVE-2008-2364) (apache-httpd-2.2.x- mod_proxy_http-dos- cve-2008- 2364)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Otkriven je propust prilikom obrade prekomernih privremenih odgovora sa glavnog servera kada se koristi mod_proxy_http. Udaljeni napadač bi mogao da izazove odbijanje servisa ili preopterećenje memorije.	BID 29653 ²⁴⁵⁵ BID 31681 ²⁴⁵⁶ CVE CVE-2008-2364 ²⁴⁵⁷ OVAL OVAL11713 ²⁴⁵⁸ OVAL OVAL6084 ²⁴⁵⁹ OVAL OVAL9577 ²⁴⁶⁰ REDHAT RHSA- 2008:0966 ²⁴⁶¹ REDHAT RHSA- 2008:0967 ²⁴⁶² SECUNIA 30621 ²⁴⁶³ SECUNIA 31026 ²⁴⁶⁴ SECUNIA 31404 ²⁴⁶⁵ SECUNIA 31416 ²⁴⁶⁶ SECUNIA 31651 ²⁴⁶⁷ SECUNIA 31904 ²⁴⁶⁸ SECUNIA 32222 ²⁴⁶⁹ SECUNIA 32685 ²⁴⁷⁰ SECUNIA 32838 ²⁴⁷¹ SECUNIA 33156 ²⁴⁷² SECUNIA 33797 ²⁴⁷³ SECUNIA 34219 ²⁴⁷⁴ SECUNIA 34259 ²⁴⁷⁵ SECUNIA 34418 ²⁴⁷⁶ XF apache-modproxy- module-dos(42987) ²⁴⁷⁷ URL1 ²⁴⁷⁸	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.9.tar.gz

²⁴⁴⁵ <http://secunia.com/advisories/27882/>²⁴⁴⁶ <http://secunia.com/advisories/27971/>²⁴⁴⁷ <http://secunia.com/advisories/28467/>²⁴⁴⁸ <http://secunia.com/advisories/28606/>²⁴⁴⁹ <http://secunia.com/advisories/28749/>²⁴⁵⁰ <http://secunia.com/advisories/28922/>²⁴⁵¹ <http://secunia.com/advisories/29420/>²⁴⁵² <http://secunia.com/advisories/30430/>²⁴⁵³ <https://www.suse.com/support/security/advisories/>²⁴⁵⁴ http://httpd.apache.org/security/vulnerabilities_22.html²⁴⁵⁵ <http://www.securityfocus.com/bid/29653>²⁴⁵⁶ <http://www.securityfocus.com/bid/31681>²⁴⁵⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-2364>²⁴⁵⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11713>²⁴⁵⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6084>²⁴⁶⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9577>²⁴⁶¹ <http://rhn.redhat.com/errata/RHSA-2008-0966.html>²⁴⁶² <http://rhn.redhat.com/errata/RHSA-2008-0967.html>²⁴⁶³ <http://secunia.com/advisories/30621/>²⁴⁶⁴ <http://secunia.com/advisories/31026/>²⁴⁶⁵ <http://secunia.com/advisories/31404/>²⁴⁶⁶ <http://secunia.com/advisories/31416/>²⁴⁶⁷ <http://secunia.com/advisories/31651/>²⁴⁶⁸ <http://secunia.com/advisories/31904/>²⁴⁶⁹ <http://secunia.com/advisories/32222/>²⁴⁷⁰ <http://secunia.com/advisories/32685/>²⁴⁷¹ <http://secunia.com/advisories/32838/>²⁴⁷² <http://secunia.com/advisories/33156/>²⁴⁷³ <http://secunia.com/advisories/33797/>²⁴⁷⁴ <http://secunia.com/advisories/34219/>²⁴⁷⁵ <http://secunia.com/advisories/34259/>²⁴⁷⁶ <http://secunia.com/advisories/34418/>²⁴⁷⁷ <http://xforce.iss.net/xforce/xfdb/42987>

16.	Apache httpd Signals to arbitrary processes (CVE-2007-3304) (apache-httpd-2_2_x-signals-to-arbitraryprocesses-cve-2007-3304)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Pre nego što je poslao signale, Apache HTTP server nije overio da li proces potiče od Apache-ovog child-a. Lokalni napadač koji ima mogućnost da pokreće skripta na HTTP serveru, mogao bi da manipuliše semaforom za signale i da prouzrokuje okončanje proizvoljnog procesa, što bi moglo da dovede do odbijanja servisa.	BID 24215 ²⁴⁷⁹ CVE CVE-2007-3304 ²⁴⁸⁰ OVAL OVAL11589 ²⁴⁸¹ REDHAT RHSA-2007:0532 ²⁴⁸² REDHAT RHSA-2007:0556 ²⁴⁸³ REDHAT RHSA-2007:0557 ²⁴⁸⁴ REDHAT RHSA-2007:0662 ²⁴⁸⁵ REDHAT RHSA-2008:0261 ²⁴⁸⁶ SECUNIA 25827 ²⁴⁸⁷ SECUNIA 25830 ²⁴⁸⁸ SECUNIA 25920 ²⁴⁸⁹ SECUNIA 26211 ²⁴⁹⁰ SECUNIA 26273 ²⁴⁹¹ SECUNIA 26443 ²⁴⁹² SECUNIA 26508 ²⁴⁹³ SECUNIA 26611 ²⁴⁹⁴ SECUNIA 26759 ²⁴⁹⁵ SECUNIA 26790 ²⁴⁹⁶ SECUNIA 26822 ²⁴⁹⁷ SECUNIA 26842 ²⁴⁹⁸ SECUNIA 26993 ²⁴⁹⁹ SECUNIA 27121 ²⁵⁰⁰ SECUNIA 27209 ²⁵⁰¹ SECUNIA 27563 ²⁵⁰² SECUNIA 27732 ²⁵⁰³ SECUNIA 28212 ²⁵⁰⁴ SECUNIA 28224 ²⁵⁰⁵ SECUNIA 28606 ²⁵⁰⁶ SGI 20070701-01-P ²⁵⁰⁷ SUSE SUSE-SA:2007:061 ²⁵⁰⁸ XF apache-child-process-dos(35095) ²⁵⁰⁹	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz

²⁴⁷⁸ http://httpd.apache.org/security/vulnerabilities_20.html²⁴⁷⁹ <http://www.securityfocus.com/bid/24215>²⁴⁸⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3304>²⁴⁸¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11589>²⁴⁸² <http://rhn.redhat.com/errata/RHSA-2007-0532.html>²⁴⁸³ <http://rhn.redhat.com/errata/RHSA-2007-0556.html>²⁴⁸⁴ <http://rhn.redhat.com/errata/RHSA-2007-0557.html>²⁴⁸⁵ <http://rhn.redhat.com/errata/RHSA-2007-0662.html>²⁴⁸⁶ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>²⁴⁸⁷ <http://secunia.com/advisories/25827/>²⁴⁸⁸ <http://secunia.com/advisories/25830/>²⁴⁸⁹ <http://secunia.com/advisories/25920/>²⁴⁹⁰ <http://secunia.com/advisories/26211/>²⁴⁹¹ <http://secunia.com/advisories/26273/>²⁴⁹² <http://secunia.com/advisories/26443/>²⁴⁹³ <http://secunia.com/advisories/26508/>²⁴⁹⁴ <http://secunia.com/advisories/26611/>²⁴⁹⁵ <http://secunia.com/advisories/26759/>²⁴⁹⁶ <http://secunia.com/advisories/26790/>²⁴⁹⁷ <http://secunia.com/advisories/26822/>²⁴⁹⁸ <http://secunia.com/advisories/26842/>²⁴⁹⁹ <http://secunia.com/advisories/26993/>²⁵⁰⁰ <http://secunia.com/advisories/27121/>²⁵⁰¹ <http://secunia.com/advisories/27209/>²⁵⁰² <http://secunia.com/advisories/27563/>²⁵⁰³ <http://secunia.com/advisories/27732/>²⁵⁰⁴ <http://secunia.com/advisories/28212/>²⁵⁰⁵ <http://secunia.com/advisories/28224/>²⁵⁰⁶ <http://secunia.com/advisories/28606/>²⁵⁰⁷ <ftp://patches.sgi.com/support/free/security/advisories/20070701-01-P> pristupljeno 18.12.2011²⁵⁰⁸ <https://www.suse.com/support/security/advisories/>²⁵⁰⁹ <http://xforce.iss.net/xforce/xfdb/35095>

			URL ²⁵¹⁰		
17.	FTP access with ftp account (ftp-generic-0001)	172.23.202.193:21 172.23.202.194:21 172.23.202.226:21 172.23.202.227:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisnikovim ID-jem (identifikacijom) "ftp" i šifrom "ftp". Dosadašnja praksa je pokazala da je najbolje ukloniti difoltnu naloge, ukoliko je to moguće. Za naloge koje sistem zahteva treba izmeniti difoltnu šifru.	CVE CVE-1999-0497 ²⁵¹¹	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko nije kritičan za dalje funkcionisanje sistema. U suprotnom, treba promeniti šifru u nedifoltnu vrednost.
18.	FTP access with anonymous account (ftp-generic-0002)	172.23.202.193:21 172.23.202.194:21 172.23.202.226:21 172.23.202.227:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisnikovim ID-jem (identifikacijom) "anonymous" i šifrom "ftp@". Dosadašnja praksa je pokazala da je najbolje ukloniti difoltnu naloge, ukoliko je to moguće. Za naloge koje sistem zahteva treba izmeniti difoltnu šifru.	CVE CVE-1999-0497 ²⁵¹²	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko nije kritičan za dalje funkcionisanje sistema. U suprotnom, treba promeniti šifru u nedifoltnu vrednost.
19.	FTP server does not support AUTH command (ftp-generic-0007)	172.23.202.193:21 172.23.202.194:21 172.23.202.226:21 172.23.202.227:21 FTP klijenti po difoltu šalju FTP server-u poverljive podatke (korisnički ID i šifru) u vidu čitkog teksta. Ova okolnost dozvoljava zlonamernim korisnicima da presreću poverljive podatke ukoliko prisluškuju vezu. Noviji FTP serveri podržavaju AUTH komandu, koja omogućava dodatne opcije autentifikacije, kao što su TLS, Kerberos, GSSAPI itd. Ona se može koristiti za sprečavanje prisluškivanja na FTP vezama.		Ozbiljan	Ažurirati/preći na FTP server koji podržava AUTH komandu.
20.	Apache httpd AllowOverride Options handling bypass (CVE-2009-1195) (http-apache-allowoverrideoptions-handling-bypass)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako web server izvršava direktivu AllowOverride sa određenim opcijama koje se koriste. Proveriti konfiguraciju web servera	APPLE APPLE-SA-2009-11-09 ²⁵¹³ BID 35115 ²⁵¹⁴ CVE CVE-2009-1195 ²⁵¹⁵ DEBIAN DSA-1816 ²⁵¹⁶ OSVDB 54733 ²⁵¹⁷ OVAL OVAL11094 ²⁵¹⁸ OVAL OVAL8704 ²⁵¹⁹ REDHAT RHSA-	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

²⁵¹⁰ http://httpd.apache.org/security/vulnerabilities_20.html²⁵¹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>²⁵¹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>²⁵¹³ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>²⁵¹⁴ <http://www.securityfocus.com/bid/35115>²⁵¹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1195>²⁵¹⁶ <http://www.debian.org/security/2009/dsa-1816>²⁵¹⁷ <http://osvdb.org/54733>²⁵¹⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11094>²⁵¹⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8704>

		radi utvrđivanja ove mogućnosti. Propust je otkriven u obradi direktiva „Options“ i „AllowOverride“. U konfiguracijama koje koriste direktivu „AllowOverride“ sa određenim „Options“ argumentima, lokalni korisnici mogu da izvršavaju komande iz web-serverskih skripti.	2009:1075 ²⁵²⁰ REDHAT RHSA-2009:1156 ²⁵²¹ SECUNIA 35261 ²⁵²² SECUNIA 35264 ²⁵²³ SECUNIA 35395 ²⁵²⁴ SECUNIA 35453 ²⁵²⁵ SECUNIA 35721 ²⁵²⁶ SECUNIA 37152 ²⁵²⁷ SUSE SA:2009:050 ²⁵²⁸ XF apache-allowoverrides-security-bypass(50808) ²⁵²⁹ URL1 ²⁵³⁰		
21.	Apache HTTP Method 413 Error Response Cross-Site Scripting Vulnerability (http-apache-malformed-413-response-xss)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Određene verzije Apache web servera ne saniraju na odgovarajući način metodu zahteva na 413 stranici sa pogrešnim odgovorom koja je uzvraćena kad je zlonameran zahtev sa velikom vrednošću za dužinu sadržaja (Content-Length) poslat serveru. Nedostatak izlaza uzrokuje ranjivost na XSS napade na serveru. Ova ranjivost se može iskoristiti samo ako napadnuti HTTP klijent bude primoran da pošalje HTTP zahtev sa nevalidnim imenom metoda. Pokretanje ranjivog HTTP servisa: Apache 2.2.3. Primer : <a href="http://172.23.202.193/3: <title>413 Request Entity Too Large</title>4: </head><body>5: <h1>Request Entity Too Large</h1>6: The requested resource

">http://172.23.202.193/3: <title>413 Request Entity Too Large</title> 4: </head><body> 5: <h1>Request Entity Too Large</h1> 6: The requested resource

	APPLE APPLE-SA-2008-03-18 ²⁵³¹ BID 26663 ²⁵³² CVE CVE-2007-6203 ²⁵³³ SECUNIA 27906 ²⁵³⁴ SECUNIA 28196 ²⁵³⁵ SECUNIA 29348 ²⁵³⁶ SECUNIA 29420 ²⁵³⁷ SECUNIA 29640 ²⁵³⁸ SECUNIA 30356 ²⁵³⁹ SECUNIA 30732 ²⁵⁴⁰ SECUNIA 33105 ²⁵⁴¹ SECUNIA 34219 ²⁵⁴² XF apache-413error-xss(38800) ²⁵⁴³ URL1 ²⁵⁴⁴ URL2 ²⁵⁴⁵ URL3 ²⁵⁴⁶ URL4 ²⁵⁴⁷	Ozbiljan	Apache >= 2.0 and < 2.1 Ažurirati na Apache verziju 2.0.62 Apache 2.0.62 nikada nije pušten u opticaj usled problema u kvalitetu koji su otkriveni u tarbolima pre puštanja u promet. Umesto toga, ažurirati na Apache verziju 2.0.63. Apache >= 2.1 and < 2.3 Ažurirajte na Apache verziju 2.2.7 Apache 2.2.7 nikada nije pušten u opticaj usled problema u kvalitetu koji su otkriveni u tarbolima pre puštanja u promet. Umesto toga, ažurirati na Apache 2.2.8.

²⁵²⁰ <http://rhn.redhat.com/errata/RHSA-2009-1075.html>²⁵²¹ <http://rhn.redhat.com/errata/RHSA-2009-1156.html>²⁵²² <http://secunia.com/advisories/35261/>²⁵²³ <http://secunia.com/advisories/35264/>²⁵²⁴ <http://secunia.com/advisories/35395/>²⁵²⁵ <http://secunia.com/advisories/35453/>²⁵²⁶ <http://secunia.com/advisories/35721/>²⁵²⁷ <http://secunia.com/advisories/37152/>²⁵²⁸ <https://www.suse.com/support/security/advisories/>²⁵²⁹ <http://xforce.iss.net/xforce/xfdb/50808>²⁵³⁰ http://httpd.apache.org/security/vulnerabilities_22.html²⁵³¹ <http://lists.apple.com/archives/security-announce/2008/Mar/msg00000.html>²⁵³² <http://www.securityfocus.com/bid/26663>²⁵³³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6203>²⁵³⁴ <http://secunia.com/advisories/27906/>²⁵³⁵ <http://secunia.com/advisories/28196/>²⁵³⁶ <http://secunia.com/advisories/29348/>²⁵³⁷ <http://secunia.com/advisories/29420/>²⁵³⁸ <http://secunia.com/advisories/29640/>²⁵³⁹ <http://secunia.com/advisories/30356/>²⁵⁴⁰ <http://secunia.com/advisories/30732/>²⁵⁴¹ <http://secunia.com/advisories/33105/>²⁵⁴² <http://secunia.com/advisories/34219/>²⁵⁴³ <http://xforce.iss.net/xforce/xfdb/38800>²⁵⁴⁴ http://procheckup.com/Vulnerability_PR07-37.php²⁵⁴⁵ <http://svn.apache.org/viewvc?revision=600645&view=revision>²⁵⁴⁶ <http://svn.apache.org/viewvc?revision=602473&view=revision>²⁵⁴⁷ <http://svn.apache.org/viewvc?revision=604425&view=revision>

		7: does not allow request data with <SCRIPT>NXSSTEST</SCRIPT> requests			
22.	Apache httpd mod_cache proxy DoS (CVE-2007-1863) (http- apache-mod_cache- proxy-dos)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Propust je otkriven u modulu mod_cache. Na sajtozima na kojima je omogućeno keširanje, udaljeni napadač bi mogao da pošalje pažljivo izrađen zahtev koji bi doveo do toga da child proces Apache-a koji to obrađuje krahira. To može dovesti samo do odbijanja servisa ako se koristi threaded MPM.	BID 24649 ²⁵⁴⁸ CERT TA08-150A ²⁵⁴⁹ CVE CVE-2007-1863 ²⁵⁵⁰ OVAL OVAL9824 ²⁵⁵¹ REDHAT RHSA- 2007:0533 ²⁵⁵² REDHAT RHSA- 2007:0534 ²⁵⁵³ REDHAT RHSA- 2007:0556 ²⁵⁵⁴ REDHAT RHSA- 2007:0557 ²⁵⁵⁵ SECUNIA 25830 ²⁵⁵⁶ SECUNIA 25873 ²⁵⁵⁷ SECUNIA 25920 ²⁵⁵⁸ SECUNIA 26273 ²⁵⁵⁹ SECUNIA 26443 ²⁵⁶⁰ SECUNIA 26508 ²⁵⁶¹ SECUNIA 26822 ²⁵⁶² SECUNIA 26842 ²⁵⁶³ SECUNIA 26993 ²⁵⁶⁴ SECUNIA 27037 ²⁵⁶⁵ SECUNIA 27563 ²⁵⁶⁶ SECUNIA 27732 ²⁵⁶⁷ SECUNIA 28606 ²⁵⁶⁸ SECUNIA 30430 ²⁵⁶⁹ SUSE SA:2007:061 ²⁵⁷⁰ URL1 ²⁵⁷¹	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dis t/httpd/httpd-2.2.6.tar.gz
23.	Apache httpd mod_proxy_ajp DoS (CVE-2010-0408) (http- apache-mod_proxy_ajp- dos)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ajp. Proveriti konfiguraciju web servera	BID 38491 ²⁵⁷² CVE CVE-2010-0408 ²⁵⁷³ DEBIAN DSA-2035 ²⁵⁷⁴ OVAL OVAL8619 ²⁵⁷⁵ OVAL OVAL9935 ²⁵⁷⁶ REDHAT RHSA- 2010:0168 ²⁵⁷⁷ SECUNIA 39100 ²⁵⁷⁸	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dis t/httpd/httpd-2.2.15.tar.gz

²⁵⁴⁸ <http://www.securityfocus.com/bid/24649>²⁵⁴⁹ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>²⁵⁵⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-1863>²⁵⁵¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9824>²⁵⁵² <http://rhn.redhat.com/errata/RHSA-2007-0533.html>²⁵⁵³ <http://rhn.redhat.com/errata/RHSA-2007-0534.html>²⁵⁵⁴ <http://rhn.redhat.com/errata/RHSA-2007-0556.html>²⁵⁵⁵ <http://rhn.redhat.com/errata/RHSA-2007-0557.html>²⁵⁵⁶ <http://secunia.com/advisories/25830/>²⁵⁵⁷ <http://secunia.com/advisories/25873/>²⁵⁵⁸ <http://secunia.com/advisories/25920/>²⁵⁵⁹ <http://secunia.com/advisories/26273/>²⁵⁶⁰ <http://secunia.com/advisories/26443/>²⁵⁶¹ <http://secunia.com/advisories/26508/>²⁵⁶² <http://secunia.com/advisories/26822/>²⁵⁶³ <http://secunia.com/advisories/26842/>²⁵⁶⁴ <http://secunia.com/advisories/26993/>²⁵⁶⁵ <http://secunia.com/advisories/27037/>²⁵⁶⁶ <http://secunia.com/advisories/27563/>²⁵⁶⁷ <http://secunia.com/advisories/27732/>²⁵⁶⁸ <http://secunia.com/advisories/28606/>²⁵⁶⁹ <http://secunia.com/advisories/30430/>²⁵⁷⁰ <https://www.suse.com/support/security/advisories/>²⁵⁷¹ http://httpd.apache.org/security/vulnerabilities_20.html²⁵⁷² <http://www.securityfocus.com/bid/38491>²⁵⁷³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0408>²⁵⁷⁴ <http://www.debian.org/security/2010/dsa-2035>²⁵⁷⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8619>²⁵⁷⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9935>²⁵⁷⁷ <http://rhn.redhat.com/errata/RHSA-2010-0168.html>

		radi utvrđivanja ove mogućnosti. Mod_proxy_ajp će vratiti pogrešan kôd statusa ako naide na grešku, prouzrokujući da backend server bude stavljen u status greške dok ne istekne vreme za ponovni pokušaj. Udaljeni napadač bi mogao da pošalje zlonameran zahtev da bi pokrenuo ovaj problem, što bi dovelo do odbijanja servisa. Zahvaljujući Niku Toivola iz Sulake Corporation, ovaj problem je prijavljen uz predloženu adekvatnu meru zaštite u vidu zakrpe.	SECUNIA 39501 ²⁵⁷⁹ SECUNIA 39628 ²⁵⁸⁰ SECUNIA 39632 ²⁵⁸¹ SECUNIA 39656 ²⁵⁸² SECUNIA 40096 ²⁵⁸³ URL1 ²⁵⁸⁴		
24.	Apache httpd mod_proxy_ftp DoS (CVE-2009-3094) (http://apache-mod_proxy_ftp-dos)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ftp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust NULL pointer dereference (pointer sa NULL vrednošću upotrebljen kao da ukazuje na validnu memorijsku oblast) otkriven je u modulu mod_proxy_ftp. Zlonamerni FTP server, kojem su zahtevi proksirani, mogao bi da iskoristi ovaj propust u smislu obaranja http child procesa uz pomoć izmenjenog odgovora EPSV ili PASV komandi, što bi dovelo do delimičnog odbijanja servisa.	CVE CVE-2009-3094 ²⁵⁸⁵ DEBIAN DSA-1934 ²⁵⁸⁶ OVAL OVAL10981 ²⁵⁸⁷ OVAL OVAL8087 ²⁵⁸⁸ SECUNIA 36549 ²⁵⁸⁹ SECUNIA 37152 ²⁵⁹⁰ SUSE SUSE-SA:2009:050 ²⁵⁹¹ URL1 ²⁵⁹²	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.gz
25.	Apache httpd Solaris pollset DoS (CVE-2009-2699) (http://apache-solaris-pollset-dos)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Otkriven je Faulty error prouzrokovan bagom u APR-u. Ova ranjivost detektovanja je na Solaris serverima. Udaljeni napadač bi mogao da pokrene ovaj problem na Solaris serverima koji koriste prefork ili event MPM. ²⁵⁹³	BID 36596 ²⁵⁹⁴ CVE CVE-2009-2699 ²⁵⁹⁵ XF apache-solaris-pollset-dos(53666) ²⁵⁹⁶ URL1 ²⁵⁹⁷	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.gz

²⁵⁷⁸ <http://secunia.com/advisories/39100/>²⁵⁷⁹ <http://secunia.com/advisories/39501/>²⁵⁸⁰ <http://secunia.com/advisories/39628/>²⁵⁸¹ <http://secunia.com/advisories/39632/>²⁵⁸² <http://secunia.com/advisories/39656/>²⁵⁸³ <http://secunia.com/advisories/40096/>²⁵⁸⁴ http://httpd.apache.org/security/vulnerabilities_22.html²⁵⁸⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3094>²⁵⁸⁶ <http://www.debian.org/security/2009/dsa-1934>²⁵⁸⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10981>²⁵⁸⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8087>²⁵⁸⁹ <http://secunia.com/advisories/36549/>²⁵⁹⁰ <http://secunia.com/advisories/37152/>²⁵⁹¹ <https://www.suse.com/support/security/advisories/>²⁵⁹² http://httpd.apache.org/security/vulnerabilities_22.html²⁵⁹³ Event MPM je eksperimentalna varijanta worker MPM-a dizajnirana sa ciljem da se omogući istovremena obrada više zahteva prepuštajući određene procese pomoćnim thread-ovima, oslobađajući glavne thread-ove za rad na novim zahtevima. Dostupno na <http://httpd.apache.org/docs/2.2/mod/event.html>, 10.02.2013²⁵⁹⁴ <http://www.securityfocus.com/bid/36596>²⁵⁹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2699>²⁵⁹⁶ <http://xforce.iss.net/xforce/xfdb/53666>²⁵⁹⁷ http://httpd.apache.org/security/vulnerabilities_22.html

26.	Browsable web directory (http-generic-browsable-dir)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Otkriven je direktorijum na web serveru koji može biti pretraživan, što znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice-spajdering (prateći hiperlinkove), ili -kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute-force napadom na liste uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skrivenne“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice. http://172.23.202.193/icons/small/ 4: <title>Index of /icons/small</title> 5: </head> 6: <body> 7: Index of /icons/small 8: ...CO]<th>Name</th><th><a href=?C=M;O=A...		Ozbiljan	Za Apache: onemogućiti pretraživanje direktorijuma mreže za sve direktorijume i poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirajti fajlove u web root, osim ako u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume. Za Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote: Onemogućiti pretraživanje direktorijuma za sve direktorijume i poddirektorijume. Uključiti Tomcat-ov web.xml file. U odeljku „default“, promeniti parametar „listings“ iz „true“ u „false“. Restartovati server. Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripta i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume.	
27.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	172.23.202.193:21 172.23.202.227:21 172.23.202.194:80 172.23.202.226:80 Kada se kod TCP-a paketa koristi Large Window Size, olakšava se	BID: 10183 ²⁵⁹⁸ CERT-VN: 415294 ²⁵⁹⁹ CVE CVE-2004-0230 ²⁶⁰⁰ MS: MS05-019 ²⁶⁰¹ MS: MS06-064 ²⁶⁰² NETBSD: NetBSD-		Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC 2385 . ²⁶¹⁶ Ono je napravljeno da smanji opasnost od određenih

²⁵⁹⁸ <http://www.securityfocus.com/bid/10183>²⁵⁹⁹ <http://www.kb.cert.org/vuls/id/415294>²⁶⁰⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>²⁶⁰¹ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>²⁶⁰² <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>

		spoljnom napadaču da otkrije sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP veze) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao što je BGP.	SA2004-006 ²⁶⁰³ OVAL: OVAL2689 ²⁶⁰⁴ OVAL: OVAL270 ²⁶⁰⁵ OVAL OVAL3508 ²⁶⁰⁶ OVAL OVAL4791 ²⁶⁰⁷ OVAL OVAL5711 ²⁶⁰⁸ SECUNIA: 11440 ²⁶⁰⁹ SECUNIA 11458 ²⁶¹⁰ SECUNIA: 22341 ²⁶¹¹ SGI 20040403-01-A ²⁶¹² XF tcp-rst-dos(15886) ²⁶¹³ URL1 ²⁶¹⁴ URL2 ²⁶¹⁵		napada na BGP, kao što su TCP reseti.
28.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podesi na jedinstvenu vrednost i da se koristi u rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da fingerprint-uje operativni sistem.	BID 4314 ²⁶¹⁷ CVE CVE-2002-0510 ²⁶¹⁸ XF linux-udp-fingerprint(8588) ²⁶¹⁹	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili pak ranjivost koju treba popravljati, tako da ne postoje rešenja koja se mogu kupiti. Jedino se može postaviti fajervol ili neka druga sprava za filtriranje između napadnutog i neprijateljskog napada koji je u mogućnosti da randomizuje IP ID-jeve.
29.	Apache httpd mod_imagemap XSS (CVE-2007-5000) (apache-httpd-2_2_x-mod_imagemap-xss-cve-2007-5000)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Propust je otkriven u modulu mod_imagemap. Na sajtovima na kojima je omogućen mod_imagemap i imagemap fajl je javno dostupan, moguć je izvesti napad tipa "crosssite scripting attack".	BID 26838 ²⁶²⁰ CERT TA08-150A ²⁶²¹ CVE CVE-2007-5000 ²⁶²² OSVDB 39134 ²⁶²³ OVAL OVAL9539 ²⁶²⁴ REDHAT 2008:0004 ²⁶²⁵ RHSA- REDHAT 2008:0005 ²⁶²⁶ RHSA- REDHAT 2008:0006 ²⁶²⁷ RHSA- REDHAT 2008:0007 ²⁶²⁸ RHSA- REDHAT 2008:0008 ²⁶²⁹ RHSA- REDHAT 2008:0009 ²⁶³⁰ RHSA-	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.8.tar.gz

²⁶¹⁶ <http://www.ietf.org/rfc/rfc2385.txt>²⁶⁰³ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>²⁶⁰⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>²⁶⁰⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>²⁶⁰⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>²⁶⁰⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>²⁶⁰⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>²⁶⁰⁹ <http://secunia.com/advisories/11440/>²⁶¹⁰ <http://secunia.com/advisories/11458/>²⁶¹¹ <http://secunia.com/advisories/22341/>²⁶¹² <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>²⁶¹³ <http://xforce.iss.net/xforce/xfdb/15886>²⁶¹⁴ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>²⁶¹⁵ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>²⁶¹⁷ <http://www.securityfocus.com/bid/4314>²⁶¹⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>²⁶¹⁹ <http://xforce.iss.net/xforce/xfdb/8588>²⁶²⁰ <http://www.securityfocus.com/bid/26838>²⁶²¹ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>²⁶²² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-5000>²⁶²³ <http://www.osvdb.org/39134>²⁶²⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9539>²⁶²⁵ <http://rhn.redhat.com/errata/RHSA-2008-0004.html>²⁶²⁶ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>²⁶²⁷ <http://rhn.redhat.com/errata/RHSA-2008-0006.html>²⁶²⁸ <http://rhn.redhat.com/errata/RHSA-2008-0007.html>²⁶²⁹ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>

			REDHAT ²⁶³¹ RHSA- 2008:0261 SECUNIA ²⁶³² 28046 SECUNIA ²⁶³³ 28073 SECUNIA ²⁶³⁴ 28081 SECUNIA ²⁶³⁵ 28196 SECUNIA ²⁶³⁶ 28375 SECUNIA ²⁶³⁷ 28467 SECUNIA ²⁶³⁸ 28471 SECUNIA ²⁶³⁹ 28525 SECUNIA ²⁶⁴⁰ 28526 SECUNIA ²⁶⁴¹ 28607 SECUNIA ²⁶⁴² 28749 SECUNIA ²⁶⁴³ 28750 SECUNIA ²⁶⁴⁴ 28922 SECUNIA ²⁶⁴⁵ 28977 SECUNIA ²⁶⁴⁶ 29420 SECUNIA ²⁶⁴⁷ 29640 SECUNIA ²⁶⁴⁸ 29806 SECUNIA ²⁶⁴⁹ 29988 SECUNIA ²⁶⁵⁰ 30356 SECUNIA ²⁶⁵¹ 30430 SECUNIA ²⁶⁵² 30732 SECUNIA ²⁶⁵³ 31142 SUSE ²⁶⁵⁴ SUSE- SA:2008:021 URL1 ²⁶⁵⁵		
30.	Apache httpd mod_proxy_ftp globbing XSS (CVE- 2008-2939) (apache- httpd-2_2_x- mod_proxy_ftp- globbing- xss-cve-2008-2939)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osjetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ftp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti.. Propust je otkriven u modulu	APPLE ²⁶⁵⁶ APPLE-SA- 2009-05-12 BID ²⁶⁵⁷ 30560 CERT ²⁶⁵⁸ TA09-133A CERT-VN ²⁶⁵⁹ 663763 CVE ²⁶⁶⁰ CVE-2008-2939 OVAL ²⁶⁶¹ OVAL11316 OVAL ²⁶⁶² OVAL7716 REDHAT ²⁶⁶³ RHSA- 2008:0966	Ozbiljan	Apache >= 2.2 i < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dis t/httpd/httpd-2.2.10.tar.gz

²⁶³⁰ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>

²⁶³¹ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>

²⁶³² <http://secunia.com/advisories/28046/>

²⁶³³ <http://secunia.com/advisories/28073/>

²⁶³⁴ <http://secunia.com/advisories/28081/>

²⁶³⁵ <http://secunia.com/advisories/28196/>

²⁶³⁶ <http://secunia.com/advisories/28375/>

²⁶³⁷ <http://secunia.com/advisories/28467/>

²⁶³⁸ <http://secunia.com/advisories/28471/>

²⁶³⁹ <http://secunia.com/advisories/28525/>

²⁶⁴⁰ <http://secunia.com/advisories/28526/>

²⁶⁴¹ <http://secunia.com/advisories/28607/>

²⁶⁴² <http://secunia.com/advisories/28749/>

²⁶⁴³ <http://secunia.com/advisories/28750/>

²⁶⁴⁴ <http://secunia.com/advisories/28922/>

²⁶⁴⁵ <http://secunia.com/advisories/28977/>

²⁶⁴⁶ <http://secunia.com/advisories/29420/>

²⁶⁴⁷ <http://secunia.com/advisories/29640/>

²⁶⁴⁸ <http://secunia.com/advisories/29806/>

²⁶⁴⁹ <http://secunia.com/advisories/29988/>

²⁶⁵⁰ <http://secunia.com/advisories/30356/>

²⁶⁵¹ <http://secunia.com/advisories/30430/>

²⁶⁵² <http://secunia.com/advisories/30732/>

²⁶⁵³ <http://secunia.com/advisories/31142/>

²⁶⁵⁴ <https://www.suse.com/support/security/advisories/>

²⁶⁵⁵ http://httpd.apache.org/security/vulnerabilities_20.html

²⁶⁵⁶ <http://lists.apple.com/archives/security-announce/2009/May/msg00001.html>

²⁶⁵⁷ <http://www.securityfocus.com/bid/30560>

²⁶⁵⁸ <http://www.us-cert.gov/ncas/alerts/TA09-133A>

²⁶⁵⁹ <http://www.kb.cert.org/vuls/id/663763>

²⁶⁶⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-2939>

²⁶⁶¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11316>

²⁶⁶² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7716>

		mod_proxy_ftp prilikom obrade "wildcard"-a ukoliko se on nađe na putanji FTP URL. Ukoliko je mod_proxy_ftp omogućen da podržava FTP-over-HTTP, zahtevi koji sadrže specijalne karaktere mogu da dovedu do cross-site scripting (XSS) napada.	REDHAT RHSA-2008:0967 ²⁶⁶⁴ SECUNIA 31384 ²⁶⁶⁵ SECUNIA 31673 ²⁶⁶⁶ SECUNIA 32685 ²⁶⁶⁷ SECUNIA 32838 ²⁶⁶⁸ SECUNIA 33156 ²⁶⁶⁹ SECUNIA 33797 ²⁶⁷⁰ SECUNIA 34219 ²⁶⁷¹ SECUNIA 35074 ²⁶⁷² XF apache-modproxyftp-xss(44223) ²⁶⁷³ URL1 ²⁶⁷⁴		
31.	Apache httpd mod_proxy_ftp UTF-7 XSS (CVE-2008-0005) (apache-httpd-2.2.x-mod_proxy_ftp-utf-7-xsscve-2008-0005)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 U modul mod_proxy_ftp je dodata zaobilaznica. Na sajtovima na kojima je omogućen mod_proxy_ftp i konfigurisan forward tip proxy-ja, moguće je izvesti napad XSS na Web pretraživače koji ne prepoznaju određeni character set prema pravilima iz dokumenta RFC 2616.	BID 27234 ²⁶⁷⁵ CVE CVE-2008-0005 ²⁶⁷⁶ OVAL OVAL10812 ²⁶⁷⁷ REDHAT RHSA-2008:0004 ²⁶⁷⁸ REDHAT RHSA-2008:0005 ²⁶⁷⁹ REDHAT RHSA-2008:0006 ²⁶⁸⁰ REDHAT RHSA-2008:0007 ²⁶⁸¹ REDHAT RHSA-2008:0008 ²⁶⁸² REDHAT RHSA-2008:0009 ²⁶⁸³ SECUNIA 28467 ²⁶⁸⁴ SECUNIA 28471 ²⁶⁸⁵ SECUNIA 28526 ²⁶⁸⁶ SECUNIA 28607 ²⁶⁸⁷ SECUNIA 28749 ²⁶⁸⁸ SECUNIA 28977 ²⁶⁸⁹ SECUNIA 29348 ²⁶⁹⁰ SECUNIA 29420 ²⁶⁹¹ SECUNIA 29640 ²⁶⁹² SECUNIA 30732 ²⁶⁹³ SECUNIA 35650 ²⁶⁹⁴	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.8.tar.gz

²⁶⁶³ <http://rhn.redhat.com/errata/RHSA-2008-0966.html>²⁶⁶⁴ <http://rhn.redhat.com/errata/RHSA-2008-0967.html>²⁶⁶⁵ <http://secunia.com/advisories/31384/>²⁶⁶⁶ <http://secunia.com/advisories/31673/>²⁶⁶⁷ <http://secunia.com/advisories/32685/>²⁶⁶⁸ <http://secunia.com/advisories/32838/>²⁶⁶⁹ <http://secunia.com/advisories/33156/>²⁶⁷⁰ <http://secunia.com/advisories/33797/>²⁶⁷¹ <http://secunia.com/advisories/34219/>²⁶⁷² <http://secunia.com/advisories/35074/>²⁶⁷³ <http://xforce.iss.net/xforce/xfdb/44223>²⁶⁷⁴ http://httpd.apache.org/security/vulnerabilities_22.html²⁶⁷⁵ <http://www.securityfocus.com/bid/27234>²⁶⁷⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0005>²⁶⁷⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10812>²⁶⁷⁸ <http://rhn.redhat.com/errata/RHSA-2008-0004.html>²⁶⁷⁹ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>²⁶⁸⁰ <http://rhn.redhat.com/errata/RHSA-2008-0006.html>²⁶⁸¹ <http://rhn.redhat.com/errata/RHSA-2008-0007.html>²⁶⁸² <http://rhn.redhat.com/errata/RHSA-2008-0008.html>²⁶⁸³ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>²⁶⁸⁴ <http://secunia.com/advisories/28467/>²⁶⁸⁵ <http://secunia.com/advisories/28471/>²⁶⁸⁶ <http://secunia.com/advisories/28526/>²⁶⁸⁷ <http://secunia.com/advisories/28607/>²⁶⁸⁸ <http://secunia.com/advisories/28749/>²⁶⁸⁹ <http://secunia.com/advisories/28977/>²⁶⁹⁰ <http://secunia.com/advisories/29348/>²⁶⁹¹ <http://secunia.com/advisories/29420/>²⁶⁹² <http://secunia.com/advisories/29640/>²⁶⁹³ <http://secunia.com/advisories/30732/>

			SUSE SA:2008:021 ²⁶⁹⁵ XF apache-modproxyftp- utf7-xss(39615) URL1 ²⁶⁹⁶		
32.	Apache httpd mod_status XSS (CVE- 2007-6388) (apache- httpd-2_2_x- mod_status-xss-cve- 2007-6388)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Propust je otkriven u modulu mod_status. Na sajtovima na kojima je omogućen mod_status i ukoliko su stranice statusa javno dostupne, postoji mogućnost XSS napada. Stranica sa statusom servera nije po difoltu omogućena, a dosadašnja praksa je pokazala da je najbolje da ona ne bude javno dostupna.	BID 27237 ²⁶⁹⁷ CERT TA08-150A ²⁶⁹⁸ CVE CVE-2007-6388 ²⁶⁹⁹ OVAL OVAL10272 ²⁷⁰⁰ REDHAT RHSA- 2008:0004 ²⁷⁰¹ REDHAT RHSA- 2008:0005 ²⁷⁰² REDHAT RHSA- 2008:0006 ²⁷⁰³ REDHAT RHSA- 2008:0007 ²⁷⁰⁴ REDHAT RHSA- 2008:0008 ²⁷⁰⁵ REDHAT RHSA- 2008:0009 ²⁷⁰⁶ REDHAT RHSA- 2008:0261 ²⁷⁰⁷ SECUNIA 28467 ²⁷⁰⁸ SECUNIA 28471 ²⁷⁰⁹ SECUNIA 28526 ²⁷¹⁰ SECUNIA 28607 ²⁷¹¹ SECUNIA 28749 ²⁷¹² SECUNIA 28922 ²⁷¹³ SECUNIA 28965 ²⁷¹⁴ SECUNIA 28977 ²⁷¹⁵ SECUNIA 29420 ²⁷¹⁶ SECUNIA 29504 ²⁷¹⁷ SECUNIA 29640 ²⁷¹⁸ SECUNIA 29806 ²⁷¹⁹ SECUNIA 29988 ²⁷²⁰ SECUNIA 30356 ²⁷²¹ SECUNIA 30430 ²⁷²² SECUNIA 30732 ²⁷²³ SECUNIA 31142 ²⁷²⁴	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dis t/httpd/httpd-2.2.8.tar.gz

²⁶⁹⁴ <http://secunia.com/advisories/35650/>²⁶⁹⁵ <https://www.suse.com/support/security/advisories/>²⁶⁹⁶ http://httpd.apache.org/security/vulnerabilities_20.html²⁶⁹⁷ <http://www.securityfocus.com/bid/27237>²⁶⁹⁸ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>²⁶⁹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6388>²⁷⁰⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10272>²⁷⁰¹ <http://rhn.redhat.com/errata/RHSA-2008-0004.html>²⁷⁰² <http://rhn.redhat.com/errata/RHSA-2008-0005.html>²⁷⁰³ <http://rhn.redhat.com/errata/RHSA-2008-0006.html>²⁷⁰⁴ <http://rhn.redhat.com/errata/RHSA-2008-0007.html>²⁷⁰⁵ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>²⁷⁰⁶ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>²⁷⁰⁷ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>²⁷⁰⁸ <http://secunia.com/advisories/28467/>²⁷⁰⁹ <http://secunia.com/advisories/28471/>²⁷¹⁰ <http://secunia.com/advisories/28526/>²⁷¹¹ <http://secunia.com/advisories/28607/>²⁷¹² <http://secunia.com/advisories/28749/>²⁷¹³ <http://secunia.com/advisories/28922/>²⁷¹⁴ <http://secunia.com/advisories/28965/>²⁷¹⁵ <http://secunia.com/advisories/28977/>²⁷¹⁶ <http://secunia.com/advisories/29420/>²⁷¹⁷ <http://secunia.com/advisories/29504/>²⁷¹⁸ <http://secunia.com/advisories/29640/>²⁷¹⁹ <http://secunia.com/advisories/29806/>²⁷²⁰ <http://secunia.com/advisories/29988/>²⁷²¹ <http://secunia.com/advisories/30356/>²⁷²² <http://secunia.com/advisories/30430/>²⁷²³ <http://secunia.com/advisories/30732/>

			SECUNIA 33200 ²⁷²⁵ SUSE SUSE-SA:2008:021 ²⁷²⁶ XF apache-status-page-xss(39472) ²⁷²⁷		
33.	Apache httpd apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpd-cve-2011-0419)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_autoindex. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_fnmatch() u sklopu APR biblioteke. Ako je omogućen mod_autoindex, a indeksi direktorijuma mod_autoindex su sadržavali fajlove sa dovoljno dugim nazivima, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do preterane upotrebe CPU-a. Ovo bi moglo da bude iskorišćeno u napadu odbijanja servisa. Zahvaljujući Maksymilian Arciemowicz prijavljen je ovaj propust.	CVE CVE-2011-0419 ²⁷²⁸ REDHAT RHSA-2011:0507 ²⁷²⁹ SECUNIA 44490 ²⁷³⁰ SECUNIA 44564 ²⁷³¹ SECUNIA 44574 ²⁷³² URL1 ²⁷³³	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.18.tar.gz
34.	Apache httpd APR-util heap underwrite (CVE-2009-0023) (http-apache-apr-util-heap-underwrite)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako napadač poseduje posebno kreiranu ključnu reč za pretraživanje one funkcije koja upravlja kompajliranjem formi zahtevane pretrage. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u načinu na koji komplet APR-biblioteke kompajlira forme zahtevanih pretraživanja. Napadač bi mogao da kreira posebno izrađenu ključnu reč pretraživanja,	BID 35221 ²⁷³⁴ CVE CVE-2009-0023 ²⁷³⁵ DEBIAN DSA-1812 ²⁷³⁶ OVAL OVAL10968 ²⁷³⁷ REDHAT RHSA-2009:1107 ²⁷³⁸ REDHAT RHSA-2009:1108 ²⁷³⁹ SECUNIA 34724 ²⁷⁴⁰ SECUNIA 35284 ²⁷⁴¹ SECUNIA 35360 ²⁷⁴² SECUNIA 35395 ²⁷⁴³ SECUNIA 35444 ²⁷⁴⁴ SECUNIA 35487 ²⁷⁴⁵ SECUNIA 35565 ²⁷⁴⁶ SECUNIA 35710 ²⁷⁴⁷ SECUNIA 35797 ²⁷⁴⁸	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

²⁷²⁴ <http://secunia.com/advisories/31142/>²⁷²⁵ <http://secunia.com/advisories/33200/>²⁷²⁶ <https://www.suse.com/support/security/advisories/>²⁷²⁷ <http://xforce.iss.net/xforce/xfdb/39472> pristupljeno 11.12.2011²⁷²⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419>²⁷²⁹ <http://rhn.redhat.com/errata/RHSA-2011-0507.html>²⁷³⁰ <http://secunia.com/advisories/44490/>²⁷³¹ <http://secunia.com/advisories/44564/>²⁷³² <http://secunia.com/advisories/44574/>²⁷³³ http://httpd.apache.org/security/vulnerabilities_22.html²⁷³⁴ <http://www.securityfocus.com/bid/35221>²⁷³⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-0023>²⁷³⁶ <http://lists.debian.org/debian-security-announce/2009/msg00124.html>²⁷³⁷ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval:def:10968>²⁷³⁸ <http://rhn.redhat.com/errata/RHSA-2009-1107.html>²⁷³⁹ <http://rhn.redhat.com/errata/RHSA-2009-1108.html>²⁷⁴⁰ <http://secunia.com/advisories/34724/>²⁷⁴¹ <http://secunia.com/advisories/35284/>²⁷⁴² <http://secunia.com/advisories/35360/>²⁷⁴³ <http://secunia.com/advisories/35395/>²⁷⁴⁴ <http://secunia.com/advisories/35444/>²⁷⁴⁵ <http://secunia.com/advisories/35487/>²⁷⁴⁶ <http://secunia.com/advisories/35565/>²⁷⁴⁷ <http://secunia.com/advisories/35710/>

		koja bi se proizvoljnim prepisivanjem gomilala u memoriji prilikom obrađivanja zahteva za pretragu.	SECUNIA 35843 ²⁷⁴⁹ SECUNIA 37221 ²⁷⁵⁰ XF apache-aprstrmatchprecompile-dos(50964) ²⁷⁵¹ URL1 ²⁷⁵²		
35.	Apache httpd mod_proxy_balancer CSRF (CVE-2007-6420) (http-apache-mod_proxy_balancer-csrf)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Mod_proxy_balancer je omogućio administrativni interfejs koji bi mogao biti ranjiv na napade lažnih zahteva CSRF (cross-site request forgery).	BID 27236 ²⁷⁵³ BID 31681 ²⁷⁵⁴ CVE CVE-2007-6420 ²⁷⁵⁵ OVAL OVAL8371 ²⁷⁵⁶ REDHAT RHSA-2008:0966 ²⁷⁵⁷ SECUNIA 31026 ²⁷⁵⁸ SECUNIA 32222 ²⁷⁵⁹ SECUNIA 33797 ²⁷⁶⁰ SECUNIA 34219 ²⁷⁶¹ URL1 ²⁷⁶²	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.9.tar.gz
36.	Apache httpd mod_proxy_balancer DoS (CVE-2007-6422) (http-apache-mod_proxy_balancer-dos)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Propust je otkriven u modulu mod_proxy_balancer. Na sajtovmu na kojima je omogućen mod_proxy_balancer, autorizovan korisnik bi mogao poslati pažljivo izrađen zahtev koji bi doveo do toga da krahira child proces Apache-a koji taj zahtev obrađuje. To može dovesti samo do odbijanja servisa ako se koristi threaded MPM.	BID 27236 ²⁷⁶³ CVE CVE-2007-6422 ²⁷⁶⁴ OVAL OVAL10181 ²⁷⁶⁵ OVAL OVAL8690 ²⁷⁶⁶ REDHAT RHSA-2008:0008 ²⁷⁶⁷ REDHAT RHSA-2008:0009 ²⁷⁶⁸ SECUNIA 28526 ²⁷⁶⁹ SECUNIA 28749 ²⁷⁷⁰ SECUNIA 28977 ²⁷⁷¹ SECUNIA 29348 ²⁷⁷² SECUNIA 29640 ²⁷⁷³ SUSE SUSE-SA:2008:021 ²⁷⁷⁴ XF apache-modproxybalancer-dos(39476) ²⁷⁷⁵ URL1 ²⁷⁷⁶	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.8.tar.gz
37.	Apache httpd mod_proxy_balancer	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80	BID 27236 ²⁷⁷⁷ CVE CVE-2007-6421 ²⁷⁷⁸ OVAL OVAL10664 ²⁷⁷⁹	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati:

²⁷⁴⁸ <http://secunia.com/advisories/35797/>²⁷⁴⁹ <http://secunia.com/advisories/35843/>²⁷⁵⁰ <http://secunia.com/advisories/37221/>²⁷⁵¹ <http://xforce.iss.net/xforce/xfdb/50964>²⁷⁵² http://httpd.apache.org/security/vulnerabilities_22.html²⁷⁵³ <http://www.securityfocus.com/bid/27236>²⁷⁵⁴ <http://www.securityfocus.com/bid/31681>²⁷⁵⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6420>²⁷⁵⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8371>²⁷⁵⁷ <http://rhn.redhat.com/errata/RHSA-2008-0966.html>²⁷⁵⁸ <http://secunia.com/advisories/31026/>²⁷⁵⁹ <http://secunia.com/advisories/32222/>²⁷⁶⁰ <http://secunia.com/advisories/33797/>²⁷⁶¹ <http://secunia.com/advisories/34219/>²⁷⁶² http://httpd.apache.org/security/vulnerabilities_22.html²⁷⁶³ <http://www.securityfocus.com/bid/27236>²⁷⁶⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6422>²⁷⁶⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10181>²⁷⁶⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8690>²⁷⁶⁷ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>²⁷⁶⁸ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>²⁷⁶⁹ <http://secunia.com/advisories/28526/>²⁷⁷⁰ <http://secunia.com/advisories/28749/>²⁷⁷¹ <http://secunia.com/advisories/28977/>²⁷⁷² <http://secunia.com/advisories/29348/>²⁷⁷³ <http://secunia.com/advisories/29640/>²⁷⁷⁴ <https://www.suse.com/support/security/advisories/>²⁷⁷⁵ <http://xforce.iss.net/xforce/xfdb/39476>²⁷⁷⁶ http://httpd.apache.org/security/vulnerabilities_22.html²⁷⁷⁷ <http://www.securityfocus.com/bid/27236>²⁷⁷⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6421>

	XSS (CVE-2007-6421) (http-apache-mod_proxy_balancer-xss)	172.23.202.227:80 Propust je otkriven u modulu mod_proxy_balancer. Na sajtovmima na kojima je omogućen mod_proxy_balancer, moguć je XSS napad prema autorizovanom korisniku.	OVAL OVAL8651 ²⁷⁸⁰ REDHAT RHSA-2008:0008 ²⁷⁸¹ REDHAT RHSA-2008:0009 ²⁷⁸² SECUNIA 28526 ²⁷⁸³ SECUNIA 28749 ²⁷⁸⁴ SECUNIA 28977 ²⁷⁸⁵ SECUNIA 29420 ²⁷⁸⁶ SECUNIA 29640 ²⁷⁸⁷ SUSE SUSE-SA:2008:021 ²⁷⁸⁸ XF apache-modproxybalancer-dos(39476) ²⁷⁸⁹ URL1 ²⁷⁹⁰		http://archive.apache.org/dist/httpd/httpd-2.2.8.tar.gz
38.	Apache httpd mod_status cross-site scripting (CVE-2006-5752) (http-apache-mod_status-xss)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Propust je otkriven u modulu mod_status. Na sajtovmima na kojima je status servera javno dostupan i omogućen je ExtendedStatus, postoji mogućnost XSS napada. Stranica sa statusom servera nije po defaultu omogućena, a dosadašnja praksa je pokazala da je najbolje da ona ne bude javno dostupna.	BID 24645 ²⁷⁹¹ CVE CVE-2006-5752 ²⁷⁹² OVAL OVAL10154 ²⁷⁹³ REDHAT RHSA-2007:0532 ²⁷⁹⁴ REDHAT RHSA-2007:0533 ²⁷⁹⁵ REDHAT RHSA-2007:0534 ²⁷⁹⁶ REDHAT RHSA-2007:0556 ²⁷⁹⁷ REDHAT RHSA-2007:0557 ²⁷⁹⁸ REDHAT RHSA-2008:0261 ²⁷⁹⁹ SECUNIA 25827 ²⁸⁰⁰ SECUNIA 25830 ²⁸⁰¹ SECUNIA 25873 ²⁸⁰² SECUNIA 25920 ²⁸⁰³ SECUNIA 26273 ²⁸⁰⁴ SECUNIA 26443 ²⁸⁰⁵ SECUNIA 26458 ²⁸⁰⁶ SECUNIA 26508 ²⁸⁰⁷ SECUNIA 26822 ²⁸⁰⁸	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz

²⁷⁷⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10664>²⁷⁸⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8651>²⁷⁸¹ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>²⁷⁸² <http://rhn.redhat.com/errata/RHSA-2008-0009.html>²⁷⁸³ <http://secunia.com/advisories/28526/>²⁷⁸⁴ <http://secunia.com/advisories/28749/>²⁷⁸⁵ <http://secunia.com/advisories/28977/>²⁷⁸⁶ <http://secunia.com/advisories/29420/>²⁷⁸⁷ <http://secunia.com/advisories/29640/>²⁷⁸⁸ <https://www.suse.com/support/security/advisories/>²⁷⁸⁹ <http://xforce.iss.net/xforce/xfdb/39476>²⁷⁹⁰ http://httpd.apache.org/security/vulnerabilities_22.html²⁷⁹¹ <http://www.securityfocus.com/bid/24645>²⁷⁹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-5752>²⁷⁹³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10154>²⁷⁹⁴ <http://rhn.redhat.com/errata/RHSA-2007-0532.html>²⁷⁹⁵ <http://rhn.redhat.com/errata/RHSA-2007-0533.html>²⁷⁹⁶ <http://rhn.redhat.com/errata/RHSA-2007-0534.html>²⁷⁹⁷ <http://rhn.redhat.com/errata/RHSA-2007-0556.html>²⁷⁹⁸ <http://rhn.redhat.com/errata/RHSA-2007-0557.html>²⁷⁹⁹ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>²⁸⁰⁰ <http://secunia.com/advisories/25827/>²⁸⁰¹ <http://secunia.com/advisories/25830/>²⁸⁰² <http://secunia.com/advisories/25873/>²⁸⁰³ <http://secunia.com/advisories/25920/>²⁸⁰⁴ <http://secunia.com/advisories/26273/>²⁸⁰⁵ <http://secunia.com/advisories/26443/>²⁸⁰⁶ <http://secunia.com/advisories/26458/>²⁸⁰⁷ <http://secunia.com/advisories/26508/>²⁸⁰⁸ <http://secunia.com/advisories/26822/>

			SECUNIA 26842 ²⁸⁰⁹ SECUNIA 26993 ²⁸¹⁰ SECUNIA 27037 ²⁸¹¹ SECUNIA 27563 ²⁸¹² SECUNIA 27732 ²⁸¹³ SECUNIA 28212 ²⁸¹⁴ SECUNIA 28224 ²⁸¹⁵ SECUNIA 28606 ²⁸¹⁶ SUSE SA:2007:061 ²⁸¹⁷ XF apache-modstatus- xss(35097) URL1 ²⁸¹⁸		
39.	Apache httpd Subrequest handling of request headers (mod_headers) (CVE-2010-0434) (http-apacherequest-header-info-disclosure)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Propust u jezgru "subrequest process code" može dovesti do greške tipa segmentation fault-a ili do otkrivanja podataka iz nekog drugog zahteva na thread-ovima servera, kao što su worker ili winnt MPM-ovi. Zahvaljujući Philip Pickett-u iz Vmware ovaj propust je prijavljen i predložen je način ispravke.	BID 38494 ²⁸¹⁹ CVE CVE-2010-0434 ²⁸²⁰ DEBIAN DSA-2035 ²⁸²¹ OVAL OVAL10358 ²⁸²² OVAL OVAL8695 ²⁸²³ REDHAT RHSA-2010:0168 ²⁸²⁴ REDHAT RHSA-2010:0175 ²⁸²⁵ SECUNIA 39100 ²⁸²⁶ SECUNIA 39115 ²⁸²⁷ SECUNIA 39501 ²⁸²⁸ SECUNIA 39628 ²⁸²⁹ SECUNIA 39632 ²⁸³⁰ SECUNIA 39656 ²⁸³¹ SECUNIA 40096 ²⁸³² XF apache-http-rh-info-disclosure(56625) ²⁸³³ URL1 ²⁸³⁴	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz
40.	OpenSSH CBC Mode Information Disclosure Vulnerability (ssh-openssh-cbc-mode-info-disclosure)	172.23.202.193:22 172.23.202.194:22 172.23.202.226:22 172.23.202.227:22 Određene verzije OpenSSH-a poseduju ranjivu implementaciju blok	BID 32319 ²⁸³⁵ CVE CVE-2008-5161 ²⁸³⁶ SECUNIA 32760 ²⁸³⁷ URL1 ²⁸³⁸ URL2 ²⁸³⁹	Ozbiljan	Uraditi download a zatim instalirati: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-5.2p1.tar.gz Verzija 5.2 OpenSSH-a je

²⁸⁰⁹ <http://secunia.com/advisories/26842/>²⁸¹⁰ <http://secunia.com/advisories/26993/>²⁸¹¹ <http://secunia.com/advisories/27037/>²⁸¹² <http://secunia.com/advisories/27563/>²⁸¹³ <http://secunia.com/advisories/27732/>²⁸¹⁴ <http://secunia.com/advisories/28212/>²⁸¹⁵ <http://secunia.com/advisories/28224/>²⁸¹⁶ <http://secunia.com/advisories/28606/>²⁸¹⁷ <https://www.suse.com/support/security/advisories/>²⁸¹⁸ http://httpd.apache.org/security/vulnerabilities_20.html²⁸¹⁹ <http://www.securityfocus.com/bid/38494>²⁸²⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0434>²⁸²¹ <http://www.debian.org/security/2010/dsa-2035>²⁸²² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10358>²⁸²³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8695>²⁸²⁴ <http://rhn.redhat.com/errata/RHSA-2010-0168.html>²⁸²⁵ <http://rhn.redhat.com/errata/RHSA-2010-0175.html>²⁸²⁶ <http://secunia.com/advisories/39100/>²⁸²⁷ <http://secunia.com/advisories/39115/>²⁸²⁸ <http://secunia.com/advisories/39501/>²⁸²⁹ <http://secunia.com/advisories/39628/>²⁸³⁰ <http://secunia.com/advisories/39632/>²⁸³¹ <http://secunia.com/advisories/39656/>²⁸³² <http://secunia.com/advisories/40096/>²⁸³³ <http://xforce.iss.net/xforce/xfdb/56625>²⁸³⁴ http://httpd.apache.org/security/vulnerabilities_22.html²⁸³⁵ <http://www.securityfocus.com/bid/32319>²⁸³⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-5161>²⁸³⁷ <http://secunia.com/advisories/32760/>²⁸³⁸ http://www.cpni.gov.uk/Docs/Vulnerability_Advisory_SSH.txt, pristupljeno 20.12.2011²⁸³⁹ <http://www.openssh.com/txt/cbc.adv>

		šifarskog algoritma u CBC modu (Cipher Block Chaining). Ovo bi udaljenom napadaču moglo omogućiti da preko nepoznatih vektora pridobije određene podatke u vidu običnog teksta iz proizvoljnog bloka šifrovanog teksta u SSH sesiji.			puštena u promet 22. februara 2009.
41.	OpenSSH „X11UseLocalhost“ X11 Forwarding Session Hijacking Vulnerability (ssh-opensshx11uselocalhost - x11-forwarding-session-hijack)	172.23.202.193:22 172.23.202.194:22 172.23.202.226:22 172.23.202.227:22 Određene verzije OpenSSH-a podešavaju SO_REUSEADDR socket opciju kada je onemogućeno podešavanje X11UseLocalhost konfiguracije. Ovo bi lokalnom napadaču moglo da omogući da preuzme X11 forwarding port preko veze ka pojedinačnoj IP adresi.	BID 30339 ²⁸⁴⁰ CVE CVE-2008-3259 ²⁸⁴¹ SECUNIA 31179 ²⁸⁴²	Ozbiljan	Uraditi download a zatim instalirati: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-5.1p1.tar.gz Verzija 5.1 OpenSSH-a je puštena u promet 21. jula 2008.
42.	HTTP TRACE Method Enabled (http-trace-method-enabled)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 HTTP TRACE metoda se obično koristi da uzvрати potpuni HTTP zahtev klijentu koji ga zahteva, u cilju debugovanja proxy servera. Napadač bi mogao da kreira web stranicu koristeći XMLHTTP, ActiveX ili XMLHttpRequest da natera klijenta da pošalje TRACE zahtev i da sačuva klijenove kolačiće. Kao posledica može da se javi XSS napad. Primer : 172.23.202.196:80 Running vulnerable HTTP service. http://172.23.202.193/ 1: TRACE / HTTP/1.1 2: Host: 172.23.202.193 3: Cookie: vulnerable=yes	CVE CVE-2004-2320 ²⁸⁴³ CVE CVE-2004-2763 ²⁸⁴⁴ CVE CVE-2005-3398 ²⁸⁴⁵ CVE CVE-2006-4683 ²⁸⁴⁶ CVE CVE-2007-3008 ²⁸⁴⁷ CVE CVE-2008-7253 ²⁸⁴⁸ CVE CVE-2009-2823 ²⁸⁴⁹ CVE CVE-2010-0386 ²⁸⁵⁰ OSVDB 877 ²⁸⁵¹ SUN 50603 ²⁸⁵² BID 9561 ²⁸⁵³ URL1 ²⁸⁵⁴ URL2 ²⁸⁵⁵	Ozbiljan	Apache Onemogućiti HTTP TRACE metodu za Apache. Novije verzije Apache-a (1.3.34 i 2.0.55 i novije) omogućuju konfiguracionu direktivu TraceEnable. Da bi se odbili TRACE zahteve, dodaje se sledeći red u konfiguraciju servera: TraceEnable off Za starije verzije Apache web servera, koristiti modul mod_rewrite da bi se odbili TRACE zahtevi: RewriteEngine On RewriteCond %{REQUEST_METHOD} ^TRACE RewriteRule .* - [F]
43.	Database Open Access (database-open-access)	172.23.202.193:3306 172.23.202.194:3306 172.23.202.226:3306 172.23.202.227:3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i	URL1 ²⁸⁵⁶	Umeren	Konfigurisati server baze podataka tako da dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.

²⁸⁴⁰ <http://www.securityfocus.com/bid/30339>²⁸⁴¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-3259>²⁸⁴² <http://secunia.com/advisories/31179/>²⁸⁴³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2320>²⁸⁴⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2763>²⁸⁴⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-3398>²⁸⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-4683>²⁸⁴⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3008>²⁸⁴⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-7253>²⁸⁴⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2823>²⁸⁵⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0386>²⁸⁵¹ <http://osvdb.org/877>²⁸⁵² <https://sunsolve.sun.com/search/document.do?assetkey=1-22-50603-1> pristupljeno 18.12.2011²⁸⁵³ <http://www.securityfocus.com/bid/9561>²⁸⁵⁴ <http://www.apacheweek.com/issues/03-01-24#news>²⁸⁵⁵ <http://www.kb.cert.org/vuls/id/867593>²⁸⁵⁶ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf

		novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posjedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7.			
44.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	CVE CVE-1999-0524 ²⁸⁵⁷ OSVDB 95 ²⁸⁵⁸ XF netmask(306) ²⁸⁵⁹ icmp- XF timestamp(322) ²⁸⁶⁰ icmp-	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost
45.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta (što zlonamerni napadač može iskoristiti pri planiranju daljih napada). Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1 ²⁸⁶¹ URL2 ²⁸⁶² URL3 ²⁸⁶³	Umeren	Onemogućite TCP vremenski pečat na Linux-u. Podesite vrednost net.ipv4.tcp_timestamps na 0 pokretanjem sledeće komande: sysctl -w net.ipv4.tcp_timestamps=0 Uz to, sledeću vrednost stavite u difoltni sysctl konfiguracioni fajl, uopšteno sysctl.conf.: net.ipv4.tcp_timestamps=0
46.	WebDAV Extensions are Enabled (http-generic-webdav-enabled)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 WebDAV je skup ekstenzija za HTTP protokol koji omogućava korisnicima da zajednički edituju i obrađuju fajlove na udaljenim web serverima. Mnogi web serveri po difoltu omogućavaju WebDAV ekstenzije, čak i kada nisu potrebne. S obzirom na dodatnu složenost, dosadašnja praksa je pokazala da treba onemogućiti WebDAV ukoliko se trenutno ne koristi.		Umeren	Apache: Potrebno je onemogućiti WebDAV ²⁸⁶⁴ (eng. Web-based Distributed Authoring and Versioning) za Apache. Proveriti da li je mod_dav modul isključen ili utvrditi da li postoji zahtevana autentifikacija na direktorijumima nad kojima se zahteva DAV. Apache Tomcat, Tomcat, Tomcat Web Server Onemogućiti WebDAV za Apache Tomcat. Isključiti WebDAV Servlet ²⁸⁶⁵ za sve web aplikacije koje se nalaze na web serveru. To se može uraditi tako što se ukloni definicija servlet-a za

²⁸⁵⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>²⁸⁵⁸ <http://www.osvdb.org/95>²⁸⁵⁹ <http://xforce.iss.net/xforce/xfdb/306>²⁸⁶⁰ <http://xforce.iss.net/xforce/xfdb/322>²⁸⁶¹ http://www.forensicswiki.org/wiki/TCP_timestamps²⁸⁶² <http://www.ietf.org/rfc/rfc1323.txt>²⁸⁶³ <http://uptime.netcraft.com/>²⁸⁶⁴ WebDAV je otvoreni standar za nabavku i prenos podataka putem računarskih mreža. Pri tome korisnici vizuelno dolaze do podataka kao da su na sopstvenom računaru. Preuzeto iz : <http://sr.wikipedia.org/sr/WebDAV> , 12.09.2012.²⁸⁶⁵ Servlet je objekat programskog jezika Java koji dinamički obrađuje zahteve i konstruiše odgovor na zahtev. Java servlet API omogućava Java programerima da dodaju dinamički sadržaj Web serveru korišćenjem Java platforme. Servlet najčešće generiše HTML kod, ali to može biti i XML ili nešto slično. Preuzeto iz : <http://sr.wikipedia.org/sr/Servlet>

					WebDAV (kategorija org.apache.catalina.servlets.WebdavServlet) i uklone sve servlet mape koje se pozivaju na WebDAV servlet.
47.	Apache HTTPD: CRLF injection in mod_negotiation when untrusted uploads are supported (CVE-2008-0456) (apache-httpd-cve-2008-0456)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_negotiation. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Moguće je ubaciti CRLF (Carriage Return and Line Feed) koji omogućava CRLF Injection napade (poznatih kao HTTP Response Splitting) za sajtove koji koriste mod_negotiation omogućavajući neproverene upload-ove na lokacije na kojima je omogućen MultiViews (višestruko pregledanje).	APPLE APPLE-SA-2009-05-12 ²⁸⁶⁶ BID 27409 ²⁸⁶⁷ CERT TA09-133A ²⁸⁶⁸ CVE CVE-2008-0456 ²⁸⁶⁹ SECUNIA 29348 ²⁸⁷⁰ SECUNIA 35074 ²⁸⁷¹ XF 39893 ²⁸⁷² URL1 ²⁸⁷³	Umeren	Apache HTTPD >= 2.2 and < 2.2.12 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

Tabela 75. Linux OS – Pronađeni servisi na IP adresi 172.23.202.193 (2011. godina)

SERVISI	FTP 172.23.202.193 tcp 21 vsFTPD 2.0.5 ftp.banner: 220 (vsFTPD 2.0.5) HTTP 172.23.202.193 tcp 80 Apache 2.2.3 WebDAV: http.banner: Apache/2.2.3 (Red Hat) http.banner.server: Apache/2.2.3 (Red Hat) MySQL 172.23.202.193 tcp 3306 SSH 172.23.202.193 tcp 22 OpenSSH 4.3 ssh.banner: SSH-2.0-OpenSSH_4.3 ssh.protocol.version: 2.0 Portmapper²⁸⁷⁴ : 172.23.202.193 tcp 111 program-number: 100000 program-version: 2 STATUS:

²⁸⁶⁶ <http://lists.apple.com/archives/security-announce/2009/May/msg00001.html>²⁸⁶⁷ <http://www.securityfocus.com/bid/27409>²⁸⁶⁸ <http://www.us-cert.gov/ncas/alerts/ta09-133a>²⁸⁶⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0456>²⁸⁷⁰ <http://secunia.com/advisories/29348/>²⁸⁷¹ <http://secunia.com/advisories/35074/>²⁸⁷² <http://xforce.iss.net/xforce/xfdb/39893>²⁸⁷³ http://httpd.apache.org/security/vulnerabilities_22.html²⁸⁷⁴ Port mapper poziva udaljene procedure je servis koji mapira RPC programe ka specifičnim portovima i daje tu informaciju klijentskim programima. S obzirom da većina RPC programa nema dobro definisan broj portova, njima se dinamički dodeljuje broj porta kada prvi put budu pokrenuti. Bilo koji klijentski program koji poželi da koristi određeni RPC program najpre stupa u kontakt sa port mapperom da bi odredio port i protokol specifikovanog RPC programa. Nakon toga, klijent koristi tu informaciju da direktno stupi u kontakt sa RPC programom. Neke implementacije port mapera dodatno omogućavaju prolazak komandi ka RPC programima kroz port mapper.

	172.23.202.193 udp 983 program-number: 100024 program-version: 1 172.23.202.193 tcp 986 program-number: 100024 program-version: 1
Spidered Web site	http://172.23.202.193:80 Common Default URLs: <i>Access Error (403)</i> cgi-bin error <i>Successful (200)</i> Icons Guessed URLs <i>Access Error (403)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+ AD4- script+AD4- script+AD4- cgi-bin error <i>Redirect (301)</i> icons small <i>Successful (200)</i> icons ?P=+ADw-script+AD4-alert(42)+ADwscript+ AD4- script+AD4- README small README Linked URLs <i>Access Error (403)</i> <i>Successful (200)</i> icons small

Tabela 76. Linux OS – Pronađeni servisi na IP adresi 172.23.202.194 (2011. godina)

SERVISI	FTP 172.23.202.194 tcp 21 vsFTPD 2.0.5 ftp.banner: 220 (vsFTPD 2.0.5) HTTP 172.23.202.194 tcp 80 Apache 2.2.3 WebDAV: http.banner: Apache/2.2.3 (Red Hat) http.banner.server: Apache/2.2.3 (Red Hat) MySQL 172.23.202.194 tcp 3306 SSH 172.23.202.194 tcp 22 OpenSSH 4.3 ssh.banner: SSH-2.0-OpenSSH_4.3 ssh.protocol.version: 2.0

	Portmapper ²⁸⁷⁵ : 172.23.202.194 tcp 111 program-number: 100000 program-version: 2 STATUS: 172.23.202.194 udp 983 program-number: 100024 program-version: 1 172.23.202.194 tcp 986 program-number: 100024 program-version: 1
Spidered Web site	http://172.23.202.194:80 Common Default URLs: <i>Access Error (403)</i> cgi-bin error <i>Successful (200)</i> Icons Guessed URLs <i>Access Error (403)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+ AD4- script+AD4- script+AD4- cgi-bin error <i>Redirect (301)</i> icons small <i>Successful (200)</i> icons ?P=+ADw-script+AD4-alert(42)+ADwscript+ AD4- script+AD4- README small README Linked URLs <i>Access Error (403)</i> <i>Successful (200)</i> icons small

Tabela 77. Linux OS – Pronađeni servisi na IP adresi 172.23.202.226 (2011. godina)

SERVISI	FTP 172.23.202.226 tcp 21 vsFTPD 2.0.5 ftp.banner: 220 (vsFTPD 2.0.5) HTTP 172.23.202.226 tcp 80 Apache 2.2.3 WebDAV:

²⁸⁷⁵ Port mapper poziva udaljene procedure je servis koji mapira RPC programe ka specifičnim portovima i daje tu informaciju klijentskim programima. S obzirom da većina RPC programa nema dobro definisan broj portova, njima se dinamički dodeljuje broj porta kada prvi put budu pokrenuti. Bilo koji klijentski program koji poželi da koristi određeni RPC program najpre stupa u kontakt sa port mapperom da bi odredio port i protokol specifikovanog RPC programa. Nakon toga, klijent koristi tu informaciju da direktno stupi u kontakt sa RPC programom. Neke implementacije port mapera dodatno omogućavaju prolazak komandi ka RPC programima kroz port mapper.

	http.banner: Apache/2.2.3 (Red Hat) http.banner.server: Apache/2.2.3 (Red Hat) MySQL 172.23.202.226 tcp 3306 SSH 172.23.202.226 tcp 22 OpenSSH 4.3 ssh.banner: SSH-2.0-OpenSSH_4.3 ssh.protocol.version: 2.0 Portmapper²⁸⁷⁶ : 172.23.202.226 tcp 111 program-number: 100000 program-version: 2 STATUS: 172.23.202.226 udp 983 program-number: 100024 program-version: 1 172.23.202.226 tcp 986 program-number: 100024 program-version: 1
Spidered Web site	http://172.23.202.226:80 Common Default URLs: <i>Access Error (403)</i> cgi-bin error <i>Successful (200)</i> Icons Guessed URLs <i>Access Error (403)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+ AD4-script+AD4-script+AD4-cgi-bin error <i>Redirect (301)</i> icons small <i>Successful (200)</i> icons ?P=+ADw-script+AD4-alert(42)+ADwscript+ AD4-script+AD4-README small README Linked URLs <i>Access Error (403)</i> <i>Successful (200)</i> icons small

²⁸⁷⁶ Port mapper pōziva udaljene procedure je servis koji mapira RPC programe ka specifičnim portovima i daje tu informaciju klijentskim programima. S obzirom da većina RPC programa nema dobro definisan broj portova, njima se dinamički dodeljuje broj porta kada prvi put budu pokrenuti. Bilo koji klijentski program koji poželi da koristi određeni RPC program najpre stupa u kontakt sa port mapperom da bi odredio port i protokol specifikovanog RPC programa. Nakon toga, klijent koristi tu informaciju da direktno stupi u kontakt sa RPC programom. Neke implementacije port mapera dodatno omogućavaju prolazak komandi ka RPC programima kroz port mapper.

Tabela 78. Linux OS – Pronađeni servisi na IP adresi 172.23.202.227 (2011. godina)

SERVISI	FTP 172.23.202.227 tcp 21 vsFTPd 2.0.5 ftp.banner: 220 (vsFTPd 2.0.5) HTTP 172.23.202.227 tcp 80 Apache 2.2.3 WebDAV: http.banner: Apache/2.2.3 (Red Hat) http.banner.server: Apache/2.2.3 (Red Hat) MySQL 172.23.202.227 tcp 3306 SSH 172.23.202.227 tcp 22 OpenSSH 4.3 ssh.banner: SSH-2.0-OpenSSH_4.3 ssh.protocol.version: 2.0 Portmapper²⁸⁷⁷ : 172.23.202.227 tcp 111 program-number: 100000 program-version: 2 STATUS: 172.23.202.227 udp 983 program-number: 100024 program-version: 1 172.23.202.227 tcp 986 program-number: 100024 program-version: 1
Spidered Web site	http://172.23.202.227:80 Common Default URLs: <i>Access Error (403)</i> cgi-bin error <i>Successful (200)</i> Icons Guessed URLs <i>Access Error (403)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-script+AD4-cgi-binerrorRedirect (301)iconssmallSuccessful (200)icons?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-READMEsmallREADME

²⁸⁷⁷ Port mapper poziva udaljene procedure je servis koji mapira RPC programe ka specifičnim portovima i daje tu informaciju klijentskim programima. S obzirom da većina RPC programa nema dobro definisan broj portova, njima se dinamički dodeljuje broj porta kada prvi put budu pokrenuti. Bilo koji klijentski program koji poželi da koristi određeni RPC program najpre stupa u kontakt sa port mapperom da bi odredio port i protokol specifikovanog RPC programa. Nakon toga, klijent koristi tu informaciju da direktno stupi u kontakt sa RPC programom. Neke implementacije port mapera dodatno omogućavaju prolazak komandi ka RPC programima kroz port mapper.

	Linked URLs Access Error (403) Successful (200) icons small

Tabela 79. Linux OS sa IP adresama 172.23.202.195, 172.23.202.196, 172.23.202.221, 172.23.202.222 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.195		OS: Red Hat Enterprise Linux 5.6 x64, redhat56entx64			45
IP adresa: 172.23.202.196		OS: Centos 5.6 x64, centos56x64			45
IP adresa: 172.23.202.221		OS: Centos 5.6 x86, centos56x86			45
IP adresa: 172.23.202.222		OS: Red Hat Enterprise Linux 5.6 x86, redhat56entx86			45
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Apache httpd mod_isapi module unload flaw (CVE-2010-0425) (apache-httpd-2_2_x-mod_isapi-moduleunload-flaw-cve-2010-0425)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 U modulu mod_isapi je pronađen propust, koji će pokušati da ukloni ISAPI dll kada naiđe na greške. To može ostaviti povratne pozive u nedefinisano stanje greške i kao posledica može da se javi segmentation fault. Na Windows platformama koje koriste mod_isapi, udaljeni napadač bi mogao da pošalje zlonameran zahtev da pokrene ovaj problem, a kako win32 MPM pokreće samo jedan proces, to bi kao ishod imalo odbijanje servisa i potencijalno dozvolilo da se pokrene proizvoljan kôd. Zahvaljujući Brett Gervasoni-ju ovaj problem je prijavljen i za njega je predložena zakrpa.	BID 38494²⁸⁷⁸ CERT-VN 280613²⁸⁷⁹ CVE CVE-2010-0425²⁸⁸⁰ OVAL OVAL8439²⁸⁸¹ SECUNIA 38978²⁸⁸² SECUNIA 39628²⁸⁸³ URL 1²⁸⁸⁴ XF apache-http-modisapi-ocp-undefined(56624)²⁸⁸⁵	Kritičan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz
2.	Apache httpd APR apr_palloc heap overflow (CVE-2009-2412) (http-apache-apr_palloc-heap-overflow)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 U modulu apr_palloc() je pronađen propust u sklopu APR-a, koji može prouzrokovati velika preopterećenja u	APPLE APPLE-SA-2009-11-09²⁸⁸⁶ BID 35949²⁸⁸⁷ CVE CVE-2009-2412²⁸⁸⁸ OSVDB 56765²⁸⁸⁹ OSVDB 56766²⁸⁹⁰ OVAL OVAL8394²⁸⁹¹	Kritičan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.13.tar.gz

²⁸⁷⁸ <http://www.securityfocus.com/bid/38494>

²⁸⁷⁹ <http://www.kb.cert.org/vuls/id/280613>

²⁸⁸⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0425>

²⁸⁸¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8439>

²⁸⁸² <http://secunia.com/advisories/38978/>

²⁸⁸³ <http://secunia.com/advisories/39628/>

²⁸⁸⁴ http://httpd.apache.org/security/vulnerabilities_22.html

²⁸⁸⁵ <http://xforce.iss.net/xforce/xfdb/56624>

²⁸⁸⁶ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>

²⁸⁸⁷ <http://www.securityfocus.com/bid/35949>

²⁸⁸⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2412>

²⁸⁸⁹ <http://osvdb.org/56765>

²⁸⁹⁰ <http://osvdb.org/56766>

		programima koji pokušaju da kontrolišu <code>apr_palloc()</code> veličinu zadate od strane korisnika. Sam Apache HTTP server ne dopušta prolaz ka ovoj funkciji neproverenim veličinama koje zadaje korisnik, tako da se on može pokrenuti samo preko neke druge aplikacije koja koristi <code>apr_palloc()</code> na ranjiv način.	OVAL OVAL9958²⁸⁹² SECUNIA 36138²⁸⁹³ SECUNIA 36140²⁸⁹⁴ SECUNIA 36166²⁸⁹⁵ SECUNIA 36233²⁸⁹⁶ SECUNIA 37152²⁸⁹⁷ SECUNIA 37221²⁸⁹⁸ SUSE SA:2009:050²⁸⁹⁹ URL1²⁹⁰⁰		
3.	Apache httpd mod_proxy_ftp FTP command injection (CVE-2009-3095) (apache-httpd-2_2_xmod_proxy_ftp-ftp-command-injection-cve-2009-3095)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 U modulu <code>mod_proxy_ftp</code> je pronađen propust. U reverznoj proxy konfiguraciji, udaljeni napadač bi mogao da iskoristi ovaj defekt da zaobiđe uobičajenu zabranu pristupa tako što bi kreirao pažljivo izrađen HTTP Authorization heder, koji omogućava napadaču da šalje proizvoljne komande FTP serveru.	APPLE APPLE-SA-2010-03-29²⁹⁰¹ CVE CVE-2009-3095²⁹⁰² DEBIAN DSA-1934²⁹⁰³ OVAL OVAL8662²⁹⁰⁴ OVAL OVAL9363²⁹⁰⁵ SECUNIA 37152²⁹⁰⁶ SUSE SUSE-SA:2009:050²⁹⁰⁷ URL1²⁹⁰⁸	Kritičan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.gz
4.	Apache httpd APR-util XML DoS (CVE-2009-1955) (http-apache-apr-util-xml-dos)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Ranjivost na DOS napad otkrivena je u sklopu kopije kompleta APR-util library Extensible Markup Language (XML) prevodioca (eng. parser). Udaljeni napadač bi mogao da kreira posebno izrađen XML dokument koji bi prouzrokovao ogromno zauzeće memorije kada ga procesira XML decoding engine.	APPLE APPLE-SA-2009-11-09²⁹⁰⁹ BID 35253²⁹¹⁰ CVE CVE-2009-1955²⁹¹¹ DEBIAN DSA-1812²⁹¹² OVAL OVAL10270²⁹¹³ REDHAT RHSA-2009:1107²⁹¹⁴ REDHAT RHSA-2009:1108²⁹¹⁵ SECUNIA 34724²⁹¹⁶ SECUNIA 35284²⁹¹⁷ SECUNIA 35360²⁹¹⁸ SECUNIA 35395²⁹¹⁹ SECUNIA 35444²⁹²⁰	Kritičan	Apache >= 2.2 and < 2.3 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

²⁸⁹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8394>²⁸⁹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9958>²⁸⁹³ <http://secunia.com/advisories/36138/>²⁸⁹⁴ <http://secunia.com/advisories/36140/>²⁸⁹⁵ <http://secunia.com/advisories/36166/>²⁸⁹⁶ <http://secunia.com/advisories/36233/>²⁸⁹⁷ <http://secunia.com/advisories/37152/>²⁸⁹⁸ <http://secunia.com/advisories/37221/>²⁸⁹⁹ <https://www.suse.com/support/security/advisories/>²⁹⁰⁰ http://httpd.apache.org/security/vulnerabilities_22.html²⁹⁰¹ <http://lists.apple.com/archives/security-announce/2010/Mar/msg00001.html>²⁹⁰² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3095>²⁹⁰³ <http://www.debian.org/security/DSA-/DSA-1934>²⁹⁰⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8662>²⁹⁰⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9363>²⁹⁰⁶ <http://secunia.com/advisories/37152/>²⁹⁰⁷ <https://www.suse.com/support/security/advisories/>²⁹⁰⁸ http://httpd.apache.org/security/vulnerabilities_22.html²⁹⁰⁹ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>²⁹¹⁰ <http://www.securityfocus.com/bid/35253>²⁹¹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1955>²⁹¹² <http://lists.debian.org/debian-security-announce/2009/msg00124.html>²⁹¹³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10270>²⁹¹⁴ <http://rhn.redhat.com/errata/RHSA-2009-1107.html>²⁹¹⁵ <http://rhn.redhat.com/errata/RHSA-2009-1108.html>²⁹¹⁶ <http://secunia.com/advisories/34724/>²⁹¹⁷ <http://secunia.com/advisories/35284/>²⁹¹⁸ <http://secunia.com/advisories/35360/>²⁹¹⁹ <http://secunia.com/advisories/35395/>²⁹²⁰ <http://secunia.com/advisories/35444/>

			SECUNIA 35487 ²⁹²¹ SECUNIA 35565 ²⁹²² SECUNIA 35710 ²⁹²³ SECUNIA 35797 ²⁹²⁴ SECUNIA 35843 ²⁹²⁵ SECUNIA 36473 ²⁹²⁶ SECUNIA 37221 ²⁹²⁷ URL1 ²⁹²⁸		
5.	OpenSSH X11 Cookie Local Authentication Bypass Vulnerability (openssh-x11-cookie-auth-bypass)	172.23.202.195:22 172.23.202.196:22 172.23.202.221:22 172.23.202.222:22 Pre verzije 4.7, OpenSSH nije adekvatno radio kada nepoverljivi kolačić (cookie) nije mogao biti kreiran. Umesto njega, koristi se poverljivi X11 kolačić. To omogućava napadačima da naruše ciljanu polisu i dobiju privilegije korisnika, što kao posledicu servis tretira klijenta X kao poverljivog.	CVE CVE-2007-4752 ²⁹²⁹ XFD 25628 ²⁹³⁰ XF openssh-x11cookie-privilege-escalation(36637) ²⁹³¹	Kritičan	Uraditi download a zatim instalirati: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-4.7p1.tar.gz Verzija 4.7 OpenSSH-a je puštena u promet 4. septembra 2007.
6	Apache httpd mod_deflate DoS (CVE-2009-1891) (http://apache-mod_deflate-dos)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Ranjivost na DOS napad otkrivena je u modulu mod_deflate. Ovaj modul nastavlja da kompresuje velike fajlove sve dok se kompresija ne završi, čak i kada je mrežna konekcija koja je zahtevala taj sadržaj prekinuta pre nego što je kompresija završena. To dovodi do toga da mod_deflate zauzima veliku količinu CPU-a ukoliko je mod_deflate bio omogućen za velike fajlove.	APPLE APPLE-SA-2009-11-09 ²⁹³² CVE CVE-2009-1891 ²⁹³³ DEBIAN DSA-1834 ²⁹³⁴ OSVDB 55782 ²⁹³⁵ OVAL OVAL8632 ²⁹³⁶ OVAL OVAL9248 ²⁹³⁷ REDHAT RHSA-2009:1148 ²⁹³⁸ REDHAT RHSA-2009:1156 ²⁹³⁹ SECUNIA 35721 ²⁹⁴⁰ SECUNIA 35781 ²⁹⁴¹ SECUNIA 35793 ²⁹⁴² SECUNIA 35865 ²⁹⁴³ SECUNIA 37152 ²⁹⁴⁴ SECUNIA 37221 ²⁹⁴⁵ SUSE SA:2009:050 ²⁹⁴⁶ URL1 ²⁹⁴⁷	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

²⁹²¹ <http://secunia.com/advisories/35487/>²⁹²² <http://secunia.com/advisories/35565/>²⁹²³ <http://secunia.com/advisories/35710/>²⁹²⁴ <http://secunia.com/advisories/35797/>²⁹²⁵ <http://secunia.com/advisories/35843/>²⁹²⁶ <http://secunia.com/advisories/36473/>²⁹²⁷ <http://secunia.com/advisories/37221/>²⁹²⁸ http://httpd.apache.org/security/vulnerabilities_22.html²⁹²⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-4752>²⁹³⁰ <http://www.securityfocus.com/bid/25628>²⁹³¹ <http://xforce.iss.net/xforce/xfdb/36637>²⁹³² <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>²⁹³³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1891>²⁹³⁴ <http://www.debian.org/security/2009/dsa-1834>²⁹³⁵ <http://osvdb.org/55782>²⁹³⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8632>²⁹³⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9248>²⁹³⁸ <http://rhn.redhat.com/errata/RHSA-2009-1148.html>²⁹³⁹ <http://rhn.redhat.com/errata/RHSA-2009-1156.html>²⁹⁴⁰ <http://secunia.com/advisories/35721/>²⁹⁴¹ <http://secunia.com/advisories/35781/>²⁹⁴² <http://secunia.com/advisories/35793/>²⁹⁴³ <http://secunia.com/advisories/35865/>²⁹⁴⁴ <http://secunia.com/advisories/37152/>²⁹⁴⁵ <http://secunia.com/advisories/37221/>²⁹⁴⁶ <https://www.suse.com/support/security/advisories/>

7.	Apache httpd mod_proxy reverse proxy DoS (CVE-2009-1890) (http-apache-mod_proxy-reverse-proxy-dos)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja prisustva mod_proxy modula. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy. Zlonamerni napadač bi mogao da iskoristi ovaj propust na takav način da primora proxy proces da zauzme veliku količinu CPU vremena.	APPLE APPLE-SA-2009-11-09 ²⁹⁴⁸ CVE CVE-2009-1890 ²⁹⁴⁹ DEBIAN DSA-1834 ²⁹⁵⁰ OSVDB 55553 ²⁹⁵¹ OVAL OVAL8616 ²⁹⁵² OVAL OVAL9403 ²⁹⁵³ REDHAT RHSA-2009:1148 ²⁹⁵⁴ REDHAT RHSA-2009:1156 ²⁹⁵⁵ SECUNIA 35691 ²⁹⁵⁶ SECUNIA 35721 ²⁹⁵⁷ SECUNIA 35793 ²⁹⁵⁸ SECUNIA 35865 ²⁹⁵⁹ SECUNIA 37152 ²⁹⁶⁰ SECUNIA 37221 ²⁹⁶¹ SUSE SA:2009:050 ²⁹⁶² URL1 2963	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz
8.	Apache httpd APR-util off-by-one overflow (CVE-2009-1956) (http-apache-apr-util-off-by-one-overflow)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Propust prepunjavanja bafera "off-by-one" je otkriven u načinu na koji APR-util library komplet procesira promenljivu listu argumenata. Napadač bi mogao da kreira posebno izrađen string kao input za već formatiranu output rutu konverzije, koja bi, na velikim platformama, potencijalno mogla da dovede do otkrivanja povreljivih informacija ili do odbijanja servisa.	APPLE APPLE-SA-2009-11-09 ²⁹⁶⁴ BID 35251 ²⁹⁶⁵ CVE CVE-2009-1956 ²⁹⁶⁶ OVAL OVAL11567 ²⁹⁶⁷ REDHAT RHSA-2009:1107 ²⁹⁶⁸ REDHAT RHSA-2009:1108 ²⁹⁶⁹ SECUNIA 34724 ²⁹⁷⁰ SECUNIA 35284 ²⁹⁷¹ SECUNIA 35395 ²⁹⁷² SECUNIA 35487 ²⁹⁷³ SECUNIA 35565 ²⁹⁷⁴ SECUNIA 35710 ²⁹⁷⁵ SECUNIA 35797 ²⁹⁷⁶ SECUNIA 35843 ²⁹⁷⁷ SECUNIA 37221 ²⁹⁷⁸	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

²⁹⁴⁷ http://httpd.apache.org/security/vulnerabilities_22.html
²⁹⁴⁸ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>
²⁹⁴⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1890>
²⁹⁵⁰ <http://www.debian.org/security/2009/dsa-1834>
²⁹⁵¹ <http://osvdb.org/55553>
²⁹⁵² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8616>
²⁹⁵³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9403>
²⁹⁵⁴ <http://rhn.redhat.com/errata/RHSA-2009-1148.html>
²⁹⁵⁵ <http://rhn.redhat.com/errata/RHSA-2009-1156.html>
²⁹⁵⁶ <http://secunia.com/advisories/35691/>
²⁹⁵⁷ <http://secunia.com/advisories/35721/>
²⁹⁵⁸ <http://secunia.com/advisories/35793/>
²⁹⁵⁹ <http://secunia.com/advisories/35865/>
²⁹⁶⁰ <http://secunia.com/advisories/37152/>
²⁹⁶¹ <http://secunia.com/advisories/37221/>
²⁹⁶² <https://www.suse.com/support/security/advisories/>
²⁹⁶³ http://httpd.apache.org/security/vulnerabilities_22.html
²⁹⁶⁴ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>
²⁹⁶⁵ <http://www.securityfocus.com/bid/35251>
²⁹⁶⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1956>
²⁹⁶⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11567>
²⁹⁶⁸ <http://rhn.redhat.com/errata/RHSA-2009-1107.html>
²⁹⁶⁹ <http://rhn.redhat.com/errata/RHSA-2009-1108.html>
²⁹⁷⁰ <http://secunia.com/advisories/34724/>
²⁹⁷¹ <http://secunia.com/advisories/35284/>
²⁹⁷² <http://secunia.com/advisories/35395/>
²⁹⁷³ <http://secunia.com/advisories/35487/>
²⁹⁷⁴ <http://secunia.com/advisories/35565/>
²⁹⁷⁵ <http://secunia.com/advisories/35710/>
²⁹⁷⁶ <http://secunia.com/advisories/35797/>
²⁹⁷⁷ <http://secunia.com/advisories/35843/>
²⁹⁷⁸ <http://secunia.com/advisories/37221/>

9.	OpenSSH X11 Forwarding Information Disclosure Vulnerability (ssh-openssh-x11-fowarding-info-disclosure)	172.23.202.195:22 172.23.202.196:22 172.23.202.221:22 172.23.202.222:22 Određene verzije OpenSSH-a ne povezuju ispravno TCP portove na lokalnom IPv6 interfejsu ako se koriste zahtevani IPv4 portovi. Ovo bi loklanom napadaču moglo da omogući da preuzme prosleđenu X11 sesiju putem otvaranja TCP port-a 6010 (IPv4).	URL1²⁹⁷⁹ BID 28444²⁹⁸⁰ CVE CVE-2008-1483²⁹⁸¹ SECUNIA 29522²⁹⁸² URL1²⁹⁸³	Ozbiljan	Nadograditi na najnoviju verziju OpenSSH-a. Najnovija verzija OpenSSH-a je 5.2 (OpenBSD izvor) i 5.2p1 (prenosivi izvor).
10.	Apache httpd expat DoS (CVE-2009-3560) (apache-httpd-2_2_x-cve-2009-3560)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u mogućnost da dovede do toga da Apache parsira nepoverljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	BID 37203²⁹⁸⁴ CVE CVE-2009-3560²⁹⁸⁵ DEBIAN DSA-1953²⁹⁸⁶ OVAL OVAL10613²⁹⁸⁷ OVAL OVAL6883²⁹⁸⁸ SECUNIA 37537²⁹⁸⁹ SECUNIA 38231²⁹⁹⁰ SECUNIA 38794²⁹⁹¹ SECUNIA 38832²⁹⁹² SECUNIA 38834²⁹⁹³ SECUNIA 39478²⁹⁹⁴ SECUNIA 41701²⁹⁹⁵ SECUNIA 43300²⁹⁹⁶ URL1²⁹⁹⁷	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
11.	Apache httpd expat DoS (CVE-2009-3720) (apache-httpd-2_2_x-cve-2009-3720)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osjetljiv na ovu ranjivost SAMO ako je napadač u mogućnosti da dovede do toga da Apache parsira nepoverljiv XML	CVE CVE-2009-3720²⁹⁹⁸ OVAL OVAL11019²⁹⁹⁹ OVAL OVAL7112³⁰⁰⁰ REDHAT RHSA-2010:0002³⁰⁰¹ SECUNIA 37324³⁰⁰² SECUNIA 37537³⁰⁰³ SECUNIA 37925³⁰⁰⁴	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz

²⁹⁷⁹ http://httpd.apache.org/security/vulnerabilities_22.html²⁹⁸⁰ <http://www.securityfocus.com/bid/28444>²⁹⁸¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-1483>²⁹⁸² <http://secunia.com/advisories/29522/>²⁹⁸³ <http://www.openssh.org/txt/release-5.0>²⁹⁸⁴ <http://www.securityfocus.com/bid/37203>²⁹⁸⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3560>²⁹⁸⁶ <http://www.debian.org/security/2009/dsa-1953>²⁹⁸⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10613>²⁹⁸⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6883>²⁹⁸⁹ <http://secunia.com/advisories/37537/>²⁹⁹⁰ <http://secunia.com/advisories/38231/>²⁹⁹¹ <http://secunia.com/advisories/38794/>²⁹⁹² <http://secunia.com/advisories/38832/>²⁹⁹³ <http://secunia.com/advisories/38834/>²⁹⁹⁴ <http://secunia.com/advisories/39478/>²⁹⁹⁵ <http://secunia.com/advisories/41701/>²⁹⁹⁶ <http://secunia.com/advisories/43300/>²⁹⁹⁷ http://httpd.apache.org/security/vulnerabilities_22.html²⁹⁹⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3720>²⁹⁹⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11019>³⁰⁰⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7112>³⁰⁰¹ <http://rhn.redhat.com/errata/RHSA-2010-0002.html>³⁰⁰² <http://secunia.com/advisories/37324/>³⁰⁰³ <http://secunia.com/advisories/37537/>³⁰⁰⁴ <http://secunia.com/advisories/37925/>

		dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	SECUNIA 38050 ³⁰⁰⁵ SECUNIA 38231 ³⁰⁰⁶ SECUNIA 38794 ³⁰⁰⁷ SECUNIA 38832 ³⁰⁰⁸ SECUNIA 38834 ³⁰⁰⁹ SECUNIA 39478 ³⁰¹⁰ SECUNIA 41701 ³⁰¹¹ SECUNIA 43300 ³⁰¹² URL1 ³⁰¹³		
12.	Apache httpd apr_bridage_split_line DoS (CVE-2010-1623) (apache-httpd-2_2_x-cve-2010-1623)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako Apache procesira ne-SSL zahteve. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_brigade_split_line() u sklopu APR-util library, koji se koristi da procesira ne-SSL zahteve. Udaljeni napadač bi mogao da šalje zahteve, pažljivo izrađujući tajming za pojedinačne bajtove, što bi polako zauzimalo memoriju i potencijalno dovelo do odbijanja servisa.	BID 43673 ³⁰¹⁴ CVE CVE-2010-1623 ³⁰¹⁵ REDHAT RHSA-2010:0950 ³⁰¹⁶ SECUNIA 41701 ³⁰¹⁷ SECUNIA 42015 ³⁰¹⁸ SECUNIA 42361 ³⁰¹⁹ SECUNIA 42367 ³⁰²⁰ SECUNIA 42403 ³⁰²¹ SECUNIA 42537 ³⁰²² SECUNIA 43211 ³⁰²³ SECUNIA 43285 ³⁰²⁴ URL1 ³⁰²⁵	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
13.	Apache httpd mod_cache and mod_dav DoS (CVE-2010-1452) (apache-httpd-2_2_x-mod_cache-andmod_dav-dos-cve-2010-1452)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako web server izvršava jedan od sledećih modula: mod_cache, mod_dav. Pregledajte konfiguraciju vašeg web servera radi validacije.	APPLE APPLE-SA-2011-03-21 ³⁰²⁶ CVE CVE-2010-1452 ³⁰²⁷ OVAL OVAL11683 ³⁰²⁸ REDHAT RHSA-2010:0659 ³⁰²⁹ SECUNIA 42367 ³⁰³⁰ URL1 ³⁰³¹	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.16.tar.gz

³⁰⁰⁵ <http://secunia.com/advisories/38050/>³⁰⁰⁶ <http://secunia.com/advisories/38231/>³⁰⁰⁷ <http://secunia.com/advisories/38794/>³⁰⁰⁸ <http://secunia.com/advisories/38832/>³⁰⁰⁹ <http://secunia.com/advisories/38834/>³⁰¹⁰ <http://secunia.com/advisories/39478/>³⁰¹¹ <http://secunia.com/advisories/41701/>³⁰¹² <http://secunia.com/advisories/43300/>³⁰¹³ http://httpd.apache.org/security/vulnerabilities_22.html³⁰¹⁴ <http://www.securityfocus.com/bid/43673>³⁰¹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1623>³⁰¹⁶ <http://rhn.redhat.com/errata/RHSA-2010-0950.html>³⁰¹⁷ <http://secunia.com/advisories/41701/>³⁰¹⁸ <http://secunia.com/advisories/42015/>³⁰¹⁹ <http://secunia.com/advisories/42361/>³⁰²⁰ <http://secunia.com/advisories/42367/>³⁰²¹ <http://secunia.com/advisories/42403/>³⁰²² <http://secunia.com/advisories/42537/>³⁰²³ <http://secunia.com/advisories/43211/>³⁰²⁴ <http://secunia.com/advisories/43285/>³⁰²⁵ http://httpd.apache.org/security/vulnerabilities_22.html³⁰²⁶ <http://lists.apple.com/archives/security-announce/2011/Mar/msg00006.html>³⁰²⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1452>³⁰²⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11683>³⁰²⁹ <http://rhn.redhat.com/errata/RHSA-2010-0659.html>³⁰³⁰ <http://secunia.com/advisories/42367/>³⁰³¹ http://httpd.apache.org/security/vulnerabilities_22.html

		Propust je otkriven u obradi zahteva od strane mod_cache i mod_dav. Zlonameran udaljeni napadač bi mogao da pošalje pažljivo izrađen zahtev i prouzrokuje da httpd child proces krahira. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM. Ovaj problem se dalje može ublažiti ako na mod_dav samo utiču zahtevi za koje postoji mogućnost autentifikovanja, a mod_cache je pod uticajem samo ako se koristi neuobičajena „CacheIgnoreURLSessionIdentifiers“ direktiva, uvedena u verziji 2.2.14. Ovaj problem je prijavio Mark Drayton.			
14.	Apache httpd mod_proxy crash (CVE-2007-3847) (apache-httpd-2_2_x-mod_proxy-crash-cve-2007-3847)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Propust je otkriven u Apache-ovom HTTP Server modulu mod_proxy. Na sajtovim na kojima je konfigurisan "reverse proxy", udaljeni napadač bi mogao da pošalje pažljivo izrađen zahtev koji bi mogao da prouzrokuje pad child procesa Apache-a koji taj zahtev obrađuje. Na sajtovim na kojima je konfigurisan "forward proxy", napadač bi mogao da prouzrokuje sličan pad ako bi korisnik bio naveden da poseti zlonameran sajt koji koristi taj proksi. Ovo bi moglo da dovede do odbijanja servisa ako se koristi threaded MPM.	APPLE APPLE-SA-2008-03-18³⁰³² APPLE APPLE-SA-2008-05-28³⁰³³ BID 25489³⁰³⁴ CERT TA08-150A³⁰³⁵ CVE CVE-2007-3847³⁰³⁶ OVAL OVAL10525³⁰³⁷ REDHAT RHSA-2007-0746³⁰³⁸ REDHAT RHSA-2007-0747³⁰³⁹ REDHAT RHSA-2007-0911³⁰⁴⁰ REDHAT RHSA-2008-0005³⁰⁴¹ SECUNIA 26636³⁰⁴² SECUNIA 26722³⁰⁴³ SECUNIA 26790³⁰⁴⁴ SECUNIA 26842³⁰⁴⁵ SECUNIA 26952³⁰⁴⁶ SECUNIA 26993³⁰⁴⁷ SECUNIA 27209³⁰⁴⁸ SECUNIA 27563³⁰⁴⁹ SECUNIA 27593³⁰⁵⁰ SECUNIA 27732³⁰⁵¹ SECUNIA 27882³⁰⁵² SECUNIA 27971³⁰⁵³ SECUNIA 28467³⁰⁵⁴	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz

³⁰³² <http://lists.apple.com/archives/security-announce/2008/Mar/msg00000.html>

³⁰³³ <http://lists.apple.com/archives/security-announce/2008/May/msg00001.html>

³⁰³⁴ <http://www.securityfocus.com/bid/25489> pristupljeno 11.12.2011

³⁰³⁵ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>

³⁰³⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3847>

³⁰³⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10525>

³⁰³⁸ <http://rhn.redhat.com/errata/RHSA-2007-0746.html>

³⁰³⁹ <http://rhn.redhat.com/errata/RHSA-2007-0747.html>

³⁰⁴⁰ <http://rhn.redhat.com/errata/RHSA-2007-0911.html>

³⁰⁴¹ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>

³⁰⁴² <http://secunia.com/advisories/26636/>

³⁰⁴³ <http://secunia.com/advisories/26722/>

³⁰⁴⁴ <http://secunia.com/advisories/26790/>

³⁰⁴⁵ <http://secunia.com/advisories/26842/>

³⁰⁴⁶ <http://secunia.com/advisories/26952/>

³⁰⁴⁷ <http://secunia.com/advisories/26993/>

³⁰⁴⁸ <http://secunia.com/advisories/27209/>

³⁰⁴⁹ <http://secunia.com/advisories/27563/>

³⁰⁵⁰ <http://secunia.com/advisories/27593/>

³⁰⁵¹ <http://secunia.com/advisories/27732/>

³⁰⁵² <http://secunia.com/advisories/27882/>

³⁰⁵³ <http://secunia.com/advisories/27971/>

			SECUNIA 28606 ³⁰⁵⁵ SECUNIA 28749 ³⁰⁵⁶ SECUNIA 28922 ³⁰⁵⁷ SECUNIA 29420 ³⁰⁵⁸ SECUNIA 30430 ³⁰⁵⁹ SUSE SUSE- SA:2007:061 ³⁰⁶⁰ URL1 ³⁰⁶¹		
15.	Apache httpd mod_proxy_http DoS (CVE-2008-2364) (apache-httpd-2_2_x- mod_proxy_http-dos- cve-2008- 2364)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Otkriven je propust prilikom obrade prekomernih privremenih odgovora sa glavnog servera kada se koristi mod_proxy_http. Udaljeni napadač bi mogao da izazove odbijanje servisa ili preopterećenje memorije.	BID 29653 ³⁰⁶² BID 31681 ³⁰⁶³ CVE CVE-2008-2364 ³⁰⁶⁴ OVAL OVAL11713 ³⁰⁶⁵ OVAL OVAL6084 ³⁰⁶⁶ OVAL OVAL9577 ³⁰⁶⁷ REDHAT RHSA- 2008:0966 ³⁰⁶⁸ REDHAT RHSA- 2008:0967 ³⁰⁶⁹ SECUNIA 30621 ³⁰⁷⁰ SECUNIA 31026 ³⁰⁷¹ SECUNIA 31404 ³⁰⁷² SECUNIA 31416 ³⁰⁷³ SECUNIA 31651 ³⁰⁷⁴ SECUNIA 31904 ³⁰⁷⁵ SECUNIA 32222 ³⁰⁷⁶ SECUNIA 32685 ³⁰⁷⁷ SECUNIA 32838 ³⁰⁷⁸ SECUNIA 33156 ³⁰⁷⁹ SECUNIA 33797 ³⁰⁸⁰ SECUNIA 34219 ³⁰⁸¹ SECUNIA 34259 ³⁰⁸² SECUNIA 34418 ³⁰⁸³ XF apache-modproxy- module-dos(42987) ³⁰⁸⁴ URL1 ³⁰⁸⁵	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dis t/httpd/httpd-2.2.9.tar.gz

³⁰⁵⁴ <http://secunia.com/advisories/28467/>³⁰⁵⁵ <http://secunia.com/advisories/28606/>³⁰⁵⁶ <http://secunia.com/advisories/28749/>³⁰⁵⁷ <http://secunia.com/advisories/28922/>³⁰⁵⁸ <http://secunia.com/advisories/29420/>³⁰⁵⁹ <http://secunia.com/advisories/30430/>³⁰⁶⁰ <https://www.suse.com/support/security/advisories/>³⁰⁶¹ http://httpd.apache.org/security/vulnerabilities_22.html³⁰⁶² <http://www.securityfocus.com/bid/29653>³⁰⁶³ <http://www.securityfocus.com/bid/31681>³⁰⁶⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-2364>³⁰⁶⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11713>³⁰⁶⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6084>³⁰⁶⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9577>³⁰⁶⁸ <http://rhn.redhat.com/errata/RHSA-2008-0966.html>³⁰⁶⁹ <http://rhn.redhat.com/errata/RHSA-2008-0967.html>³⁰⁷⁰ <http://secunia.com/advisories/30621/>³⁰⁷¹ <http://secunia.com/advisories/31026/>³⁰⁷² <http://secunia.com/advisories/31404/>³⁰⁷³ <http://secunia.com/advisories/31416/>³⁰⁷⁴ <http://secunia.com/advisories/31651/>³⁰⁷⁵ <http://secunia.com/advisories/31904/>³⁰⁷⁶ <http://secunia.com/advisories/32222/>³⁰⁷⁷ <http://secunia.com/advisories/32685/>³⁰⁷⁸ <http://secunia.com/advisories/32838/>³⁰⁷⁹ <http://secunia.com/advisories/33156/>³⁰⁸⁰ <http://secunia.com/advisories/33797/>³⁰⁸¹ <http://secunia.com/advisories/34219/>³⁰⁸² <http://secunia.com/advisories/34259/>³⁰⁸³ <http://secunia.com/advisories/34418/>³⁰⁸⁴ <http://xforce.iss.net/xforce/xfdb/42987>³⁰⁸⁵ http://httpd.apache.org/security/vulnerabilities_20.html

16.	Apache httpd Signals to arbitrary processes (CVE-2007-3304) (apache-httpd-2_2_x-signals-to-arbitraryprocesses-cve-2007-3304)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Pre nego što mu je poslao signale, Apache HTTP server nije overio da li proces potiče od Apache-ovog child procesa. Lokalni napadač koji ima mogućnost da pokreće skripte na HTTP serveru, mogao bi da manipuliše semaforom za signale i da prouzrokuje okončanje proizvoljnog procesa, što bi moglo da dovede do odbijanja servisa.	BID 24215 ³⁰⁸⁶ CVE CVE-2007-3304 ³⁰⁸⁷ OVAL OVAL11589 ³⁰⁸⁸ REDHAT RHSA-2007:0532 ³⁰⁸⁹ REDHAT RHSA-2007:0556 ³⁰⁹⁰ REDHAT RHSA-2007:0557 ³⁰⁹¹ REDHAT RHSA-2007:0662 ³⁰⁹² REDHAT RHSA-2008:0261 ³⁰⁹³ SECUNIA 25827 ³⁰⁹⁴ SECUNIA 25830 ³⁰⁹⁵ SECUNIA 25920 ³⁰⁹⁶ SECUNIA 26211 ³⁰⁹⁷ SECUNIA 26273 ³⁰⁹⁸ SECUNIA 26443 ³⁰⁹⁹ SECUNIA 26508 ³¹⁰⁰ SECUNIA 26611 ³¹⁰¹ SECUNIA 26759 ³¹⁰² SECUNIA 26790 ³¹⁰³ SECUNIA 26822 ³¹⁰⁴ SECUNIA 26842 ³¹⁰⁵ SECUNIA 26993 ³¹⁰⁶ SECUNIA 27121 ³¹⁰⁷ SECUNIA 27209 ³¹⁰⁸ SECUNIA 27563 ³¹⁰⁹ SECUNIA 27732 ³¹¹⁰ SECUNIA 28212 ³¹¹¹ SECUNIA 28224 ³¹¹² SECUNIA 28606 ³¹¹³ SGI 20070701-01-P ³¹¹⁴ SUSE SUSE-SA:2007:061 ³¹¹⁵ XF apache-child-process-dos(35095) ³¹¹⁶ URL1 ³¹¹⁷	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz

³⁰⁸⁶ <http://www.securityfocus.com/bid/24215>³⁰⁸⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3304>³⁰⁸⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11589>³⁰⁸⁹ <http://rhn.redhat.com/errata/RHSA-2007-0532.html>³⁰⁹⁰ <http://rhn.redhat.com/errata/RHSA-2007-0556.html>³⁰⁹¹ <http://rhn.redhat.com/errata/RHSA-2007-0557.html>³⁰⁹² <http://rhn.redhat.com/errata/RHSA-2007-0662.html>³⁰⁹³ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>³⁰⁹⁴ <http://secunia.com/advisories/25827/>³⁰⁹⁵ <http://secunia.com/advisories/25830/>³⁰⁹⁶ <http://secunia.com/advisories/25920/>³⁰⁹⁷ <http://secunia.com/advisories/26211/>³⁰⁹⁸ <http://secunia.com/advisories/26273/>³⁰⁹⁹ <http://secunia.com/advisories/26443/>³¹⁰⁰ <http://secunia.com/advisories/26508/>³¹⁰¹ <http://secunia.com/advisories/26611/>³¹⁰² <http://secunia.com/advisories/26759/>³¹⁰³ <http://secunia.com/advisories/26790/>³¹⁰⁴ <http://secunia.com/advisories/26822/>³¹⁰⁵ <http://secunia.com/advisories/26842/>³¹⁰⁶ <http://secunia.com/advisories/26993/>³¹⁰⁷ <http://secunia.com/advisories/27121/>³¹⁰⁸ <http://secunia.com/advisories/27209/>³¹⁰⁹ <http://secunia.com/advisories/27563/>³¹¹⁰ <http://secunia.com/advisories/27732/>³¹¹¹ <http://secunia.com/advisories/28212/>³¹¹² <http://secunia.com/advisories/28224/>³¹¹³ <http://secunia.com/advisories/28606/>³¹¹⁴ <ftp://patches.sgi.com/support/free/security/advisories/20070701-01-P> pristupljeno 18.12.2011³¹¹⁵ <https://www.suse.com/support/security/advisories/>³¹¹⁶ <http://xforce.iss.net/xforce/xfdb/35095>

17.	FTP access with ftp account (ftp-generic-0001)	172.23.202.195:21 172.23.202.196:21 172.23.202.221:21 172.23.202.222:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisničkim ID-jem (identifikacijom) „ftp“ i šifrom „ftp“. Dosadašnja praksa je pokazala da treba ukloniti difoltna naloga, ukoliko je to moguće. Za naloge koje zahteva sistem, treba promeniti difoltnu šifru.	CVE CVE-1999-0497 ³¹¹⁸	Ozbiljan	Ukloniti ili onemogućiti nalog, ukoliko to nije kritično za funkcionisanje sistema. U suprotnom, šifru treba promeniti u onu koja nije po difoltu.
18.	FTP access with anonymous account (ftp-generic-0002)	172.23.202.195:21 172.23.202.196:21 172.23.202.221:21 172.23.202.222:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisničkim ID-jem (identifikacijom) „anonymous“ i šifrom „ftp@“. Dosadašnja praksa je pokazala da treba ukloniti difoltna naloga, ukoliko je to moguće. Za naloge koje zahteva sistem, treba promeniti difoltnu šifru.	CVE CVE-1999-0497 ³¹¹⁹	Ozbiljan	Ukloniti ili onemogućiti nalog, ukoliko to nije kritično za funkcionisanje sistema. U suprotnom, šifru treba promeniti u onu koja nije po difoltu.
19.	FTP server does not support AUTH command (ftp-generic-0007)	172.23.202.195:21 172.23.202.196:21 172.23.202.221:21 172.23.202.222:21 FTP klijenti po difoltu šalju FTP server-u poverljive podatke (korisnički ID i šifru) u vidu čitkog teksta. Ova okolnost dozvoljava zlonamernim korisnicima da presreću poverljive podatke ukoliko prisluškuju vezu. Noviji FTP serveri podržavaju AUTH komandu, koja omogućava dodatne opcije autentifikacije, kao što su TLS, Kerberos, GSSAPI itd. Ona se može koristiti za sprečavanje prisluškivanja na FTP vezama.		Ozbiljan	Ažurirati/preći na FTP server koji podržava AUTH komandu.
20.	Apache httpd AllowOverride Options handling bypass (CVE-2009-1195) (http-apache-allowoverrideoptions-handling-bypass)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako web server izvršava direktivu AllowOverride sa određenim opcijama koje se koriste. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u obradi direktiva „Options“ i „AllowOverride“. U	APPLE APPLE-SA-2009-11-09 ³¹²⁰ BID 35115 ³¹²¹ CVE CVE-2009-1195 ³¹²² DEBIAN DSA-1816 ³¹²³ OSVDB 54733 ³¹²⁴ OVAL OVAL11094 ³¹²⁵ OVAL OVAL8704 ³¹²⁶ REDHAT RHSA-2009:1075 ³¹²⁷ REDHAT RHSA-2009:1156 ³¹²⁸	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

³¹¹⁷ http://httpd.apache.org/security/vulnerabilities_20.html³¹¹⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>³¹¹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>³¹²⁰ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>³¹²¹ <http://www.securityfocus.com/bid/35115>³¹²² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1195>³¹²³ <http://www.debian.org/security/2009/dsa-1816>³¹²⁴ <http://osvdb.org/54733>³¹²⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11094>³¹²⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8704>³¹²⁷ <http://rhn.redhat.com/errata/RHSA-2009-1075.html>

		konfiguracijama koje koriste direktivu „AllowOverride“ sa određenim „Options“ argumentima, lokalni korisnici mogu da izvršavaju komande iz web-serverskih skripti.	SECUNIA 35261 ³¹²⁹ SECUNIA 35264 ³¹³⁰ SECUNIA 35395 ³¹³¹ SECUNIA 35453 ³¹³² SECUNIA 35721 ³¹³³ SECUNIA 37152 ³¹³⁴ SUSE SA:2009:050 ³¹³⁵ XF apache-allowoverrides-security-bypass(50808) ³¹³⁶ URL1 ³¹³⁷		
21.	Apache httpd mod_cache proxy DoS (CVE-2007-1863) (http://apache-mod_cache-proxy-dos)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Propust je otkriven u modulu mod_cache. Na sajtovima na kojima je omogućeno keširanje, udaljeni napadač bi mogao da pošalje pažljivo izrađen zahtev koji bi doveo do toga da child proces Apache-a koji to obrađuje krahira. To može dovesti samo do odbijanja servisa ako se koristi threaded MPM.	BID 24649 ³¹³⁸ CERT TA08-150A ³¹³⁹ CVE CVE-2007-1863 ³¹⁴⁰ OVAL OVAL9824 ³¹⁴¹ REDHAT RHSA-2007:0533 ³¹⁴² REDHAT RHSA-2007:0534 ³¹⁴³ REDHAT RHSA-2007:0556 ³¹⁴⁴ REDHAT RHSA-2007:0557 ³¹⁴⁵ SECUNIA 25830 ³¹⁴⁶ SECUNIA 25873 ³¹⁴⁷ SECUNIA 25920 ³¹⁴⁸ SECUNIA 26273 ³¹⁴⁹ SECUNIA 26443 ³¹⁵⁰ SECUNIA 26508 ³¹⁵¹ SECUNIA 26822 ³¹⁵² SECUNIA 26842 ³¹⁵³ SECUNIA 26993 ³¹⁵⁴ SECUNIA 27037 ³¹⁵⁵ SECUNIA 27563 ³¹⁵⁶ SECUNIA 27732 ³¹⁵⁷ SECUNIA 28606 ³¹⁵⁸ SECUNIA 30430 ³¹⁵⁹	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz

³¹²⁸ <http://rhn.redhat.com/errata/RHSA-2009-1156.html>³¹²⁹ <http://secunia.com/advisories/35261/>³¹³⁰ <http://secunia.com/advisories/35264/>³¹³¹ <http://secunia.com/advisories/35395/>³¹³² <http://secunia.com/advisories/35453/>³¹³³ <http://secunia.com/advisories/35721/>³¹³⁴ <http://secunia.com/advisories/37152/>³¹³⁵ <https://www.suse.com/support/security/advisories/>³¹³⁶ <http://xforce.iss.net/xforce/xfdb/50808>³¹³⁷ http://httpd.apache.org/security/vulnerabilities_22.html³¹³⁸ <http://www.securityfocus.com/bid/24649>³¹³⁹ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>³¹⁴⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-1863>³¹⁴¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9824>³¹⁴² <http://rhn.redhat.com/errata/RHSA-2007-0533.html>³¹⁴³ <http://rhn.redhat.com/errata/RHSA-2007-0534.html>³¹⁴⁴ <http://rhn.redhat.com/errata/RHSA-2007-0556.html>³¹⁴⁵ <http://rhn.redhat.com/errata/RHSA-2007-0557.html>³¹⁴⁶ <http://secunia.com/advisories/25830/>³¹⁴⁷ <http://secunia.com/advisories/25873/>³¹⁴⁸ <http://secunia.com/advisories/25920/>³¹⁴⁹ <http://secunia.com/advisories/26273/>³¹⁵⁰ <http://secunia.com/advisories/26443/>³¹⁵¹ <http://secunia.com/advisories/26508/>³¹⁵² <http://secunia.com/advisories/26822/>³¹⁵³ <http://secunia.com/advisories/26842/>³¹⁵⁴ <http://secunia.com/advisories/26993/>³¹⁵⁵ <http://secunia.com/advisories/27037/>³¹⁵⁶ <http://secunia.com/advisories/27563/>³¹⁵⁷ <http://secunia.com/advisories/27732/>³¹⁵⁸ <http://secunia.com/advisories/28606/>³¹⁵⁹ <http://secunia.com/advisories/30430/>

			SUSE SA:2007:061 ³¹⁶⁰ URL1 ³¹⁶¹		
22.	Apache httpd mod_proxy_ajp DoS (CVE-2010-0408) (http://apache-mod_proxy_ajp-dos)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ajp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Mod_proxy_ajp će vratiti pogrešan kôd statusa ako naide na grešku, prouzrokujući da backend server bude stavljen u status greške dok ne istekne vreme za ponovni pokušaj. Udaljeni napadač bi mogao da pošalje zlonameran zahtev da bi pokrenuo ovaj problem, što bi dovelo do odbijanja servisa. Zahvaljujući Niku Toivola ovaj problem je prijavljen uz predloženu adekvatnu meru zaštite u vidu zakrpe.	BID 38491 ³¹⁶² CVE CVE-2010-0408 ³¹⁶³ DEBIAN DSA-2035 ³¹⁶⁴ OVAL OVAL8619 ³¹⁶⁵ OVAL OVAL9935 ³¹⁶⁶ REDHAT RHSA-2010:0168 ³¹⁶⁷ SECUNIA 39100 ³¹⁶⁸ SECUNIA 39501 ³¹⁶⁹ SECUNIA 39628 ³¹⁷⁰ SECUNIA 39632 ³¹⁷¹ SECUNIA 39656 ³¹⁷² SECUNIA 40096 ³¹⁷³ URL1 ³¹⁷⁴	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz
23.	Apache httpd mod_proxy_ftp DoS (CVE-2009-3094) (http://apache-mod_proxy_ftp-dos)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ftp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust NULL pointer dereference (pointer sa NULL vrednošću upotrebljen kao da ukazuje na validnu memorijsku oblast) otkriven je u modulu mod_proxy_ftp. Zlonamerni FTP server, kojem su zahtevi proksirani, mogao bi da iskoristi ovaj propust u smislu obaranja http child procesa uz pomoć namerno izmenjenog odgovora EPSV ili PASV komandi, što bi dovelo do delimičnog odbijanja servisa.	CVE CVE-2009-3094 ³¹⁷⁵ DEBIAN DSA-1934 ³¹⁷⁶ OVAL OVAL10981 ³¹⁷⁷ OVAL OVAL8087 ³¹⁷⁸ SECUNIA 36549 ³¹⁷⁹ SECUNIA 37152 ³¹⁸⁰ SUSE SA:2009:050 ³¹⁸¹ URL1 ³¹⁸²	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.gz

³¹⁶⁰ <https://www.suse.com/support/security/advisories/>³¹⁶¹ http://httpd.apache.org/security/vulnerabilities_20.html³¹⁶² <http://www.securityfocus.com/bid/38491>³¹⁶³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0408>³¹⁶⁴ <http://www.debian.org/security/2010/dsa-2035>³¹⁶⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8619>³¹⁶⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9935>³¹⁶⁷ <http://rhn.redhat.com/errata/RHSA-2010-0168.html>³¹⁶⁸ <http://secunia.com/advisories/39100/>³¹⁶⁹ <http://secunia.com/advisories/39501/>³¹⁷⁰ <http://secunia.com/advisories/39628/>³¹⁷¹ <http://secunia.com/advisories/39632/>³¹⁷² <http://secunia.com/advisories/39656/>³¹⁷³ <http://secunia.com/advisories/40096/>³¹⁷⁴ http://httpd.apache.org/security/vulnerabilities_22.html³¹⁷⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3094>³¹⁷⁶ <http://www.debian.org/security/2009/dsa-1934>³¹⁷⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10981>³¹⁷⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8087>³¹⁷⁹ <http://secunia.com/advisories/36549/>³¹⁸⁰ <http://secunia.com/advisories/37152/>³¹⁸¹ <https://www.suse.com/support/security/advisories/>³¹⁸² http://httpd.apache.org/security/vulnerabilities_22.html

24.	Browsable web directory (http-generic-browsable-dir)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Otkriven je direktorijum na web serveru koji može biti pretraživan, što znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice-spajdering (prateći hiperlinkove), ili -kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute-force napadom na liste uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skrivenne“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice. http://172.23.202.195/icons/small/ 4: <title>Index of /icons/small</title> 5: </head> 6: <body> 7: <h1>Index of /icons/small</h1> 8: ...CO]<th>Name</th><th><a href=?C=M;O=A...		Ozbiljan	Za Apache: onemogućiti pretraživanje direktorijuma mreže za sve direktorijume i poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume. Za Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote: Onemogućiti pretraživanje direktorijuma za sve direktorijume i poddirektorijume. Uključiti Tomcat-ov web.xml file. U odeljku „default“, promeniti parametar „listings“ iz „true“ u „false“. Restartovati server. Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripta i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume.
25.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	172.23.202.195:22 172.23.202.221:80 172.23.202.196:80 172.23.202.222:22 Kada se kod TCP-a paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije	BID: 10183³¹⁸³ CERT-VN: 415294³¹⁸⁴ CVE CVE-2004-0230³¹⁸⁵ MS: MS05-019³¹⁸⁶ MS: MS06-064³¹⁸⁷ NETBSD: NetBSD-SA2004-006³¹⁸⁸	Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC 2385.³²⁰¹ Ono je napravljeno da smanji opasnost od određenih napada na BGP, kao što su

³¹⁸³ <http://www.securityfocus.com/bid/10183>³¹⁸⁴ <http://www.kb.cert.org/vuls/id/415294>³¹⁸⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>³¹⁸⁶ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>³¹⁸⁷ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>

		sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	OVAL: OVAL2689 ³¹⁸⁹ OVAL: OVAL270 ³¹⁹⁰ OVAL OVAL3508 ³¹⁹¹ OVAL OVAL4791 ³¹⁹² OVAL OVAL5711 ³¹⁹³ SECUNIA: 11440 ³¹⁹⁴ SECUNIA 11458 ³¹⁹⁵ SECUNIA: 22341 ³¹⁹⁶ SGI 20040403-01-A ³¹⁹⁷ XF tcp-rst-dos(15886) ³¹⁹⁸ URL1 ³¹⁹⁹ URL2 ³²⁰⁰		TCP reseti.
26.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podesi na jedinstvenu vrednost i da se koristi u rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da fingerprint-uje operativni sistem.	BID 4314 ³²⁰² CVE CVE-2002-0510 ³²⁰³ XF linux-udp-fingerprint(8588) ³²⁰⁴	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili pak ranjivost koju treba popravljati, tako da ne postoje rešenja koja se mogu kupiti. Jedino se može postaviti fajervol ili neka druga sprava za filtriranje između napadnutog i neprijateljskog napada koji je u mogućnosti da randomizuje IP ID-jeve.
27.	Apache httpd mod_imagemap XSS (CVE-2007-5000) (apache-httpd-2_2_x-mod_imagemap-xss-cve-2007-5000)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Propust je otkriven u modulu mod_imagemap. Na sajtovima na kojima je omogućen mod_imagemap i imagemap fajl je javno dostupan, moguć je napad unakrsnog skriptovanja.	BID 26838 ³²⁰⁵ CERT TA08-150A ³²⁰⁶ CVE CVE-2007-5000 ³²⁰⁷ OSVDB 39134 ³²⁰⁸ OVAL OVAL9539 ³²⁰⁹ REDHAT RHSA-2008:0004 ³²¹⁰ REDHAT RHSA-2008:0005 ³²¹¹ REDHAT RHSA-2008:0006 ³²¹² REDHAT RHSA-2008:0007 ³²¹³ REDHAT RHSA-2008:0008 ³²¹⁴ REDHAT RHSA-2008:0009 ³²¹⁵	Ozbiljan	Apache >= 2.2 and < 2.3 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.8.tar.gz

³¹⁸⁸ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>³²⁰¹ <http://www.ietf.org/rfc/rfc2385.txt>³¹⁸⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>³¹⁹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>³¹⁹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>³¹⁹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>³¹⁹³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>³¹⁹⁴ <http://secunia.com/advisories/11440/>³¹⁹⁵ <http://secunia.com/advisories/11458/>³¹⁹⁶ <http://secunia.com/advisories/22341/>³¹⁹⁷ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>³¹⁹⁸ <http://xforce.iss.net/xforce/xfdb/15886>³¹⁹⁹ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>³²⁰⁰ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>³²⁰² <http://www.securityfocus.com/bid/4314>³²⁰³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>³²⁰⁴ <http://xforce.iss.net/xforce/xfdb/8588>³²⁰⁵ <http://www.securityfocus.com/bid/26838>³²⁰⁶ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>³²⁰⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-5000>³²⁰⁸ <http://www.osvdb.org/39134>³²⁰⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9539>³²¹⁰ <http://rhn.redhat.com/errata/RHSA-2008-0004.html>³²¹¹ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>³²¹² <http://rhn.redhat.com/errata/RHSA-2008-0006.html>³²¹³ <http://rhn.redhat.com/errata/RHSA-2008-0007.html>³²¹⁴ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>³²¹⁵ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>

			REDHAT ³²¹⁶ RHSA- 2008:0261 SECUNIA 28046 ³²¹⁷ SECUNIA 28073 ³²¹⁸ SECUNIA 28081 ³²¹⁹ SECUNIA 28196 ³²²⁰ SECUNIA 28375 ³²²¹ SECUNIA 28467 ³²²² SECUNIA 28471 ³²²³ SECUNIA 28525 ³²²⁴ SECUNIA 28526 ³²²⁵ SECUNIA 28607 ³²²⁶ SECUNIA 28749 ³²²⁷ SECUNIA 28750 ³²²⁸ SECUNIA 28922 ³²²⁹ SECUNIA 28977 ³²³⁰ SECUNIA 29420 ³²³¹ SECUNIA 29640 ³²³² SECUNIA 29806 ³²³³ SECUNIA 29988 ³²³⁴ SECUNIA 30356 ³²³⁵ SECUNIA 30430 ³²³⁶ SECUNIA 30732 ³²³⁷ SECUNIA 31142 ³²³⁸ SUSE ³²³⁹ SUSE- SA:2008:021 URL1 ³²⁴⁰		
28.	Apache httpd mod_proxy_ftp globbing XSS (CVE- 2008-2939) (apache- httpd-2_2_x- mod_proxy_ftp- globbing- xss-cve-2008-2939)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osjetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ftp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u modulu	APPLE ³²⁴¹ APPLE-SA- 2009-05-12 BID 30560 ³²⁴² CERT TA09-133A ³²⁴³ CERT-VN 663763 ³²⁴⁴ CVE CVE-2008-2939 ³²⁴⁵ OVAL OVAL11316 ³²⁴⁶ OVAL OVAL7716 ³²⁴⁷ REDHAT ³²⁴⁸ RHSA- 2008:0966	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dis t/httpd/httpd-2.2.10.tar.gz

³²¹⁶ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>³²¹⁷ <http://secunia.com/advisories/28046/>³²¹⁸ <http://secunia.com/advisories/28073/>³²¹⁹ <http://secunia.com/advisories/28081/>³²²⁰ <http://secunia.com/advisories/28196/>³²²¹ <http://secunia.com/advisories/28375/>³²²² <http://secunia.com/advisories/28467/>³²²³ <http://secunia.com/advisories/28471/>³²²⁴ <http://secunia.com/advisories/28525/>³²²⁵ <http://secunia.com/advisories/28526/>³²²⁶ <http://secunia.com/advisories/28607/>³²²⁷ <http://secunia.com/advisories/28749/>³²²⁸ <http://secunia.com/advisories/28750/>³²²⁹ <http://secunia.com/advisories/28922/>³²³⁰ <http://secunia.com/advisories/28977/>³²³¹ <http://secunia.com/advisories/29420/>³²³² <http://secunia.com/advisories/29640/>³²³³ <http://secunia.com/advisories/29806/>³²³⁴ <http://secunia.com/advisories/29988/>³²³⁵ <http://secunia.com/advisories/30356/>³²³⁶ <http://secunia.com/advisories/30430/>³²³⁷ <http://secunia.com/advisories/30732/>³²³⁸ <http://secunia.com/advisories/31142/>³²³⁹ <https://www.suse.com/support/security/advisories/>³²⁴⁰ http://httpd.apache.org/security/vulnerabilities_20.html³²⁴¹ <http://lists.apple.com/archives/security-announce/2009/May/msg00001.html>³²⁴² <http://www.securityfocus.com/bid/30560>³²⁴³ <http://www.us-cert.gov/ncas/alerts/TA09-133A>³²⁴⁴ <http://www.kb.cert.org/vuls/id/663763>³²⁴⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-2939>³²⁴⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11316>³²⁴⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7716>³²⁴⁸ <http://rhn.redhat.com/errata/RHSA-2008-0966.html>

		mod_proxy_ftp prilikom obrade "wildcard-a" ukoliko se on nađe u putanji FTP URL. Ukoliko je mod_proxy_ftp omogućen da podržava FTP-over-HTTP, zahtevi koji sadrže specijalne karaktere mogu da dovedu do cross-site scripting napada (XSS).	REDHAT ³²⁴⁹ RHSA-2008:0967 SECUNIA ³²⁵⁰ 31384 SECUNIA ³²⁵¹ 31673 SECUNIA ³²⁵² 32685 SECUNIA ³²⁵³ 32838 SECUNIA ³²⁵⁴ 33156 SECUNIA ³²⁵⁵ 33797 SECUNIA ³²⁵⁶ 34219 SECUNIA ³²⁵⁷ 35074 XF ³²⁵⁸ apache-modproxyftp-xss(44223) URL1 ³²⁵⁹		
29.	Apache httpd mod_proxy_ftp UTF-7 XSS (CVE-2008-0005) (apache-httpd-2_2_x-mod_proxy_ftp-utf-7-xsscve-2008-0005)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 U modul mod_proxy_ftp je dodata zaobilaznica. Na sajtovima na kojima je omogućen mod_proxy_ftp i konfigurisan je forward tipa proxy-ja, moguće je izvesti napad XSS na Web pretraživače koji neprepoznaju određeni character set prema pravilima iz dokumenta RFC 2616.	BID ³²⁶⁰ 27234 CVE ³²⁶¹ CVE-2008-0005 OVAL ³²⁶² OVAL10812 REDHAT ³²⁶³ RHSA-2008:0004 REDHAT ³²⁶⁴ RHSA-2008:0005 REDHAT ³²⁶⁵ RHSA-2008:0006 REDHAT ³²⁶⁶ RHSA-2008:0007 REDHAT ³²⁶⁷ RHSA-2008:0008 REDHAT ³²⁶⁸ RHSA-2008:0009 SECUNIA ³²⁶⁹ 28467 SECUNIA ³²⁷⁰ 28471 SECUNIA ³²⁷¹ 28526 SECUNIA ³²⁷² 28607 SECUNIA ³²⁷³ 28749 SECUNIA ³²⁷⁴ 28977 SECUNIA ³²⁷⁵ 29348 SECUNIA ³²⁷⁶ 29420 SECUNIA ³²⁷⁷ 29640 SECUNIA ³²⁷⁸ 30732 SECUNIA ³²⁷⁹ 35650	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.8.tar.gz

³²⁴⁹ <http://rhn.redhat.com/errata/RHSA-2008-0967.html>³²⁵⁰ <http://secunia.com/advisories/31384/>³²⁵¹ <http://secunia.com/advisories/31673/>³²⁵² <http://secunia.com/advisories/32685/>³²⁵³ <http://secunia.com/advisories/32838/>³²⁵⁴ <http://secunia.com/advisories/33156/>³²⁵⁵ <http://secunia.com/advisories/33797/>³²⁵⁶ <http://secunia.com/advisories/34219/>³²⁵⁷ <http://secunia.com/advisories/35074/>³²⁵⁸ <http://xforce.iss.net/xforce/xfdb/44223>³²⁵⁹ http://httpd.apache.org/security/vulnerabilities_22.html³²⁶⁰ <http://www.securityfocus.com/bid/27234>³²⁶¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0005>³²⁶² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10812>³²⁶³ <http://rhn.redhat.com/errata/RHSA-2008-0004.html>³²⁶⁴ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>³²⁶⁵ <http://rhn.redhat.com/errata/RHSA-2008-0006.html>³²⁶⁶ <http://rhn.redhat.com/errata/RHSA-2008-0007.html>³²⁶⁷ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>³²⁶⁸ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>³²⁶⁹ <http://secunia.com/advisories/28467/>³²⁷⁰ <http://secunia.com/advisories/28471/>³²⁷¹ <http://secunia.com/advisories/28526/>³²⁷² <http://secunia.com/advisories/28607/>³²⁷³ <http://secunia.com/advisories/28749/>³²⁷⁴ <http://secunia.com/advisories/28977/>³²⁷⁵ <http://secunia.com/advisories/29348/>³²⁷⁶ <http://secunia.com/advisories/29420/>³²⁷⁷ <http://secunia.com/advisories/29640/>³²⁷⁸ <http://secunia.com/advisories/30732/>³²⁷⁹ <http://secunia.com/advisories/35650/>

			SUSE SA:2008:021 ³²⁸⁰ XF apache-modproxyftp- utf7-xss(39615) URL1 ³²⁸¹		
30.	Apache httpd mod_status XSS (CVE- 2007-6388) (apache- httpd-2_2_x- mod_status-xss-cve- 2007-6388)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Propust je otkriven u modulu mod_status. Na sajtovima na kojima je omogućen mod_status ukoliko su stranice statusa javno dostupne, postoji mogućnost XSS napada. Stranica sa statusom servera nije po difoltu omogućena, a dosadašnja praksa je pokazala da je najbolje da ona ne bude javno dostupna.	BID 27237 ³²⁸² CERT TA08-150A ³²⁸³ CVE CVE-2007-6388 ³²⁸⁴ OVAL OVAL10272 ³²⁸⁵ REDHAT RHSA- 2008:0004 ³²⁸⁶ REDHAT RHSA- 2008:0005 ³²⁸⁷ REDHAT RHSA- 2008:0006 ³²⁸⁸ REDHAT RHSA- 2008:0007 ³²⁸⁹ REDHAT RHSA- 2008:0008 ³²⁹⁰ REDHAT RHSA- 2008:0009 ³²⁹¹ REDHAT RHSA- 2008:0261 ³²⁹² SECUNIA 28467 ³²⁹³ SECUNIA 28471 ³²⁹⁴ SECUNIA 28526 ³²⁹⁵ SECUNIA 28607 ³²⁹⁶ SECUNIA 28749 ³²⁹⁷ SECUNIA 28922 ³²⁹⁸ SECUNIA 28965 ³²⁹⁹ SECUNIA 28977 ³³⁰⁰ SECUNIA 29420 ³³⁰¹ SECUNIA 29504 ³³⁰² SECUNIA 29640 ³³⁰³ SECUNIA 29806 ³³⁰⁴ SECUNIA 29988 ³³⁰⁵ SECUNIA 30356 ³³⁰⁶ SECUNIA 30430 ³³⁰⁷ SECUNIA 30732 ³³⁰⁸ SECUNIA 31142 ³³⁰⁹	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dis t/httpd/httpd-2.2.8.tar.gz

³²⁸⁰ <https://www.suse.com/support/security/advisories/>³²⁸¹ http://httpd.apache.org/security/vulnerabilities_20.html³²⁸² <http://www.securityfocus.com/bid/27237>³²⁸³ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>³²⁸⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6388>³²⁸⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10272>³²⁸⁶ <http://rhn.redhat.com/errata/RHSA-2008-0004.html>³²⁸⁷ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>³²⁸⁸ <http://rhn.redhat.com/errata/RHSA-2008-0006.html>³²⁸⁹ <http://rhn.redhat.com/errata/RHSA-2008-0007.html>³²⁹⁰ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>³²⁹¹ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>³²⁹² <http://rhn.redhat.com/errata/RHSA-2008-0261.html>³²⁹³ <http://secunia.com/advisories/28467/>³²⁹⁴ <http://secunia.com/advisories/28471/>³²⁹⁵ <http://secunia.com/advisories/28526/>³²⁹⁶ <http://secunia.com/advisories/28607/>³²⁹⁷ <http://secunia.com/advisories/28749/>³²⁹⁸ <http://secunia.com/advisories/28922/>³²⁹⁹ <http://secunia.com/advisories/28965/>³³⁰⁰ <http://secunia.com/advisories/28977/>³³⁰¹ <http://secunia.com/advisories/29420/>³³⁰² <http://secunia.com/advisories/29504/>³³⁰³ <http://secunia.com/advisories/29640/>³³⁰⁴ <http://secunia.com/advisories/29806/>³³⁰⁵ <http://secunia.com/advisories/29988/>³³⁰⁶ <http://secunia.com/advisories/30356/>³³⁰⁷ <http://secunia.com/advisories/30430/>³³⁰⁸ <http://secunia.com/advisories/30732/>³³⁰⁹ <http://secunia.com/advisories/31142/>

			SECUNIA 33200 ³³¹⁰ SUSE SUSE-SA:2008:021 ³³¹¹ XF apache-status-page-xss(39472) ³³¹²		
31.	Apache httpd apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpd-cve-2011-0419)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_autoindex. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_fnmatch() u sklopu APR biblioteke. Ako je omogućen mod_autoindex, a indeksi direktorijuma mod_autoindex su sadržavali fajlove sa dovoljno dugim nazivima, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do preterane upotrebe CPU-a. Ovo bi moglo da bude iskorišćeno u napadu odbijanja servisa. Zahvaljujući Maksymilian Arciemowicz-u prijavljen je ovaj propust.	CVE CVE-2011-0419 ³³¹³ REDHAT RHSA-2011:0507 ³³¹⁴ SECUNIA 44490 ³³¹⁵ SECUNIA 44564 ³³¹⁶ SECUNIA 44574 ³³¹⁷ URL1 ³³¹⁸	Ozbiljan	Apache >= 2.2 and < 2.3 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.18.tar.gz
32.	Apache httpd APR-util heap underwrite (CVE-2009-0023) (http-apache-apr-util-heap-underwrite)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako napadač poseduje posebno kreiranu ključnu reč za pretraživanje one funkcije koja upravlja kompajliranjem formi zahteva pretrage. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u načinu na koji komplet APR-biblioteke kompajlira forme zahtevanih pretraživanja. Napadač bi mogao da kreira posebno izrađenu ključnu reč pretraživanja,	BID 35221 ³³¹⁹ CVE CVE-2009-0023 ³³²⁰ DEBIAN DSA-1812 ³³²¹ OVAL OVAL10968 ³³²² REDHAT RHSA-2009:1107 ³³²³ REDHAT RHSA-2009:1108 ³³²⁴ SECUNIA 34724 ³³²⁵ SECUNIA 35284 ³³²⁶ SECUNIA 35360 ³³²⁷ SECUNIA 35395 ³³²⁸ SECUNIA 35444 ³³²⁹ SECUNIA 35487 ³³³⁰ SECUNIA 35565 ³³³¹ SECUNIA 35710 ³³³² SECUNIA 35797 ³³³³	Ozbiljan	Apache >= 2.2 and < 2.3 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

³³¹⁰ <http://secunia.com/advisories/33200/>³³¹¹ <https://www.suse.com/support/security/advisories/>³³¹² <http://xforce.iss.net/xforce/xfdb/39472> pristupljeno 11.12.2011³³¹³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419>³³¹⁴ <http://rhn.redhat.com/errata/RHSA-2011-0507.html>³³¹⁵ <http://secunia.com/advisories/44490/>³³¹⁶ <http://secunia.com/advisories/44564/>³³¹⁷ <http://secunia.com/advisories/44574/>³³¹⁸ http://httpd.apache.org/security/vulnerabilities_22.html³³¹⁹ <http://www.securityfocus.com/bid/35221>³³²⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-0023>³³²¹ <http://lists.debian.org/debian-security-announce/2009/msg00124.html>³³²² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10968>³³²³ <http://rhn.redhat.com/errata/RHSA-2009-1107.html>³³²⁴ <http://rhn.redhat.com/errata/RHSA-2009-1108.html>³³²⁵ <http://secunia.com/advisories/34724/>³³²⁶ <http://secunia.com/advisories/35284/>³³²⁷ <http://secunia.com/advisories/35360/>³³²⁸ <http://secunia.com/advisories/35395/>³³²⁹ <http://secunia.com/advisories/35444/>³³³⁰ <http://secunia.com/advisories/35487/>³³³¹ <http://secunia.com/advisories/35565/>³³³² <http://secunia.com/advisories/35710/>

		koja bi se proizvoljnim prepisivanjem gomilala u memoriji prilikom obrađivanja zahteva za pretragu.	SECUNIA 35843 ³³³⁴ SECUNIA 37221 ³³³⁵ XF apache-aprstrmatchprecompile-dos(50964) ³³³⁶ URL1 ³³³⁷		
33.	Apache httpd mod_proxy_balancer CSRF (CVE-2007-6420) (http-apache-mod_proxy_balancer-csrf)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Mod_proxy_balancer je omogućio administrativni interfejs koji bi mogao biti ranjiv na napade lažnih zahteva CSRF (cross-site request forgery).	BID 27236 ³³³⁸ BID 31681 ³³³⁹ CVE CVE-2007-6420 ³³⁴⁰ OVAL OVAL8371 ³³⁴¹ REDHAT RHSA-2008:0966 ³³⁴² SECUNIA 31026 ³³⁴³ SECUNIA 32222 ³³⁴⁴ SECUNIA 33797 ³³⁴⁵ SECUNIA 34219 ³³⁴⁶ URL1 ³³⁴⁷	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.9.tar.gz
34.	Apache httpd mod_proxy_balancer DoS (CVE-2007-6422) (http-apache-mod_proxy_balancer-dos)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Propust je otkriven u modulu mod_proxy_balancer. Na sajtovmu na kojima je omogućen mod_proxy_balancer, autorizovan korisnik bi mogao poslati pažljivo izrađen zahtev koji bi doveo do toga da krahira child proces Apache-a koji taj zahtev obrađuje. To može dovesti samo do odbijanja servisa ako se koristi threaded MPM.	BID 27236 ³³⁴⁸ CVE CVE-2007-6422 ³³⁴⁹ OVAL OVAL10181 ³³⁵⁰ OVAL OVAL8690 ³³⁵¹ REDHAT RHSA-2008:0008 ³³⁵² REDHAT RHSA-2008:0009 ³³⁵³ SECUNIA 28526 ³³⁵⁴ SECUNIA 28749 ³³⁵⁵ SECUNIA 28977 ³³⁵⁶ SECUNIA 29348 ³³⁵⁷ SECUNIA 29640 ³³⁵⁸ SUSE SUSE-SA:2008:021 ³³⁵⁹ XF apache-modproxybalancer-dos(39476) ³³⁶⁰ URL1 ³³⁶¹	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.8.tar.gz
35.	Apache httpd mod_proxy_balancer	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80	BID 27236 ³³⁶² CVE CVE-2007-6421 ³³⁶³ OVAL OVAL10664 ³³⁶⁴	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati:

³³³³ <http://secunia.com/advisories/35797/>
³³³⁴ <http://secunia.com/advisories/35843/>
³³³⁵ <http://secunia.com/advisories/37221/>
³³³⁶ <http://xforce.iss.net/xforce/xfdb/50964>
³³³⁷ http://httpd.apache.org/security/vulnerabilities_22.html
³³³⁸ <http://www.securityfocus.com/bid/27236>
³³³⁹ <http://www.securityfocus.com/bid/31681>
³³⁴⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6420>
³³⁴¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8371>
³³⁴² <http://rhn.redhat.com/errata/RHSA-2008-0966.html>
³³⁴³ <http://secunia.com/advisories/31026/>
³³⁴⁴ <http://secunia.com/advisories/32222/>
³³⁴⁵ <http://secunia.com/advisories/33797/>
³³⁴⁶ <http://secunia.com/advisories/34219/>
³³⁴⁷ http://httpd.apache.org/security/vulnerabilities_22.html
³³⁴⁸ <http://www.securityfocus.com/bid/27236>
³³⁴⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6422>
³³⁵⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10181>
³³⁵¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8690>
³³⁵² <http://rhn.redhat.com/errata/RHSA-2008-0008.html>
³³⁵³ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>
³³⁵⁴ <http://secunia.com/advisories/28526/>
³³⁵⁵ <http://secunia.com/advisories/28749/>
³³⁵⁶ <http://secunia.com/advisories/28977/>
³³⁵⁷ <http://secunia.com/advisories/29348/>
³³⁵⁸ <http://secunia.com/advisories/29640/>
³³⁵⁹ <https://www.suse.com/support/security/advisories/>
³³⁶⁰ <http://xforce.iss.net/xforce/xfdb/39476>
³³⁶¹ http://httpd.apache.org/security/vulnerabilities_22.html
³³⁶² <http://www.securityfocus.com/bid/27236>
³³⁶³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6421>

	XSS (CVE-2007-6421) (http-apache-mod_proxy_balancer-xss)	172.23.202.222:80 Propust je otkriven u modulu mod_proxy_balancer. Na sajtovima na kojima je omogućen mod_proxy_balancer, moguć je XSS napad prema autorizovanom korisniku.	OVAL OVAL8651 ³³⁶⁵ REDHAT RHSA-2008:0008 ³³⁶⁶ REDHAT RHSA-2008:0009 ³³⁶⁷ SECUNIA 28526 ³³⁶⁸ SECUNIA 28749 ³³⁶⁹ SECUNIA 28977 ³³⁷⁰ SECUNIA 29420 ³³⁷¹ SECUNIA 29640 ³³⁷² SUSE SUSE-SA:2008:021 ³³⁷³ XF apache-modproxybalancer-dos(39476) ³³⁷⁴ URL1 ³³⁷⁵		http://archive.apache.org/dist/httpd/httpd-2.2.8.tar.gz
36.	Apache httpd mod_status cross-site scripting (CVE-2006-5752) (http-apache-mod_status-xss)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Propust otkriven u modulu mod_status. Na sajtovima na kojima je status servera javno dostupan i omogućen je ExtendedStatus, postoji mogućnost XSS napada. Stranica sa statusom servera nije po defaultu omogućena, a dosadašnja praksa je pokazala da je najbolje da ona ne bude javno dostupna.	BID 24645 ³³⁷⁶ CVE CVE-2006-5752 ³³⁷⁷ OVAL OVAL10154 ³³⁷⁸ REDHAT RHSA-2007:0532 ³³⁷⁹ REDHAT RHSA-2007:0533 ³³⁸⁰ REDHAT RHSA-2007:0534 ³³⁸¹ REDHAT RHSA-2007:0556 ³³⁸² REDHAT RHSA-2007:0557 ³³⁸³ REDHAT RHSA-2008:0261 ³³⁸⁴ SECUNIA 25827 ³³⁸⁵ SECUNIA 25830 ³³⁸⁶ SECUNIA 25873 ³³⁸⁷ SECUNIA 25920 ³³⁸⁸ SECUNIA 26273 ³³⁸⁹ SECUNIA 26443 ³³⁹⁰ SECUNIA 26458 ³³⁹¹ SECUNIA 26508 ³³⁹² SECUNIA 26822 ³³⁹³	Ozbiljan	Apache >= 2.2 and < 2.3 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz

³³⁶⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10664>³³⁶⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8651>³³⁶⁶ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>³³⁶⁷ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>³³⁶⁸ <http://secunia.com/advisories/28526/>³³⁶⁹ <http://secunia.com/advisories/28749/>³³⁷⁰ <http://secunia.com/advisories/28977/>³³⁷¹ <http://secunia.com/advisories/29420/>³³⁷² <http://secunia.com/advisories/29640/>³³⁷³ <https://www.suse.com/support/security/advisories/>³³⁷⁴ <http://xforce.iss.net/xforce/xfdb/39476>³³⁷⁵ http://httpd.apache.org/security/vulnerabilities_22.html³³⁷⁶ <http://www.securityfocus.com/bid/24645>³³⁷⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-5752>³³⁷⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10154>³³⁷⁹ <http://rhn.redhat.com/errata/RHSA-2007-0532.html>³³⁸⁰ <http://rhn.redhat.com/errata/RHSA-2007-0533.html>³³⁸¹ <http://rhn.redhat.com/errata/RHSA-2007-0534.html>³³⁸² <http://rhn.redhat.com/errata/RHSA-2007-0556.html>³³⁸³ <http://rhn.redhat.com/errata/RHSA-2007-0557.html>³³⁸⁴ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>³³⁸⁵ <http://secunia.com/advisories/25827/>³³⁸⁶ <http://secunia.com/advisories/25830/>³³⁸⁷ <http://secunia.com/advisories/25873/>³³⁸⁸ <http://secunia.com/advisories/25920/>³³⁸⁹ <http://secunia.com/advisories/26273/>³³⁹⁰ <http://secunia.com/advisories/26443/>³³⁹¹ <http://secunia.com/advisories/26458/>³³⁹² <http://secunia.com/advisories/26508/>³³⁹³ <http://secunia.com/advisories/26822/>

			SECUNIA 26842 ³³⁹⁴ SECUNIA 26993 ³³⁹⁵ SECUNIA 27037 ³³⁹⁶ SECUNIA 27563 ³³⁹⁷ SECUNIA 27732 ³³⁹⁸ SECUNIA 28212 ³³⁹⁹ SECUNIA 28224 ³⁴⁰⁰ SECUNIA 28606 ³⁴⁰¹ SUSE SA:2007:061 ³⁴⁰² XF apache-modstatus- xss(35097) URL1 ³⁴⁰³		
37.	Apache httpd Subrequest handling of request headers (mod_headers) (CVE-2010-0434) (http-apacherequest-header-info-disclosure)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osjetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_headers. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust u jezgu "subrequest process code" može dovesti do greške tipa segmentation fault-a ili do otkrivanja podataka iz nekog drugog zahteva na thread-ovima servera, kao što su worker ili winnt MPM-ovi. Zahvaljujući Philip Pickett-u iz Vmware ovaj propust je prijavljen i predložen je način ispravke.	BID 38494 ³⁴⁰⁴ CVE CVE-2010-0434 ³⁴⁰⁵ DEBIAN DSA-2035 ³⁴⁰⁶ OVAL OVAL10358 ³⁴⁰⁷ OVAL OVAL8695 ³⁴⁰⁸ REDHAT RHSA-2010:0168 ³⁴⁰⁹ REDHAT RHSA-2010:0175 ³⁴¹⁰ SECUNIA 39100 ³⁴¹¹ SECUNIA 39115 ³⁴¹² SECUNIA 39501 ³⁴¹³ SECUNIA 39628 ³⁴¹⁴ SECUNIA 39632 ³⁴¹⁵ SECUNIA 39656 ³⁴¹⁶ SECUNIA 40096 ³⁴¹⁷ XF apache-http-rh-info-disclosure(56625) ³⁴¹⁸ URL1 ³⁴¹⁹	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz
38.	OpenSSH CBC Mode Information Disclosure Vulnerability (ssh-openssh-cbc-mode-info-disclosure)	172.23.202.195:22 172.23.202.196:22 172.23.202.221:22 172.23.202.222:22 Odredene verzije OpenSSH-a poseduju ranjivu implementaciju blok šifarskog algoritma u CBC modu	BID 32319 ³⁴²⁰ CVE CVE-2008-5161 ³⁴²¹ SECUNIA 32760 ³⁴²² URL1 ³⁴²³ URL2 ³⁴²⁴	Ozbiljan	Uraditi download a zatim instalirati: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-5.2p1.tar.gz Verzija 5.2 OpenSSH-a je puštena u promet 22.

³³⁹⁴ <http://secunia.com/advisories/26842/>³³⁹⁵ <http://secunia.com/advisories/26993/>³³⁹⁶ <http://secunia.com/advisories/27037/>³³⁹⁷ <http://secunia.com/advisories/27563/>³³⁹⁸ <http://secunia.com/advisories/27732/>³³⁹⁹ <http://secunia.com/advisories/28212/>³⁴⁰⁰ <http://secunia.com/advisories/28224/>³⁴⁰¹ <http://secunia.com/advisories/28606/>³⁴⁰² <https://www.suse.com/support/security/advisories/>³⁴⁰³ http://httpd.apache.org/security/vulnerabilities_20.html³⁴⁰⁴ <http://www.securityfocus.com/bid/38494>³⁴⁰⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0434>³⁴⁰⁶ <http://www.debian.org/security/2010/dsa-2035>³⁴⁰⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10358>³⁴⁰⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8695>³⁴⁰⁹ <http://rhn.redhat.com/errata/RHSA-2010-0168.html>³⁴¹⁰ <http://rhn.redhat.com/errata/RHSA-2010-0175.html>³⁴¹¹ <http://secunia.com/advisories/39100/>³⁴¹² <http://secunia.com/advisories/39115/>³⁴¹³ <http://secunia.com/advisories/39501/>³⁴¹⁴ <http://secunia.com/advisories/39628/>³⁴¹⁵ <http://secunia.com/advisories/39632/>³⁴¹⁶ <http://secunia.com/advisories/39656/>³⁴¹⁷ <http://secunia.com/advisories/40096/>³⁴¹⁸ <http://xforce.iss.net/xforce/xfdb/56625>³⁴¹⁹ http://httpd.apache.org/security/vulnerabilities_22.html³⁴²⁰ <http://www.securityfocus.com/bid/32319>³⁴²¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-5161>³⁴²² <http://secunia.com/advisories/32760/>³⁴²³ http://www.cpni.gov.uk/Docs/Vulnerability_Advisory_SSH.txt, pristupljeno 20.12.2011³⁴²⁴ <http://www.openssh.com/txt/cbc.adv>

		(Cipher Block Chaining). Ovo bi udaljenom napadaču moglo omogućiti da preko nepoznatih vektora pridobije određene podatke u vidu običnog teksta iz proizvoljnog bloka šifrovanog teksta u SSH sesiji.			februara 2009.
39.	OpenSSH „X11UseLocalhost“ X11 Forwarding Session Hijacking Vulnerability (ssh-opensshx11uselocalhost-x11-forwarding-session-hijack)	172.23.202.195:22 172.23.202.196:22 172.23.202.221:22 172.23.202.222:22 Određene verzije OpenSSH-a podešavaju SO_REUSEADDR socket opciju kada je onemogućeno podešavanje X11UseLocalhost konfiguracije. Ovo bi lokalnom napadaču moglo da omogući da preuzme X11 forwarding port preko veze ka pojedinačnoj IP adresi.	BID 30339 ³⁴²⁵ CVE CVE-2008-3259 ³⁴²⁶ SECUNIA 31179 ³⁴²⁷	Ozbiljan	Uraditi download a zatim instalirati: http://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-5.1p1.tar.gz Verzija 5.1 OpenSSH-a je puštena u promet 21. jula 2008.
40.	HTTP TRACE Method Enabled (http-trace-method-enabled)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 HTTP TRACE metoda se obično koristi da uzvрати potpuni HTTP zahtev klijentu koji ga zahteva, u cilju debagovanja proxy servera. Napadač bi mogao da kreira web stranicu koristeći XML, HTTP, ActiveX ili XMLDOM da natera klijenta da pošalje TRACE zahtev i da sačuva klijenove kolačiće. Efektivno, to dovodi do XSS napada. Primer : 172.23.202.196:80 Running vulnerable HTTP service. http://172.23.202.195/ 1: TRACE / HTTP/1.1 2: Host: 172.23.202.195 3: Cookie: vulnerable=yes	CVE CVE-2004-2320 ³⁴²⁸ CVE CVE-2004-2763 ³⁴²⁹ CVE CVE-2005-3398 ³⁴³⁰ CVE CVE-2006-4683 ³⁴³¹ CVE CVE-2007-3008 ³⁴³² CVE CVE-2008-7253 ³⁴³³ CVE CVE-2009-2823 ³⁴³⁴ CVE CVE-2010-0386 ³⁴³⁵ OSVDB 877 ³⁴³⁶ SUN 50603 ³⁴³⁷ BID 9561 ³⁴³⁸ URL1 ³⁴³⁹ URL2 ³⁴⁴⁰	Ozbiljan	Onemogućiti HTTP TRACE metodu za Apache. Novije verzije Apache-a (1.3.34 i 2.0.55 i novije) omogućuju konfiguracionu direktivu koja se zove TraceEnable. Da bis se odbili TRACE zahtevi, dodaje se sledeći red u konfiguraciji servera: TraceEnable off Za starije verzije Apache web servera, koristiti modul mod_rewrite da bi se odbili TRACE zahtevi: RewriteEngine On RewriteCond %{REQUEST_METHOD} ^TRACE RewriteRule .* - [F]
41.	Database Open Access (database-open-access)	172.23.202.195: 3306 172.23.202.196: 3306 172.23.202.221: 3306 172.23.202.222: 3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posedovanje baza	URL1 ³⁴⁴¹	Umeren	Konfigurisati server baze podataka tako da se dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.

³⁴²⁵ <http://www.securityfocus.com/bid/30339>³⁴²⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-3259>³⁴²⁷ <http://secunia.com/advisories/31179/>³⁴²⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2320>³⁴²⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2763>³⁴³⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-3398>³⁴³¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-4683>³⁴³² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3008>³⁴³³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-7253>³⁴³⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2823>³⁴³⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0386>³⁴³⁶ <http://osvdb.org/887>³⁴³⁷ <https://sunsolve.sun.com/search/document.do?assetkey=1-22-50603-1> pristupljeno 18.12.2011³⁴³⁸ <http://www.securityfocus.com/bid/9561>³⁴³⁹ <http://www.apacheweek.com/issues/03-01-24#news>³⁴⁴⁰ <http://www.kb.cert.org/vuls/id/867593>³⁴⁴¹ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf

		podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7.			
42.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	CVE CVE-1999-0524 ³⁴⁴² OSVDB 95 ³⁴⁴³ XF icmp-netmask(306) ³⁴⁴⁴ XF icmp-timestamp(322) ³⁴⁴⁵	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
43.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom, koristi se za procenu vremena neprekidnog rada udaljenog hosta (što zlonamerni napadač može iskoristiti pri planiranju daljih napada). Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1 ³⁴⁴⁶ URL2 ³⁴⁴⁷ URL3 ³⁴⁴⁸	Umeren	Onemogućiti TCP vremenske pečate na Linux-u. Podesiti vrednost net.ipv4.tcp_timestamps na 0 pokretanjem sledeće komande: sysctl -w net.ipv4.tcp_timestamps=0 Uz to, sledeću vrednost postaviti u difoltni sysctl konfiguracioni fajl, uopšteno sysctl.conf: net.ipv4.tcp_timestamps=0
44.	WebDAV Extensions are Enabled (http-generic-webdav-enabled)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 WebDAV je skup ekstenzija za HTTP protokol koji omogućava korisnicima da zajednički edituju i obrađuju fajlove na udaljenim web serverima. Mnogi web serveri po difoltu omogućavaju WebDAV ekstenzije, čak i kada nisu potrebne. S obzirom na dodatnu složenost, dosadašnja praksa je pokazala da treba onemogućiti WebDAV ukoliko se trenutno ne koristi.		Umeren	Apache: Potrebno je onemogućiti WebDAV ³⁴⁴⁹ (eng. Web-based Distributed Authoring and Versioning) za Apache. Proveriti da li je mod_dav modul isključen ili utvrditi da li postoji zahtevana autentifikacija na direktorijumima nad kojima se zahteva DAV. Apache Tomcat, Tomcat, Tomcat Web Server Onemogućiti WebDAV za Apache Tomcat. Isključiti WebDAV Servlet ³⁴⁵⁰ za sve web aplikacije koje se nalaze na web serveru. To se može uraditi tako što se ukloni definicija servlet-a za

³⁴⁴² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>³⁴⁴³ <http://www.osvdb.org/95>³⁴⁴⁴ <http://xforce.iss.net/xforce/xfdb/306>³⁴⁴⁵ <http://xforce.iss.net/xforce/xfdb/322>³⁴⁴⁶ http://www.forensicswiki.org/wiki/TCP_timestamps³⁴⁴⁷ <http://www.ietf.org/rfc/rfc1323.txt>³⁴⁴⁸ <http://uptime.netcraft.com/>³⁴⁴⁹ WebDAV je otvoreni standar za nabavku i prenos podataka putem računarskih mreža. Pri tome korisnici vizuelno dolaze do podataka kao da su na sopstvenom računaru. Preuzeto iz : <http://sr.wikipedia.org/sr/WebDAV> , 12.09.2012.³⁴⁵⁰ Servlet je objekat programskog jezika Java koji dinamički obrađuje zahteve i konstruiše odgovor na zahtev. Java servlet API omogućava Java programerima da dodaju dinamički sadržaj Web serveru korišćenjem Java platforme. Servlet najčešće generiše HTML kod, ali to može biti i XML ili nešto slično. Preuzeto iz : <http://sr.wikipedia.org/sr/Servlet>

					WebDAV (kategorija org.apache.catalina.servlets.WebdavServlet) i uklone sve servlet mape koje se pozivaju na WebDAV servlet.
45.	Apache HTTPD: CRLF injection in mod_negotiation when untrusted uploads are supported (CVE-2008-0456) (apache-httpd-cve-2008-0456)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_negotiation. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Moguće je ubaciti CRLF (Carriage Return and Line Feed) koji omogućava CRLF Injection napade (poznatih i kao HTTP Response Splitting) za sajtove koji koriste mod_negotiation, omogućavajući neproverene upload-ove na lokacije na kojima je omogućen MultiViews (višestruko pregledanje).	APPLE APPLE-SA-2009-05-12 ³⁴⁵¹ BID 27409 ³⁴⁵² CERT TA09-133A ³⁴⁵³ CVE CVE-2008-0456 ³⁴⁵⁴ SECUNIA 29348 ³⁴⁵⁵ SECUNIA 35074 ³⁴⁵⁶ XF 39893 ³⁴⁵⁷ URL1 ³⁴⁵⁸	Umeren	Apache HTTPD >= 2.2 and < 2.2.12 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

Tabela 80. Linux OS – Pronađeni servisi na IP adresi 172.23.202.195 (2011. godina)

SERVISI	FTP 172.23.202.195 tcp 21 vsFTPD 2.0.5 ftp.banner: 220 (vsFTPD 2.0.5) HTTP 172.23.202.195 tcp 80 Apache 2.2.3 WebDAV: http.banner: Apache/2.2.3 (Red Hat) http.banner.server: Apache/2.2.3 (Red Hat) MySQL 172.23.202.195 tcp 3306 SSH 172.23.202.195 tcp 22 OpenSSH 4.3 ssh.banner: SSH-2.0-OpenSSH_4.3 ssh.protocol.version: 2.0 Portmapper³⁴⁵⁹ : 172.23.202.195 tcp 111 program-number: 100000 program-version: 2 172.23.202.195 udp 111 program-number: 100000 program-version: 2 STATUS: 172.23.202.195 udp 774 program-number: 100024

³⁴⁵¹ <http://lists.apple.com/archives/security-announce/2009/May/msg00001.html>³⁴⁵² <http://www.securityfocus.com/bid/27409>³⁴⁵³ <http://www.us-cert.gov/ncas/alerts/ta09-133a>³⁴⁵⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0456>³⁴⁵⁵ <http://secunia.com/advisories/29348/>³⁴⁵⁶ <http://secunia.com/advisories/35074/>³⁴⁵⁷ <http://xforce.iss.net/xforce/xfdb/39893>³⁴⁵⁸ http://httpd.apache.org/security/vulnerabilities_22.html³⁴⁵⁹ The Remote Procedure Call portmapper is a service that maps RPC programs to specific ports, and provides that information to client programs. Since most RPC programs do not have a well defined port number, they are dynamically allocated a port number when they are first run. Any client program that wishes to use a particular RPC program first contacts the portmapper to determine the port and protocol of the specified RPC program. The client then uses that information to contact the RPC program directly. In addition some implementations of the portmapper allow tunneling commands to RPC programs through the portmapper.

	program-version: 1 172.23.202.195 tcp 777 program-number: 100024 program-version: 1
Spidered Web site	http://172.23.202.195:80 Common Default URLs: <i>Access Error (403)</i> cgi-bin error <i>Successful (200)</i> Icons Guessed URLs <i>Access Error (403)</i> ?P=+ADw-script+AD4-alert(42)+Adw script+AD4- script+AD4- script+AD4- cgi-bin error <i>Redirect (301)</i> icons small <i>Successful (200)</i> icons ?P=+ADw-script+AD4-alert(42)+Adw script+AD4- script+AD4- README small README Linked URLs <i>Access Error (403)</i> <i>Successful (200)</i> icons small

Tabela 81. Linux OS – Pronađeni servisi na IP adresi 172.23.202.196 (2011. godina)

SERVISI	FTP 172.23.202.196 tcp 21 vsFTPD 2.0.5 ftp.banner: 220 (vsFTPD 2.0.5) HTTP 172.23.202.196 tcp 80 Apache 2.2.3 WebDAV: http.banner: Apache/2.2.3 (Red Hat) http.banner.server: Apache/2.2.3 (Red Hat) MySQL 172.23.202.196 tcp 3306 SSH 172.23.202.196 tcp 22 OpenSSH 4.3 ssh.banner: SSH-2.0-OpenSSH_4.3 ssh.protocol.version: 2.0

	Portmapper³⁴⁶⁰ : 172.23.202.196 tcp 111 program-number: 100000 program-version: 2 172.23.202.196 udp 111 program-number: 100000 program-version: 2 STATUS: 172.23.202.196 udp 774 program-number: 100024 program-version: 1 172.23.202.196 tcp 777 program-number: 100024 program-version: 1
Spidered Web site	http://172.23.202.196:80 Common Default URLs: <i>Access Error (403)</i> cgi-bin error <i>Successful (200)</i> Icons Guessed URLs <i>Access Error (403)</i> ?P=+ADw-script+AD4-alert(42)+Adw script+AD4- script+AD4- script+AD4- cgi-bin error <i>Redirect (301)</i> icons small <i>Successful (200)</i> icons ?P=+ADw-script+AD4-alert(42)+Adw script+AD4- script+AD4- README small README Linked URLs <i>Access Error (403)</i> <i>Successful (200)</i> icons small

Tabela 82. Linux OS – Pronađeni servisi na IP adresi 172.23.202.221 (2011. godina)

SERVISI	FTP 172.23.202.221 tcp 21 vsFTPD 2.0.5 ftp.banner: 220 (vsFTPD 2.0.5) HTTP 172.23.202.221 tcp 80 Apache 2.2.3

³⁴⁶⁰ The Remote Procedure Call portmapper is a service that maps RPC programs to specific ports, and provides that information to client programs. Since most RPC programs do not have a well defined port number, they are dynamically allocated a port number when they are first run. Any client program that wishes to use a particular RPC program first contacts the portmapper to determine the port and protocol of the specified RPC program. The client then uses that information to contact the RPC program directly. In addition some implementations of the portmapper allow tunneling commands to RPC programs through the portmapper.

	WebDAV: http.banner: Apache/2.2.3 (Red Hat) http.banner.server: Apache/2.2.3 (Red Hat) MySQL 172.23.202.221 tcp 3306 SSH 172.23.202.221 tcp 22 OpenSSH 4.3 ssh.banner: SSH-2.0-OpenSSH_4.3 ssh.protocol.version: 2.0 Portmapper³⁴⁶¹ : 172.23.202.221 tcp 111 program-number: 100000 program-version: 2 172.23.202.221 udp 111 program-number: 100000 program-version: 2 STATUS: 172.23.202.221 udp 774 program-number: 100024 program-version: 1 172.23.202.221 tcp 777 program-number: 100024 program-version: 1
Spidered Web site	http://172.23.202.221:80 Common Default URLs: <i>Access Error (403)</i> cgi-bin error <i>Successful (200)</i> Icons Guessed URLs <i>Access Error (403)</i> ?P=+ADw-script+AD4-alert(42)+Adw-script+AD4-script+AD4-script+AD4-cgi-bin-error <i>Redirect (301)</i> icons small <i>Successful (200)</i> icons ?P=+ADw-script+AD4-alert(42)+Adw-script+AD4-script+AD4-README small README Linked URLs <i>Access Error (403)</i> <i>Successful (200)</i> icons small

³⁴⁶¹ The Remote Procedure Call portmapper is a service that maps RPC programs to specific ports, and provides that information to client programs. Since most RPC programs do not have a well defined port number, they are dynamically allocated a port number when they are first run. Any client program that wishes to use a particular RPC program first contacts the portmapper to determine the port and protocol of the specified RPC program. The client then uses that information to contact the RPC program directly. In addition some implementations of the portmapper allow tunneling commands to RPC programs through the portmapper.

Tabela 83. Linux OS – Pronađeni servisi na IP adresi 172.23.202.222 (2011. godina)

SERVISI	FTP 172.23.202.222 tcp 21 vsFTPd 2.0.5 ftp.banner: 220 (vsFTPd 2.0.5) HTTP 172.23.202.222 tcp 80 Apache 2.2.3 WebDAV: http.banner: Apache/2.2.3 (Red Hat) http.banner.server: Apache/2.2.3 (Red Hat) MySQL 172.23.202.222 tcp 3306 SSH 172.23.202.222 tcp 22 OpenSSH 4.3 ssh.banner: SSH-2.0-OpenSSH_4.3 ssh.protocol.version: 2.0 Portmapper³⁴⁶² ; 172.23.202.222 tcp 111 program-number: 100000 program-version: 2 172.23.202.222 udp 111 program-number: 100000 program-version: 2 STATUS: 172.23.202.222 udp 774 program-number: 100024 program-version: 1 172.23.202.222 tcp 777 program-number: 100024 program-version: 1
Spidered Web site	http://172.23.202.222:80 Common Default URLs: <i>Access Error (403)</i> cgi-bin error <i>Successful (200)</i> Icons Guessed URLs <i>Access Error (403)</i> ?P=+ADw-script+AD4-alert(42)+Adw script+AD4- script+AD4- script+AD4- cgi-bin error <i>Redirect (301)</i> icons small <i>Successful (200)</i> icons ?P=+ADw-script+AD4-alert(42)+Adw script+AD4- script+AD4-

³⁴⁶² The Remote Procedure Call portmapper is a service that maps RPC programs to specific ports, and provides that information to client programs. Since most RPC programs do not have a well defined port number, they are dynamically allocated a port number when they are first run. Any client program that wishes to use a particular RPC program first contacts the portmapper to determine the port and protocol of the specified RPC program. The client then uses that information to contact the RPC program directly. In addition some implementations of the portmapper allow tunneling commands to RPC programs through the portmapper.

	README small README Linked URLs Access Error (403) Successful (200) icons small

Tabela 84. Linux OS sa IP adresama 172.23.202.122, 172.23.202.232, 172.23.202.200, 172.23.202.230, 172.23.202.135, 172.23.202.231 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara		Broj ranjivosti	
IP adresa: 172.23.202.122		OS: Kubuntu 11.04 x86 desktop, kubun1104dskx86		22	
IP adresa: 172.23.202.232		OS: Kubuntu 11.04 x86 desktop, kubun1104dskx64		22	
IP adresa: 172.23.202.200		OS: Ubuntu 11.04 x64 desktop, ubunt1104dskx64		22	
IP adresa: 172.23.202.230		OS: Ubuntu 11.04 x86 desktop, ubunt1104dskx86		22	
IP adresa: 172.23.202.135		OS: Ubuntu 11.04 x64 server, ubunt1104srvx64		22	
IP adresa: 172.23.202.231		OS: Ubuntu 11.04 x86 server, ubunt1104srvx86		22	
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Anonymous users can obtain the Windows password policy (cifs-nt-0002)	Korišćenjem CIFS NULL sesije, anonimni korisnik može da dobije uvid u polisu šifri. Polisa šifri sadrži osetljive informacije o najmanjoj mogućoj dužini lozinke, zaključavanje šifre, vremensko trajanje zaključanosti šifre itd.	SANS-01 W5 ³⁴⁶³ CVE CVE-2000-1200 ³⁴⁶⁴ XF nt-lsa-domain-sid(4015) ³⁴⁶⁵ SANS-02 W5 ³⁴⁶⁶ BID 959 ³⁴⁶⁷ SANS-04 W3 ³⁴⁶⁸ SANS-03 W5 ³⁴⁶⁹ BID 87 ³⁴⁷⁰	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost
2.	HTTP Basic Authentication Enabled (http-basic-auth-cleartext)	172.23.202.122:8080 172.23.202.232:8080 172.23.202.200:8080 172.23.202.230:8080 172.23.202.135:8080 172.23.202.231:8080 HTTP Basic Authentication šema se ne smatra sigurnom metodom autentifikacije korisnika (ukoliko se ne koristi u kombinaciji sa nekim spoljnim sigurnosnim sistemom, kao TLS/SSL), s obzirom da se korisničko ime i lozinka preko mreže prenose kao običan tekst. Primer:	URL1 ³⁴⁷¹	Kritičan	Koristiti Osnovnu Autentifikaciju preko TLS/SSL (HTTPS). Omogućiti HTTPS na Web serveru. TLS/SSL protokol će zaštititi akreditivne osnovne autentifikacije u običnom tekstu. Koristiti Digest Authentication Replace Basic Authentication sa alternativnom Digest Authentication shemom. Po savremenim kriptografskim standardima, Digest

³⁴⁶³ <http://www.sans.org/critical-security-controls/#w5>

³⁴⁶⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2000-1200>

³⁴⁶⁵ <http://xforce.iss.net/xforce/xfdb/4015>

³⁴⁶⁶ <http://www.sans.org/critical-security-controls/#w5>

³⁴⁶⁷ <http://www.securityfocus.com/bid/959>

³⁴⁶⁸ <http://www.sans.org/critical-security-controls/#w3>

³⁴⁶⁹ <http://www.sans.org/critical-security-controls/#w5>

³⁴⁷⁰ <http://www.securityfocus.com/bid/87>

³⁴⁷¹ <http://tools.ietf.org/html/rfc2617>

		Pokretanje ranjivog HTTP servisa. http://172.23.202.122:8080/manager/html 1: Basic realm="Tomcat Manager Application"			Authentication je slaba. Ali za širok spektar namena, ona je korisna zamena za Basic Authentication (osnovnu autentifikaciju). Ona ispravlja neke, ali ne sve, slabosti Basic Authentication (osnovne autentifikacije). Videti RFC 2617 ³⁴⁷² (odjeljak 4 Security Considerations) za više informacija.
3.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.122:139 172.23.202.122:445 172.23.202.232:139 172.23.202.232:445 172.23.202.200:139 172.23.202.200:445 172.23.202.230:139 172.23.202.230:445 172.23.202.135:139 172.23.202.135:445 172.23.202.231:139 172.23.202.231:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB 887429 URL1 ³⁴⁷³	Ozbiljan	Metoda za konfigurisanje SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429 ³⁴⁷⁴ . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracionom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing = auto</i> ili da se zahteva SMB potpisivanje: <i>server signing = mandatory</i>
4.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.122:139 172.23.202.122:445 172.23.202.232:139 172.23.202.232:445 172.23.202.200:139 172.23.202.200:445 172.23.202.230:139 172.23.202.230:445 172.23.202.135:139 172.23.202.135:445 172.23.202.231:139 172.23.202.231:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti
5.	X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch)	172.23.202.122:993 172.23.202.122:995 172.23.202.232:993 172.23.202.232:995 172.23.202.200:993 172.23.202.200:995 172.23.202.230:993 172.23.202.230:995 172.23.202.135:993 172.23.202.135:995 172.23.202.231:993 172.23.202.231:995 Rubrika u sertifikatu X.509 sa uobičajenim nazivom subjekta (CN)		Ozbiljan	Rubrika sa uobičajenim nazivom subjekta (CN) u sertifikatu X.509 treba da bude podešena da sadrži ime pojedinca koji prikazuje sertifikat (npr. ime hosta). To se postiže izradom novog sertifikata, koji najčešće potpisuje Certification Authority (CA), koji je od poverenja kako za klijenta, tako i za server.

³⁴⁷² <http://tools.ietf.org/html/rfc2617#section-4>³⁴⁷³ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>³⁴⁷⁴ <http://support.microsoft.com/kb/887429>

		ne poklapa se sa imenom pojedinca koje je navedeno u sertifikatu. Pre izdavanja sertifikata, Certification Authority (CA) mora da proveri identitet pojedinca koji potražuje sertifikat, kako je navedeno u CA-ovom Certification Practice Statement (CPS). Zbog toga, uobičajene procedure validacije sertifikata zahtevaju da rubrika sertifikata sa CN subjektom odgovara pravom imenu pojedinca koji prikazuje sertifikat. Na primer, u sertifikatu prikazanom na „https://www.example.com/“, naziv subjekta (CN) treba da bude „www.example.com“. U cilju otkrivanja i sprečavanja napada prisluškivanja, validnost sertifikata mora da bude overena, jer bi u suprotnom napadač mogao da otpočne napad preko posrednika i da stekne potpunu kontrolu nad protokom podataka. Od posebne važnosti je validnost naziva subjekta (CN), koji treba da se poklapa sa imenom pojedinca (imenom host-a). Neodgovarajući CN se najčešće javlja usled greške u konfiguraciji, iako on takođe može da ukazuje na to da se sprovodi napad preko posrednika.			
6.	FTP server does not support AUTH command (ftp-generic-0007)	172.23.202.122:21 172.23.202.232:21 172.23.202.200:21 172.23.202.230:21 172.23.202.135:21 172.23.202.231:21 Klijenti na FTP server po defaultu šalju poverljive podatke (korisnički ID i šifru) u vidu čitkog teksta. Ova okolnost dozvoljava zlonamernim korisnicima omogućava da presreću poverljive podatke ukoliko prisluškuju vezu. Noviji FTP serveri podržavaju komandu AUTH, koja daje veće opcije autentifikacije, kao TLS, Kerberos, GSSAPI, itd. Njih treba koristiti da bi se sprečilo prisluškivanje na FTP vezama.		Ozbiljan	Nadograditi/Ažurirati na a FTP server koji podržava komandu AUTH.
7.	Browsable web directory (http-generic-browsable-dir)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80 172.23.202.231:80 Otkriven je direktorijum na web serveru koji može biti pretraživan, što znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice - spajdering (prateći hiperlinkove), ili -kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute force napadom na liste		Ozbiljan	Za Apache: onemogućiti brauzovanje direktorijuma mreže za sve direktorijume i poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim ako postoji

		uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skriven“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice. Primer: <pre> http://172.23.202.122/icons/small/ 4: <title>Index of /icons/small</title> 5: </head> 6: <body> 7: <h1>Index of /icons/small</h1> 8: ...COJ]></th><th>Name</th><th><a href="?C=M;O=A... </pre>			potreba da ovi fajlovi budu dostupni preko web-a. Povremeno proći kroz web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastsareo, kao i nepoznate fajlove i direktorijume. Za Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote: Onemogućiti brauzovanje direktorijuma mreže za sve direktorijume i poddirektorijume. Uključiti Tomcat-ov web.xml file. U odeljku „default“, promeniti parametar „listings“ iz „true“ u „false“. Restartovati server. Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim ako ne postoji potreba da ovi fajlovi budu dostupni preko web-a. Povremeno proći kroz web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastsareo, kao i nepoznate fajlove i direktorijume.
8.	Form action submits sensitive data in the clear (http-generic-sensitive-form-data-unencrypted)	172.23.202.122:8080 172.23.202.232:8080 172.23.202.200:8080 172.23.202.230:8080 172.23.202.135:8080 172.23.202.231:8080 Web forma sadrži rubrike sa podacima koji su možda po prirodi osetljivi. Ovakvi podaci se prenose preko nezaštićene veze, koja bi mogla da omogućiti zlonamernim napadačima da prisluškujući mrežu pregledaju podatke u vidu običnog teksta. Formatiranje preko http://localhost:8080/examples/jsp/security/protected/vti_shm/j_security_check prosleđuje sledeće nezaštićene osetljive rubrike: j_password		Ozbiljan	Isključiti HTTPS protokol na serveru. Promeniti „action“ URL na oznaci rubrike da koristi HTTP protokol („http://...“) umesto samo HTTP protokol („http://...“). Sve osetljive podatke treba slati preko HTTP umesto preko HTTPS.
9.	TLS/SSL Server Supports Weak Cipher Algorithms (ssl-weak-ciphers)	172.23.202.122:993 172.23.202.232:993 172.23.202.200:993 172.23.202.230:993 172.23.202.135:993 172.23.202.231:993 negotiated the SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA cipher suite 172.23.202.122:995 172.23.202.232:995 172.23.202.200:995		Ozbiljan	Konfigurisati server tako da onemogući podršku za slabe šifre. Za Apache web servere sa mod_ssl, uključiti fajl Apache konfiguracije i izmeniti liniju SSLCipherSuite tako da u njoj piše: ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM

		172.23.202.230:995 172.23.202.135:995 172.23.202.231:995 negotiated the SSL_DHE_RSA_EXPORT_WITH_ DES40_CBC_SHA cipher suite TLS/SSL server podržava šifre koje se zasnivaju na slabim algoritmima. To napadaču može omogućiti da pokrene napade preko posrednika i da pregleda ili čačka osetljive podatke. Uopšteno, sledeće šifre se smatraju slabim: Tzv. „null“ (nula) šifre, jer ne šifruju podatke. Eksportne šifre koje koriste dužine tajnih ključeva ograničene na 40 bitova. Na to najčešće ukazuje reč EXP/EXPORT u nazivu šifre. Zastareli algoritmi za šifrovanje čije se dužine tajnih ključeva po današnjim standardima smatraju kratkim, npr. DES ili RC4 sa 56-bitnim ključevima.			
10.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	TCP reset with incorrect sequence number triggered this fault on 172.23.202.122:21 172.23.202.232:21 172.23.202.200:21 172.23.202.230:21 172.23.202.135:21 172.23.202.231:21 Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hедера i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183³⁴⁷⁵ CERT-VN: 415294³⁴⁷⁶ CVE CVE-2004-0230³⁴⁷⁷ MS: MS05-019³⁴⁷⁸ MS: MS06-064³⁴⁷⁹ NETBSD: NetBSD-SA2004-006³⁴⁸⁰ OVAL: OVAL2689³⁴⁸¹ OVAL: OVAL270³⁴⁸² OVAL OVAL3508³⁴⁸³ OVAL OVAL4791³⁴⁸⁴ OVAL OVAL5711³⁴⁸⁵ SECUNIA: 11440³⁴⁸⁶ SECUNIA 11458³⁴⁸⁷ SECUNIA: 22341³⁴⁸⁸ SGI 20040403-01-A³⁴⁸⁹ XF tcp-rst-dos(15886)³⁴⁹⁰ URL1³⁴⁹¹ URL2³⁴⁹²	Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC 2385 . ³⁴⁹³ Ono je napravljeno da smanji opasnost od određenih napada na BGP, kao što su TCP reseti.
11.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podesi na	BID 4314³⁴⁹⁴ CVE CVE-2002-0510³⁴⁹⁵ XF linux-udp-	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili pak ranjivost koju treba

³⁴⁷⁵ <http://www.securityfocus.com/bid/10183>³⁴⁷⁶ <http://www.kb.cert.org/vuls/id/415294>³⁴⁷⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>³⁴⁷⁸ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>³⁴⁷⁹ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>³⁴⁸⁰ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>³⁴⁸¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>³⁴⁸² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>³⁴⁸³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>³⁴⁸⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>³⁴⁸⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>³⁴⁸⁶ <http://secunia.com/advisories/11440/>³⁴⁸⁷ <http://secunia.com/advisories/11458/>³⁴⁸⁸ <http://secunia.com/advisories/22341/>³⁴⁸⁹ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>³⁴⁹⁰ <http://xforce.iss.net/xforce/xfdb/15886>³⁴⁹¹ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>³⁴⁹² <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>³⁴⁹³ <http://www.ietf.org/rfc/rfc2385.txt>³⁴⁹⁴ <http://www.securityfocus.com/bid/4314>³⁴⁹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>

		jedinstvenu vrednost i da se koristi u rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da fingerprint-uje operativni sistem.	fingerprint(8588) ³⁴⁹⁶		popravljanje, tako da ne postoje rešenja koja se mogu kupiti. Jedino se može postaviti fajervol ili neka druga sprava za filtriranje između napadnutog i neprijateljskog napada koji je u mogućnosti da randomizuje IP ID-jeve.
12.	Apache httpd apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpd-cve-2011-0419)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80 172.23.202.231:80 Skenirani servis je osjetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_autoindex. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_fnmatch() u sklopu APR biblioteke. Ako je omogućen mod_autoindex, a indeksi direktorijuma mod_autoindex su sadržavali fajlove sa dovoljno dugim nazivima, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do preterane upotrebe CPU-a. Ovo bi moglo da bude iskorišćeno u napadu odbijanja servisa. Zahvaljujući Maksymilian Arciemowicz-u prijavljen je ovaj propust.	CVE CVE-2011-0419 ³⁴⁹⁷ REDHAT RHSA-2011:0507 ³⁴⁹⁸ SECUNIA 44490 ³⁴⁹⁹ SECUNIA 44564 ³⁵⁰⁰ SECUNIA 44574 ³⁵⁰¹ URL1 ³⁵⁰²	Ozbiljan	Apache >= 2.2 and < 2.3 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.18.tar.gz
13.	Apache Etag Inode Information Leakage (http-apache-etag-inode-leak)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80 172.23.202.231:80 U određenim konfiguracijama, Apache HTTP server dozvoljava udaljenim napadačima da dobiju poverljive informacije preko (1) Etag heder-a, koji otkriva broj inoda ili (2) razdvajanje višedelnih MIME-a, koja ukazuje na ID child procesa (PID). Određene verzije Apache-a koriste zahtevani broj čvorova fajla da bi konstruisali 'Etag' heder za odgovor. Iako sama po sebi nije ranjivost, ova informacija olakšava sprovođenje određenih NFS napada. „Running vulnerable HTTP service: Apache 2.2.17.	BID 6939 ³⁵⁰³ BID 6943 ³⁵⁰⁴ CVE CVE-2003-1418 ³⁵⁰⁵ XF apache-mime-information-disclosure(11438) ³⁵⁰⁶	Ozbiljan	Onemogućiti Etag mehanizam ³⁵⁰⁷ tipa "inod-based" konfiguraciji Apache-a. Takođe, inod informacije je moguće ukloniti iz Etag heder-a tako što će se dodati direktiva u Apache konfiguraciju: <i>FileETag Mtime Size</i>

³⁴⁹⁶ <http://xforce.iss.net/xforce/xfdb/8588>³⁴⁹⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419>³⁴⁹⁸ <http://rhn.redhat.com/errata/RHSA-2011-0507.html>³⁴⁹⁹ <http://secunia.com/advisories/44490/>³⁵⁰⁰ <http://secunia.com/advisories/44564/>³⁵⁰¹ <http://secunia.com/advisories/44574/>³⁵⁰² http://httpd.apache.org/security/vulnerabilities_22.html³⁵⁰³ <http://www.securityfocus.com/bid/6939>³⁵⁰⁴ <http://www.securityfocus.com/bid/6943>³⁵⁰⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-1418>³⁵⁰⁶ <http://xforce.iss.net/xforce/xfdb/11438>³⁵⁰⁷ Entity tags predstavljaju mehanizam koji web serveri i web pretraživači koriste da se utvrdi da li komponenta u kešu pretraživača odgovara poreklu servera sa kojeg je poslata.

		http://172.23.202.206/1:c2979-b1-4a76e5063f807			
14.	Apache Tomcat v4.x Example Scripts Information Leakage (http-tomcat-0005)	172.23.202.122:8080 172.23.202.232:8080 172.23.202.200:8080 172.23.202.230:8080 172.23.202.135:8080 172.23.202.231:8080 Sledeći primeri skripti dolaze uz Apache Tomcat v4.x a napadači ih mogu iskoristiti da bi dobili informacije o sistemu. Ove skripte su takode ranjive na XSS napade: /examples/jsp/num/numguess.jsp /examples/jsp/dates/date.jsp /examples/jsp/snp/snoop.jsp /examples/jsp/error/error.html /examples/jsp/sessions/carts.html /examples/jsp/checkbox/check.html /examples/jsp/colors/colors.html /examples/jsp/cal/login.html /examples/jsp/include/include.jsp /examples/jsp/forward/forward.jsp /examples/jsp/plugin/plugin.jsp /examples/jsp/sptoserv/sptoservlet.jsp /examples/jsp/simpletag/foo.jsp /examples/jsp/mail/sendmail.jsp /examples/servlet/HelloWorldExample /examples/servlet/RequestInfoExample /examples/servlet/RequestHeaderExample /examples/servlet/RequestParamExample /examples/servlet/CookieExample /examples/servlet/JndiServlet /examples/servlet/SessionExample /tomcat-docs/appdev/sample/web/hello.jsp „Running vulnerable HTTP service: Apache Tomcat. http://172.23.202.122:8080/examples/jsp/sessions/carts.html 24: 25: 26: <form type=POST action=carts.jsp> 27:
 28: Please enter item to add or remove.“		Kritičan	Potpuno izbrisati ove skripte. Primeri skripti nikada ne treba da budu instalirani na proizvodnim serverima.
15.	Self-signed TLS/SSL certificate (ssl-self-signed-certificate)	172.23.202.122:993 172.23.202.122:995 172.23.202.232:993 172.23.202.232:995 172.23.202.200:993 172.23.202.200:995 172.23.202.230:993 172.23.202.230:995 172.23.202.135:993 172.23.202.135:995 172.23.202.231:993 172.23.202.231:995 TLS/SSL-a sertifikat servera je samopotpisan. Samopotpisani		Ozbiljan	Nabaviti novi TLS/SSL serverov sertifikat koji NIJE samopotpisan i instalirati ga na server. Precizna uputstva za dobijanje novog sertifikata zavise od zahteva organizacije. Uopšteno, treba napraviti zahtev za sertifikat i taj zahtev sačuvati kao fajl. Ovaj fajl se zatim šalje Certificate Authority-ju (CA) na obradu. Organizacija možda poseduje sopstveni interni Certificate Authority. U

		sertifikati po defaultu nisu od poverenja, naročito zato što napadi na TLS/SSL preko posrednika obično koriste samopotpisane sertifikate da prisluškuju TLS/SSL veze.			suprotnom, potrebno je platiti sertifikat iz spoljnog poverljivog Certificate Authority-ja, kao što su Thawte , Verisign .
16.	Autocomplete enabled for sensitive HTML form fields (spider-sensitive-form-data-autocomplete-enabled)	172.23.202.122:8080 172.23.202.232:8080 172.23.202.200:8080 172.23.202.230:8080 172.23.202.135:8080 172.23.202.231:8080 Web forma sadrži lozinke i druge rubrike sa osetljivim tekstom za koje je otvorena mogućnost auto-complete od strane web pretraživača. Funkcija auto-complete skladišti forme popunjenih rubrika i lozinke lokalno, na web pretraživaču, tako da se ove rubrike automatski popunjavaju kada korisnik ponovo poseti sajt. Osetljivi podaci i lozinke mogu biti ukradeni ako je korisnikov sistem kompromitovan. Međutim, treba imati u vidu da forma auto-complete nije standardna i da je to karakteristika web pretraživača koju svaki web pretraživač tretira na različit način. Na primer Opera zanemaruje ovu opciju i zahteva od korisnika da unese poverljive podatke svaki put kada posećuje određeni web sajt.		Umeren	Za svaku osetljivu rubriku u HTML, stavku „autocomplete“ potrebno je podesiti na „off“. Na primer: <pre><input type="password" autocomplete="off" name="pw"></pre> Ako ima previše rubrika, možda je brže podesiti stavku „autocomplete“ na „off“ u spoljnom tagu <form>. Na primer: <pre><form action="/login.jsp" autocomplete="off" name="pw"> <input type="password" name="pw"> </form></pre>
17.	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server. Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko poziva udaljenih procedura (RPC). Ovi servisi su i u prošlosti bili skloni ranjivostima.. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu omogućiti da sprovedu i mnogo prefinjenije napade. Primer: <pre>Found user(s): nobody root vanja Found server name: UBUNT1104DSKX64 Found local group(s): Found policy for domain(s): UBUNT1104DSKX64 Builtin</pre>	BID: 494³⁵⁰⁸ CVE: CVE-1999-0519³⁵⁰⁹ MSKB: 143474³⁵¹⁰ URL1³⁵¹¹	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost.
18.	Apache default installation/welcome	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80	OSVDB 2117 ³⁵¹²	Umeren	Ako se od servera zahteva da obezbedi neophodnu funkcionalnost, onda

³⁵⁰⁸ <http://www.securityfocus.com/bid/494>³⁵⁰⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>³⁵¹⁰ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>³⁵¹¹ http://www.hsc.fr/ressources/presentations/null_sessions/³⁵¹² http://www.osvdb.org/displayvuln.php?osvdb_id=2117 pristupljeno 11.12.2011

	page installed (http://apache-default-install-page)	172.23.202.230:80 172.23.202.135:80 172.23.202.231:80 Apache difoltna instalacija ili „Welcome“ stranica je instalirana na serveru. To obično ukazuje na novoinstalirani server. U mnogim slučajevima, Apache se instalira zajedno sa drugim aplikacijama i korisnik možda nije svestan da je web server pokrenut. Ovakvi serveri se retko patch-uju i još rede nadgledaju, što zlonamernim napadačima postaje pogodna meta koja najverovatnije neće pokrenuti nikakvo upozorenje. Primer : Running vulnerable HTTP service: Apache 2.2.17. http://172.23.202.122/ 1: <code><html><body><h1>It works!</h1></code>			difoltnu stranicu treba zameniti odgovarajućim sadržajem. U suprotnom, ovakav server treba ukloniti sa mreže, prateći bezbednosni princip minimalne složenosti (više složenosti = manja bezbednost). Ako server nije potreban, treba ga ukloniti iz svih startup fajlova (npr. /etc/rc*) ili skripti, a zatim prekinuti servis. Proveriti da li se on ponovo pokreće kada se mašina reboot-uje. Apache se uglavnom instalira kao /usr/sbin/httpd na UNIX mašinama ili kao C:\Program Files\Apache Group na Windows mašinama. Razmotriti uklanjanje binara i svih srodnih biblioteka iz sistema.
19.	Apache Tomcat default installation/welcome page installed (http://tomcat-default-install-page)	172.23.202.122:8080 172.23.202.232:8080 172.23.202.200:8080 172.23.202.230:8080 172.23.202.135:8080 172.23.202.231:8080 Tomcat difoltna instalacija ili „Welcome“ stranica je instalirana na serveru. To obično ukazuje na novoinstalirani server. U mnogim slučajevima, Tomcat se instalira zajedno sa drugim aplikacijama i korisnik možda nije svestan da je web server pokrenut. Ovakvi serveri se retko patch-uju i još rede nadgledaju, što zlonamernim napadačima postaje pogodna meta koja najverovatnije neće pokrenuti nikakvo upozorenje. Pokretanje ranjivog HTTP servisa: Apache Tomcat. http://172.23.202.122:8080/ 8: 9: <code><body></code> 10: <code><h1>It works !</h1></code> 11: 12: ... means you've setup Tomcat successfully. Congratulations!</p>	OSVDB 2117 ³⁵¹³	Umeren	Ako se od servera zahteva da obezbedi neophodnu funkcionalnost, onda difoltnu stranicu treba zameniti odgovarajućim sadržajem. U suprotnom, ovakav server treba ukloniti sa mreže, prateći bezbednosni princip minimalne složenosti (više složenosti = manja bezbednost).
20.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatišu slabe time-based generatore slučajnih	CVE CVE-1999-0524³⁵¹⁴ OSVDB 95³⁵¹⁵ XF icmp-netmask(306)³⁵¹⁶ XF icmp-timestamp(322)³⁵¹⁷	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti

³⁵¹³ http://www.osvdb.org/displayvuln.php?osvdb_id=2117 pristupljeno 11.12.2011

³⁵¹⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>

³⁵¹⁵ <http://www.osvdb.org/95>

³⁵¹⁶ <http://xforce.iss.net/xforce/xfdb/306>

³⁵¹⁷ <http://xforce.iss.net/xforce/xfdb/322>

		brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.			detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost
21.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1³⁵¹⁸ URL2³⁵¹⁹ URL3³⁵²⁰	Umeren	Onemogućavanje TCP timestamp odgovora na Linux OS. Podesiti net.ipv4.tcp_timestamps vrednost na sledećem ključu na 0 pokretanjem sledeće komande: sysctl -w net.ipv4.tcp_timestamps=0 Dodatno, sledeću vrednost u difoltnom sysctl konfiguracionom fajlu, generally sysctl.conf: net.ipv4.tcp_timestamps=0
22	Database Open Access (database-open-access)	172.23.202.122:3306 172.23.202.232:3306 172.23.202.200:3306 172.23.202.230:3306 172.23.202.135:3306 172.23.202.231:3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7	URL1³⁵²¹	Umeren	Konfigurisati server baze podataka tako da dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.

Tabela 85. Linux OS – Pronađeni servisi na IP adresi 172.23.202.122 (2011. godina)

SERVISI	SAMBA 172.23.202.122 tcp 139 Samba 3.5.8 172.23.202.122 tcp 445 Samba 3.5.8 CIFS Name Service 172.23.202.122 udp 137 FTP 172.23.202.122 tcp 21 vsFTPD 2.3.2 ftp.banner: 220 (vsFTPD 2.3.2) HTTP 172.23.202.122 tcp 80 Apache 2.2.17 http.banner: Apache/2.2.17 (Ubuntu) http.banner.server: Apache/2.2.17 (Ubuntu) 172.23.202.122 tcp 8080 Apache Tomcat

³⁵¹⁸ http://www.forensicswiki.org/wiki/TCP_timestamps³⁵¹⁹ <http://www.ietf.org/rfc/rfc1323.txt>³⁵²⁰ <http://uptime.netcraft.com/>³⁵²¹ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf

	Coyote: 1.1 http.banner: Apache-Coyote/1.1 IMAP 172.23.202.122 tcp 143 Dovecot imap.banner: * OK [CAPABILITY IMAP4rev1 LITERAL+SASL-IR LOGIN-REFERRALS ID ENABLE STARTTLS LOGINDISABLED] Dovecot ready. IMAPS³⁵²² 172.23.202.122 tcp 993 Dovecot imap.banner: * OK [CAPABILITY IMAP4rev1 LITERAL+SASL-IR LOGIN-REFERRALS ID ENABLE AUTH=PLAIN] Dovecot ready. POP 172.23.202.122 tcp 110 0 Dovecot pop.banner: +OK Dovecot ready. POPS³⁵²³ 172.23.202.122 tcp 995 2 Dovecot pop.banner: +OK Dovecot ready. MySQL 172.23.202.122 tcp 3306 SSH 172.23.202.122 tcp 22 OpenSSH 5.8p1 ssh.banner: SSH-2.0-OpenSSH_5.8p1 ssh.protocol.version: 2.0
Spidered Web site	http://172.23.202.122:80 Common Default URLs: Access Error (403) cgi-bin Successful (200) Icons Guessed URLs Access Error (403) cgi-bin ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-doc%3f.jsp .svn Entries ADw-script AD4-alert(42) ADwscript AD4-CVS Entries Root DEADJOE Trace.axd WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config

³⁵²² Internet Message Access Protocol (IMAPS) preko TLS/SSL-a se koristi za pristupanje i obradu elektronske pošte (e-mail) korišćenjem dešifrovanih (TLS/SSL) konekcija. Kada se uspostavi TLS/SSL konekcija, koristi se standardni IMAP protokol. IMAP serveri mogu sadržavati nekoliko foldera, aka mailbox-ova, koji sadrže poruke (e-mails) za korisnike.

³⁵²³ Post Office Protocol (POP) omogućava radnim stanicama da dinamički iz mailbox servera uzvraćaju elektronsku poštu (e-mail). POPS dodaje SSLpodršku POP3.

	<i>Redirect (301)</i> icons small <i>Successful (200)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-script+AD4- icons small index.html Linked URLs <i>Successful (200)</i> icons README README.html Small http://172.23.202.122:8080 Common Default URLs <i>Successful (200)</i> docs examples Guessed URLs <i>Error (400)</i> examples jsp cal cal1.jsp%00 cal1.jsp%5C checkbox checkresult.jsp%00 checkresult.jsp%5C colors colrs.jsp%00 colrs.jsp%5C dates date.jsp%00 date.jsp%5C error err.jsp%00 err.jsp%5C forward forward.jsp%00 forward.jsp%5C include include.jsp%00 include.jsp%5C jsp2 el basic-arithmetic.jsp%00 basic-arithmetic.jsp%5C basic-comparisons.jsp%00 basic-comparisons.jsp%5C functions.jsp%00 functions.jsp%5C

	implicit-objects.jsp%00 jspattribute jspattribute.jsp%00 jspattribute.jsp%5C shuffle.jsp%00 shuffle.jsp%5C misc config.jsp%00 config.jsp%5C dynamicattrs.jsp%00 dynamicattrs.jsp%5C simpletag book.jsp%00 book.jsp%5C hello.jsp%00 hello.jsp%5C repeat.jsp%00 repeat.jsp%5C foo.jsp%00 foo.jsp%5C tagfiles hello.jsp%00 hello.jsp%5C panel.jsp%00 panel.jsp%5C products.jsp%00 products.jsp%5C jsptoserv jsptoservlet.jsp%00 num numguess.jsp%00 numguess.jsp%5C plugin plugin.jsp%00 plugin.jsp%5C sessions carts.jsp%00 carts.jsp%5C snp snoop.jsp%00 snoop.jsp%5C tagplugin choose.jsp%00 choose.jsp%5C foreach.jsp%00 foreach.jsp%5C if.jsp%00 if.jsp%5C xml xml.jsp%00 xml.jsp%5C Error (500) examples jsp error errorpage.jsp Redirect (302) examples examples manager Requires Authentication (401) manager jmxproxy

	%3f.jsp .svn entries ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4- ADw-script AD4-alert(42) ADwscript AD4- CVS Entries Root DEADJOE WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config Successful (200) ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4- script+AD4- script+AD4- script+AD4- script+AD4- script+AD4- docs api appdev sample index.html architecture Linked URLs Error (500) examples jsp jsp2 el functions.jsp?foo=JSP+2.0 functions.jsp?foo=JSP+2.0 implicit-objects.jsp?foo=bar implicit-objects.jsp?foo=bar jspx textRotate.jspx textRotate.jspx?name=JSPX tagfiles products.jsp Redirect (302) examples jsp jsp jsp servlets servlets servlets manager Requires Authentication (401) host-manager html manager deploy?path=foo

	findleaks html jmxproxy list reload?path= examples roles serverinfo sessions?path= examples <i>Successful (200)</i> docs RELEASE-NOTES.txt aio.html api index.html appdev build.xml.txt deployment.html index.html installation.html introduction.html processes.html sample sample.war source.html web.xml.txt apr.html architecture index.html overview.html requestProcess.html requestProcess requestProcess.pdf startup.html startup serverStartup.pdf serverStartup.txt balancer-howto.html building.html cgi-howto.html changelog.html class-loader-howto.html cluster-howto.html config ajp.html cluster-channel.html cluster-deployer.html colors ColorGameBean.html ColorGameBean.html clr.html clr.html colors.html colors.html colrs.jsp colrs.jsp colrs.jsp.html colrs.jsp.html dates date.html date.html date.jsp date.jsp date.jsp.html

	date.jsp.html

Tabela 86. Linux OS – Pronađeni servisi na IP adresi 172.23.202.232 (2011. godina)

SERVISI	SAMBA 172.23.202.232 tcp 139 Samba 3.5.8 172.23.202.232 tcp 445 Samba 3.5.8 CIFS Name Service 172.23.202.232 udp 137 FTP 172.23.202.232 tcp 21 vsFTPD 2.3.2 ftp.banner: 220 (vsFTPD 2.3.2) HTTP 172.23.202.232 tcp 80 Apache 2.2.17 http.banner: Apache/2.2.17 (Ubuntu) http.banner.server: Apache/2.2.17 (Ubuntu) 172.23.202.232 tcp 8080 5 Apache Tomcat Coyote: 1.1 http.banner: Apache-Coyote/1.1 IMAP 172.23.202.232 tcp 143 Dovecot imap.banner: * OK [CAPABILITY IMAP4rev1 LITERAL+SASL-IR LOGIN-REFERRALS ID ENABLE STARTTLS LOGINDISABLED] Dovecot ready. IMAPS³⁵²⁴ 172.23.202.232 tcp 993 Dovecot imap.banner: * OK [CAPABILITY IMAP4rev1 LITERAL+SASL-IR LOGIN-REFERRALS ID ENABLE AUTH=PLAIN] Dovecot ready. POP 172.23.202.232 tcp 110 0 Dovecot pop.banner: +OK Dovecot ready. POPS³⁵²⁵ 172.23.202.232 tcp 995 2 Dovecot pop.banner: +OK Dovecot ready. MySQL 172.23.202.232 tcp 3306 SSH 172.23.202.232 tcp 22 OpenSSH 5.8p1 ssh.banner: SSH-2.0-OpenSSH_5.8p1 ssh.protocol.version: 2.0
Spidered Web site	http://172.23.202.232:80 Common Default URLs: <i>Access Error (403)</i> cgi-bin <i>Successful (200)</i>

³⁵²⁴ Internet Message Access Protocol (IMAPS) preko TLS/SSL-a se koristi za pristupanje i obradu elektronske pošte (e-mail) korišćenjem dešifrovanih (TLS/SSL) konekcija. Kada se uspostavi TLS/SSL konekcija, koristi se standardni IMAP protokol. IMAP serveri mogu sadržavati nekoliko foldera, aka mailbox-ova, koji sadrže poruke (e-mails) za korisnike.

³⁵²⁵ Post Office Protocol (POP) omogućava radnim stanicama da dinamički iz mailbox servera uzvraćaju elektronsku poštu (e-mail). POPS dodaje SSLpodršku POP3.

	Icons Guessed URLs <i>Access Error (403)</i> cgi-bin ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-doc %3f.jsp .svn Entries ADw-script AD4-alert(42) ADwscript AD4- CVS Entries Root DEADJOE Trace.axd WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config <i>Redirect (301)</i> icons small <i>Successful (200)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-script+AD4-icons small index.html Linked URLs <i>Successful (200)</i> icons README README.html Small http://172.23.202.232:8080 Common Default URLs <i>Successful (200)</i> docs examples Guessed URLs <i>Error (400)</i> examples jsp cal cal1.jsp%00 cal1.jsp%5C checkbox checkresult.jsp%00 checkresult.jsp%5C

	colors colrs.jsp%00 colrs.jsp%5C dates date.jsp%00 date.jsp%5C error err.jsp%00 err.jsp%5C forward forward.jsp%00 forward.jsp%5C include include.jsp%00 include.jsp%5C jsp2 el basic-arithmetic.jsp%00 basic-arithmetic.jsp%5C basic-comparisons.jsp%00 basic-comparisons.jsp%5C functions.jsp%00 functions.jsp%5C implicit-objects.jsp%00 jspattribute jspattribute.jsp%00 jspattribute.jsp%5C shuffle.jsp%00 shuffle.jsp%5C misc config.jsp%00 config.jsp%5C dynamicattrs.jsp%00 dynamicattrs.jsp%5C simpletag book.jsp%00 book.jsp%5C hello.jsp%00 hello.jsp%5C repeat.jsp%00 repeat.jsp%5C foo.jsp%00 foo.jsp%5C tagfiles hello.jsp%00 hello.jsp%5C panel.jsp%00 panel.jsp%5C products.jsp%00 products.jsp%5C jsptoserv jsptoservlet.jsp%00 num numguess.jsp%00 numguess.jsp%5C plugin plugin.jsp%00 plugin.jsp%5C sessions carts.jsp%00 carts.jsp%5C snp snoop.jsp%00 snoop.jsp%5C

	tagplugin choose.jsp%00 choose.jsp%5C foreach.jsp%00 foreach.jsp%5C if.jsp%00 if.jsp%5C xml xml.jsp%00 xml.jsp%5C Error (500) examples jsp error errorpage.jsp Redirect (302) examples examples manager Requires Authentication (401) manager jmxproxy %3f.jsp .svn entries ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4- ADw-script AD4-alert(42) ADwscript AD4- CVS Entries Root DEADJOE WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config Successful (200) ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4- script+AD4- script+AD4- script+AD4- script+AD4- script+AD4- script+AD4- docs api appdev sample index.html architecture Linked URLs Error (500) examples jsp jsp2 el functions.jsp?foo=JSP+2.0 functions.jsp?foo=JSP+2.0 implicit-objects.jsp?foo=bar implicit-objects.jsp?foo=bar jspx

	textRotate.jspx textRotate.jspx?name=JSPX tagfiles products.jsp <i>Redirect (302)</i> examples jsp jsp jsp servlets servlets servlets manager <i>Requires Authentication (401)</i> host-manager html manager deploy?path= foo findleaks html jmxproxy list reload?path= examples roles serverinfo sessions?path= examples <i>Successful (200)</i> docs RELEASE-NOTES.txt aio.html api index.html appdev build.xml.txt deployment.html index.html installation.html introduction.html processes.html sample sample.war source.html web.xml.txt apr.html architecture index.html overview.html requestProcess.html requestProcess requestProcess.pdf startup.html startup serverStartup.pdf serverStartup.txt balancer-howto.html building.html cgi-howto.html changelog.html class-loader-howto.html cluster-howto.html

	config ajp.html cluster-channel.html cluster-deployer.html colors ColorGameBean.html ColorGameBean.html clr.html clr.html colors.html colors.html colrs.jsp colrs.jsp colrs.jsp.html colrs.jsp.html dates date.html date.html date.jsp date.jsp date.jsp.html date.jsp.html

Tabela 87. Linux OS – Pronađeni servisi na IP adresi 172.23.202.200 (2011. godina)

SERVISI	SAMBA 172.23.202.200 tcp 139 Samba 3.5.8 172.23.202.200 tcp 445 Samba 3.5.8 CIFS Name Service 172.23.202.200 udp 137 FTP 172.23.202.200 tcp 21 vsFTPD 2.3.2 ftp.banner: 220 (vsFTPD 2.3.2) HTTP 172.23.202.200 tcp 80 Apache 2.2.17 http.banner: Apache/2.2.17 (Ubuntu) http.banner.server: Apache/2.2.17 (Ubuntu) 172.23.202.200 tcp 8080 Apache Tomcat Coyote: 1.1 http.banner: Apache-Coyote/1.1 IMAP 172.23.202.200 tcp 143 Dovecot imap.banner: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE STARTTLS LOGINDISABLED] Dovecot ready. IMAPS³⁵²⁶ 172.23.202.200 tcp 993 Dovecot imap.banner: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE AUTH=PLAIN] Dovecot ready. POP 172.23.202.200 tcp 110 0 Dovecot pop.banner: +OK Dovecot ready.

³⁵²⁶ Internet Message Access Protocol (IMAPS) preko TLS/SSL-a se koristi za pristupanje i obradu elektronske pošte (e-mail) korišćenjem dešifrovanih (TLS/SSL) konekcija. Kada se uspostavi TLS/SSL konekcija, koristi se standardni IMAP protokol. IMAP serveri mogu sadržavati nekoliko foldera, aka mailbox-ova, koji sadrže poruke (e-mails) za korisnike.

	POPS³⁵²⁷ 172.23.202.200 tcp 995 2 Dovecot pop.banner: +OK Dovecot ready. MySQL 172.23.202.200 tcp 3306 SSH 172.23.202.200 tcp 22 OpenSSH 5.8p1 ssh.banner: SSH-2.0-OpenSSH_5.8p1 ssh.protocol.version: 2.0
Spidered Web site	http://172.23.202.200:80 Common Default URLs: <i>Access Error (403)</i> cgi-bin <i>Successful (200)</i> Icons Guessed URLs <i>Access Error (403)</i> cgi-bin ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-doc%3f.jsp .svn Entries ADw-script AD4-alert(42) ADwscript AD4-CVS Entries Root DEADJOE Trace.axd WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config <i>Redirect (301)</i> icons small <i>Successful (200)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-script+AD4-icons small index.html Linked URLs <i>Successful (200)</i> icons README

³⁵²⁷ Post Office Protocol (POP) omogućava radnim stanicama da dinamički iz mailbox servera uzvraćaju elektronsku poštu (e-mail). POPS dodaje SSLpodršku POP3.

	README.html Small http://172.23.202.200:8080 Common Default URLs <i>Successful (200)</i> docs examples Guessed URLs <i>Error (400)</i> examples jsp cal cal1.jsp%00 cal1.jsp%5C checkbox checkresult.jsp%00 checkresult.jsp%5C colors colrs.jsp%00 colrs.jsp%5C dates date.jsp%00 date.jsp%5C error err.jsp%00 err.jsp%5C forward forward.jsp%00 forward.jsp%5C include include.jsp%00 include.jsp%5C jsp2 el basic-arithmetic.jsp%00 basic-arithmetic.jsp%5C basic-comparisons.jsp%00 basic-comparisons.jsp%5C functions.jsp%00 functions.jsp%5C implicit-objects.jsp%00 jspattribute jspattribute.jsp%00 jspattribute.jsp%5C shuffle.jsp%00 shuffle.jsp%5C misc config.jsp%00 config.jsp%5C dynamicattrs.jsp%00 dynamicattrs.jsp%5C simpletag book.jsp%00 book.jsp%5C hello.jsp%00 hello.jsp%5C repeat.jsp%00 repeat.jsp%5C foo.jsp%00 foo.jsp%5C tagfiles hello.jsp%00

	hello.jsp%5C panel.jsp%00 panel.jsp%5C products.jsp%00 products.jsp%5C jsptoserv jsptoservlet.jsp%00 num numguess.jsp%00 numguess.jsp%5C plugin plugin.jsp%00 plugin.jsp%5C sessions carts.jsp%00 carts.jsp%5C snp snoop.jsp%00 snoop.jsp%5C tagplugin choose.jsp%00 choose.jsp%5C foreach.jsp%00 foreach.jsp%5C if.jsp%00 if.jsp%5C xml xml.jsp%00 xml.jsp%5C Error (500) examples jsp error errorpge.jsp Redirect (302) examples examples manager Requires Authentication (401) manager jmxproxy %3f.jsp .svn entries ?P=+ADw-script+AD4-alert(42)+ADwscript+ AD4- ADw-script AD4-alert(42) ADwscript AD4- CVS Entries Root DEADJOE WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config Successful (200) ?P=+ADw-script+AD4-alert(42)+Adw script+ AD4- script+AD4- script+AD4- script+AD4- script+AD4-

	script+AD4- script+AD4- docs api appdev sample index.html architecture Linked URLs <i>Error (500)</i> examples jsp jsp2 el functions.jsp?foo=JSP+2.0 functions.jsp?foo=JSP+2.0 implicit-objects.jsp?foo=bar implicit-objects.jsp?foo=bar jspx textRotate.jspx textRotate.jspx?name=JSPX tagfiles products.jsp <i>Redirect (302)</i> examples jsp jsp jsp servlets servlets servlets manager <i>Requires Authentication (401)</i> host-manager html manager deploy?path= foo findleaks html jmxproxy list reload?path= examples roles serverinfo sessions?path= examples <i>Successful (200)</i> docs RELEASE-NOTES.txt aio.html api index.html appdev build.xml.txt deployment.html index.html installation.html introduction.html processes.html sample

	sample.war source.html web.xml.txt apr.html architecture index.html overview.html requestProcess.html requestProcess requestProcess.pdf startup.html startup serverStartup.pdf serverStartup.txt balancer-howto.html building.html cgi-howto.html changelog.html class-loader-howto.html cluster-howto.html config ajp.html cluster-channel.html cluster-deployer.html colors ColorGameBean.html ColorGameBean.html clr.html clr.html colors.html colors.html colrs.jsp colrs.jsp colrs.jsp.html colrs.jsp.html dates date.html date.html date.jsp date.jsp date.jsp.html date.jsp.html

Tabela 88. Linux OS – Pronađeni servisi na IP adresi 172.23.202.230 (2011. godina)

SERVISI	SAMBA 172.23.202.230 tcp 139 Samba 3.5.8 172.23.202.230 tcp 445 Samba 3.5.8 CIFS Name Service 172.23.202.230 udp 137 FTP 172.23.202.230 tcp 21 vsFTPD 2.3.2 ftp.banner: 220 (vsFTPD 2.3.2) HTTP 172.23.202.230 tcp 80 Apache 2.2.17 http.banner: Apache/2.2.17 (Ubuntu) http.banner.server: Apache/2.2.17 (Ubuntu) 172.23.202.230 tcp 8080 5 Apache Tomcat

	Coyote: 1.1 http.banner: Apache-Coyote/1.1 IMAP 172.23.202.230 tcp 143 Dovecot imap.banner: * OK [CAPABILITY IMAP4rev1 LITERAL+SASL-IR LOGIN-REFERRALS ID ENABLE STARTTLS LOGINDISABLED] Dovecot ready. IMAPS³⁵²⁸ 172.23.202.230 tcp 993 Dovecot imap.banner: * OK [CAPABILITY IMAP4rev1 LITERAL+SASL-IR LOGIN-REFERRALS ID ENABLE AUTH=PLAIN] Dovecot ready. POP 172.23.202.230 tcp 110 0 Dovecot pop.banner: +OK Dovecot ready. POPS³⁵²⁹ 172.23.202.230 tcp 995 2 Dovecot pop.banner: +OK Dovecot ready. MySQL 172.23.202.230 tcp 3306 SSH 172.23.202.230 tcp 22 OpenSSH 5.8p1 ssh.banner: SSH-2.0-OpenSSH_5.8p1 ssh.protocol.version: 2.0
Spidered Web site	http://172.23.202.230:80 Common Default URLs: Access Error (403) cgi-bin Successful (200) Icons Guessed URLs Access Error (403) cgi-bin ?P=+ADw-script+AD4-alert(42)+Adw-script+AD4-script+AD4-doc%3f.jsp .svn Entries ADw-script AD4-alert(42) Adw-script AD4- CVS Entries Root DEADJOE Trace.axd WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config

³⁵²⁸ Internet Message Access Protocol (IMAPS) preko TLS/SSL-a se koristi za pristupanje i obradu elektronske pošte (e-mail) korišćenjem dešifrovanih (TLS/SSL) konekcija. Kada se uspostavi TLS/SSL konekcija, koristi se standardni IMAP protokol. IMAP serveri mogu sadržavati nekoliko foldera, aka mailbox-ova, koji sadrže poruke (e-mails) za korisnike.

³⁵²⁹ Post Office Protocol (POP) omogućava radnim stanicama da dinamički iz mailbox servera uzvraćaju elektronsku poštu (e-mail). POPS dodaje SSLpodršku POP3.

	<i>Redirect (301)</i> icons small <i>Successful (200)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-script+AD4-icons small index.html Linked URLs <i>Successful (200)</i> icons README README.html Small http://172.23.202.230:8080 Common Default URLs <i>Successful (200)</i> docs examples Guessed URLs <i>Error (400)</i> examples jsp cal cal1.jsp%00 cal1.jsp%5C checkbox checkresult.jsp%00 checkresult.jsp%5C colors colrs.jsp%00 colrs.jsp%5C dates date.jsp%00 date.jsp%5C error err.jsp%00 err.jsp%5C forward forward.jsp%00 forward.jsp%5C include include.jsp%00 include.jsp%5C jsp2 el basic-arithmetic.jsp%00 basic-arithmetic.jsp%5C basic-comparisons.jsp%00 basic-comparisons.jsp%5C functions.jsp%00 functions.jsp%5C implicit-objects.jsp%00 jspattribute jspattribute.jsp%00

	jspattribute.jsp%5C shuffle.jsp%00 shuffle.jsp%5C misc config.jsp%00 config.jsp%5C dynamicattrs.jsp%00 dynamicattrs.jsp%5C simpletag book.jsp%00 book.jsp%5C hello.jsp%00 hello.jsp%5C repeat.jsp%00 repeat.jsp%5C foo.jsp%00 foo.jsp%5C tagfiles hello.jsp%00 hello.jsp%5C panel.jsp%00 panel.jsp%5C products.jsp%00 products.jsp%5C jsptoserv jsptoservlet.jsp%00 num numguess.jsp%00 numguess.jsp%5C plugin plugin.jsp%00 plugin.jsp%5C sessions carts.jsp%00 carts.jsp%5C snp snoop.jsp%00 snoop.jsp%5C tagplugin choose.jsp%00 choose.jsp%5C foreach.jsp%00 foreach.jsp%5C if.jsp%00 if.jsp%5C xml xml.jsp%00 xml.jsp%5C Error (500) examples jsp error errorpage.jsp Redirect (302) examples examples manager Requires Authentication (401) manager jmxproxy %3f.jsp .svn entries ?P=+ADw-script+AD4-alert(42)+ADwscript+ AD4- ADw-script AD4-alert(42) ADwscript

	AD4- CVS Entries Root DEADJOE WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config <i>Successful (200)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+ AD4- script+AD4- script+AD4- script+AD4- script+AD4- script+AD4- docs api appdev sample index.html architecture Linked URLs <i>Error (500)</i> examples jsp jsp2 el functions.jsp?foo=JSP+2.0 functions.jsp?foo=JSP+2.0 implicit-objects.jsp?foo=bar implicit-objects.jsp?foo=bar jspx textRotate.aspx textRotate.aspx?name=JSPX tagfiles products.jsp <i>Redirect (302)</i> examples jsp jsp jsp servlets servlets servlets manager <i>Requires Authentication (401)</i> host-manager html manager deploy?path= foo findleaks html jmxproxy list reload?path= examples roles

	serverinfo sessions?path= examples ucessful (200) docs RELEASE-NOTES.txt aio.html api index.html appdev build.xml.txt deployment.html index.html installation.html introduction.html processes.html sample sample.war source.html web.xml.txt apr.html architecture index.html overview.html requestProcess.html requestProcess requestProcess.pdf startup.html startup serverStartup.pdf serverStartup.txt balancer-howto.html building.html cgi-howto.html changelog.html class-loader-howto.html cluster-howto.html config ajp.html cluster-channel.html cluster-deployer.html colors ColorGameBean.html ColorGameBean.html clr.html clr.html colors.html colors.html colrs.jsp colrs.jsp colrs.jsp.html colrs.jsp.html dates date.html date.html date.jsp date.jsp date.jsp.html date.jsp.html

Tabela 89. Linux OS – Pronađeni servisi na IP adresi 172.23.202.135 (2011. godina)

SERVISI	SAMBA 172.23.202.135 tcp 139 Samba 3.5.8 172.23.202.135 tcp 445 Samba 3.5.8

	CIFS Name Service 172.23.202.135 udp 137 FTP 172.23.202.135 tcp 21 vsFTPD 2.3.2 ftp.banner: 220 (vsFTPD 2.3.2) HTTP 172.23.202.135 tcp 80 Apache 2.2.17 http.banner: Apache/2.2.17 (Ubuntu) http.banner.server: Apache/2.2.17 (Ubuntu) 172.23.202.135 tcp 8080 5 Apache Tomcat Coyote: 1.1 http.banner: Apache-Coyote/1.1 IMAP 172.23.202.135 tcp 143 Dovecot imap.banner: * OK [CAPABILITY IMAP4rev1 LITERAL+SASL-IR LOGIN-REFERRALS ID ENABLE STARTTLS LOGINDISABLED] Dovecot ready. IMAPS³⁵³⁰ 172.23.202.135 tcp 993 Dovecot imap.banner: * OK [CAPABILITY IMAP4rev1 LITERAL+SASL-IR LOGIN-REFERRALS ID ENABLE AUTH=PLAIN] Dovecot ready. POP 172.23.202.135 tcp 110 0 Dovecot pop.banner: +OK Dovecot ready. POPS³⁵³¹ 172.23.202.135 tcp 995 2 Dovecot pop.banner: +OK Dovecot ready. MySQL 172.23.202.135 tcp 3306 SSH 172.23.202.135 tcp 22 OpenSSH 5.8p1 ssh.banner: SSH-2.0-OpenSSH_5.8p1 ssh.protocol.version: 2.0
Spidered Web site	http://172.23.202.135:80 Common Default URLs: <i>Access Error (403)</i> cgi-bin <i>Successful (200)</i> Icons Guessed URLs <i>Access Error (403)</i> cgi-bin ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-doc

³⁵³⁰ Internet Message Access Protocol (IMAPS) preko TLS/SSL-a se koristi za pristupanje i obradu elektronske pošte (e-mail) korišćenjem dešifrovanih (TLS/SSL) konekcija. Kada se uspostavi TLS/SSL konekcija, koristi se standardni IMAP protokol. IMAP serveri mogu sadržavati nekoliko foldera, aka mailbox-ova, koji sadrže poruke (e-mails) za korisnike.

³⁵³¹ Post Office Protocol (POP) omogućava radnim stanicama da dinamički iz mailbox servera uzvraćaju elektronsku poštu (e-mail). POPS dodaje SSLpodršku POP3.

	%3f.jsp .svn Entries ADw-script AD4-alert(42) ADwscript AD4- CVS Entries Root DEADJOE Trace.axd WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config <i>Redirect (301)</i> icons small <i>Successful (200)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+ AD4- script+AD4- script+AD4- icons small index.html Linked URLs <i>Successful (200)</i> icons README README.html Small http://172.23.202.135:8080 Common Default URLs <i>Successful (200)</i> docs examples Guessed URLs <i>Error (400)</i> examples jsp cal cal1.jsp%00 cal1.jsp%5C checkbox checkresult.jsp%00 checkresult.jsp%5C colors colrs.jsp%00 colrs.jsp%5C dates date.jsp%00 date.jsp%5C error err.jsp%00 err.jsp%5C

	forward forward.jsp%00 forward.jsp%5C include include.jsp%00 include.jsp%5C jsp2 el basic-arithmetic.jsp%00 basic-arithmetic.jsp%5C basic-comparisons.jsp%00 basic-comparisons.jsp%5C functions.jsp%00 functions.jsp%5C implicit-objects.jsp%00 jspattribute jspattribute.jsp%00 jspattribute.jsp%5C shuffle.jsp%00 shuffle.jsp%5C misc config.jsp%00 config.jsp%5C dynamicattrs.jsp%00 dynamicattrs.jsp%5C simpletag book.jsp%00 book.jsp%5C hello.jsp%00 hello.jsp%5C repeat.jsp%00 repeat.jsp%5C foo.jsp%00 foo.jsp%5C tagfiles hello.jsp%00 hello.jsp%5C panel.jsp%00 panel.jsp%5C products.jsp%00 products.jsp%5C jsptoserv jsptoservlet.jsp%00 num numguess.jsp%00 numguess.jsp%5C plugin plugin.jsp%00 plugin.jsp%5C sessions carts.jsp%00 carts.jsp%5C snp snoop.jsp%00 snoop.jsp%5C tagplugin choose.jsp%00 choose.jsp%5C foreach.jsp%00 foreach.jsp%5C if.jsp%00 if.jsp%5C xml xml.jsp%00 xml.jsp%5C Error (500) examples

	jsp error errorpage.jsp Redirect (302) examples examples manager Requires Authentication (401) manager jmxproxy %3f.jsp .svn entries ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4- ADw-script AD4-alert(42) ADwscript AD4- CVS Entries Root DEADJOE WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config Successful (200) ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4- script+AD4- script+AD4- script+AD4- script+AD4- script+AD4- script+AD4- docs api appdev sample index.html architecture Linked URLs Error (500) examples jsp jsp2 el functions.jsp?foo=JSP+2.0 functions.jsp?foo=JSP+2.0 implicit-objects.jsp?foo=bar implicit-objects.jsp?foo=bar jspx textRotate.jspx textRotate.jspx?name=JSPX tagfiles products.jsp Redirect (302) examples jsp jsp jsp servlets servlets

	servlets manager <i>Requires Authentication (401)</i> host-manager html manager deploy?path= foo findleaks html jmxproxy list reload?path= examples roles serverinfo sessions?path= examples <i>Successful (200)</i> docs RELEASE-NOTES.txt aio.html api index.html appdev build.xml.txt deployment.html index.html installation.html introduction.html processes.html sample sample.war source.html web.xml.txt apr.html architecture index.html overview.html requestProcess.html requestProcess requestProcess.pdf startup.html startup serverStartup.pdf serverStartup.txt balancer-howto.html building.html cgi-howto.html changelog.html class-loader-howto.html cluster-howto.html config ajp.html cluster-channel.html cluster-deployer.html colors ColorGameBean.html ColorGameBean.html clr.html clr.html colors.html colors.html colrs.jsp

	colrs.jsp colrs.jsp.html colrs.jsp.html dates date.html date.html date.jsp date.jsp date.jsp.html date.jsp.html

Tabela 90. Linux OS – Pronađeni servisi na IP adresi 172.23.202.231 (2011. godina)

SERVISI	SAMBA 172.23.202.231 tcp 139 Samba 3.5.8 172.23.202.231 tcp 445 Samba 3.5.8 CIFS Name Service 172.23.202.231 udp 137 FTP 172.23.202.231 tcp 21 vsFTPD 2.3.2 ftp.banner: 220 (vsFTPD 2.3.2) HTTP 172.23.202.231 tcp 80 Apache 2.2.17 http.banner: Apache/2.2.17 (Ubuntu) http.banner.server: Apache/2.2.17 (Ubuntu) 172.23.202.231 tcp 8080 5 Apache Tomcat Coyote: 1.1 http.banner: Apache-Coyote/1.1 IMAP 172.23.202.231 tcp 143 Dovecot imap.banner: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE STARTTLS LOGINDISABLED] Dovecot ready. IMAPS³⁵³² 172.23.202.231 tcp 993 Dovecot imap.banner: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE AUTH=PLAIN] Dovecot ready. POP 172.23.202.231 tcp 110 0 Dovecot pop.banner: +OK Dovecot ready. POPS³⁵³³ 172.23.202.231 tcp 995 2 Dovecot pop.banner: +OK Dovecot ready. MySQL 172.23.202.231 tcp 3306 SSH 172.23.202.231 tcp 22 OpenSSH 5.8p1 ssh.banner: SSH-2.0-OpenSSH_5.8p1

³⁵³² Internet Message Access Protocol (IMAPS) preko TLS/SSL-a se koristi za pristupanje i obradu elektronske pošte (e-mail) korišćenjem dešifrovanih (TLS/SSL) konekcija. Kada se uspostavi TLS/SSL konekcija, koristi se standardni IMAP protokol. IMAP serveri mogu sadržavati nekoliko foldera, aka mailbox-ova, koji sadrže poruke (e-mails) za korisnike.

³⁵³³ Post Office Protocol (POP) omogućava radnim stanicama da dinamički iz mailbox servera uzvraćaju elektronsku poštu (e-mail). POPS dodaje SSLpodršku POP3.

Spidered Web site	ssh.protocol.version: 2.0 http://172.23.202.231:80 Common Default URLs: <i>Access Error (403)</i> cgi-bin <i>Successful (200)</i> Icons Guessed URLs <i>Access Error (403)</i> cgi-bin ?P=+ADw-script+AD4-alert(42)+Adwscript+AD4- doc %3f.jsp .svn Entries ADw-script AD4-alert(42) ADwscript AD4- CVS Entries Root DEADJOE Trace.axd WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config <i>Redirect (301)</i> icons small <i>Successful (200)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4- script+AD4- script+AD4- script+AD4- icons small index.html Linked URLs <i>Successful (200)</i> icons README README.html Small http://172.23.202.231:8080 Common Default URLs <i>Successful (200)</i> docs examples Guessed URLs <i>Error (400)</i> examples

	jsp cal cal1.jsp%00 cal1.jsp%5C checkbox checkresult.jsp%00 checkresult.jsp%5C colors colrs.jsp%00 colrs.jsp%5C dates date.jsp%00 date.jsp%5C error err.jsp%00 err.jsp%5C forward forward.jsp%00 forward.jsp%5C include include.jsp%00 include.jsp%5C jsp2 el basic-arithmetic.jsp%00 basic-arithmetic.jsp%5C basic-comparisons.jsp%00 basic-comparisons.jsp%5C functions.jsp%00 functions.jsp%5C implicit-objects.jsp%00 jspattribute jspattribute.jsp%00 jspattribute.jsp%5C shuffle.jsp%00 shuffle.jsp%5C misc config.jsp%00 config.jsp%5C dynamicattrs.jsp%00 dynamicattrs.jsp%5C simpletag book.jsp%00 book.jsp%5C hello.jsp%00 hello.jsp%5C repeat.jsp%00 repeat.jsp%5C foo.jsp%00 foo.jsp%5C tagfiles hello.jsp%00 hello.jsp%5C panel.jsp%00 panel.jsp%5C products.jsp%00 products.jsp%5C jsptoserv jsptoservlet.jsp%00 num numguess.jsp%00 numguess.jsp%5C plugin plugin.jsp%00 plugin.jsp%5C sessions carts.jsp%00

	carts.jsp%5C snp snoop.jsp%00 snoop.jsp%5C tagplugin choose.jsp%00 choose.jsp%5C foreach.jsp%00 foreach.jsp%5C if.jsp%00 if.jsp%5C xml xml.jsp%00 xml.jsp%5C Error (500) examples jsp error errorpge.jsp Redirect (302) examples examples manager Requires Authentication (401) manager jmxproxy %3f.jsp .svn entries ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4- ADw-script AD4-alert(42) ADwscript AD4- CVS Entries Root DEADJOE WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config Successful (200) ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4- script+AD4- script+AD4- script+AD4- script+AD4- script+AD4- script+AD4- docs api appdev sample index.html architecture Linked URLs Error (500) examples jsp jsp2 el functions.jsp?foo=JSP+2.0

	functions.jsp?foo=JSP+2.0 implicit-objects.jsp?foo=bar implicit-objects.jsp?foo=bar jspx textRotate.jspx textRotate.jspx?name=JSPX tagfiles products.jsp <i>Redirect (302)</i> examples jsp jsp jsp servlets servlets servlets manager <i>Requires Authentication (401)</i> host-manager html manager deploy?path= foo findleaks html jmxproxy list reload?path= examples roles serverinfo sessions?path= examples <i>Successful (200)</i> docs RELEASE-NOTES.txt aio.html api index.html appdev build.xml.txt deployment.html index.html installation.html introduction.html processes.html sample sample.war source.html web.xml.txt apr.html architecture index.html overview.html requestProcess.html requestProcess requestProcess.pdf startup.html startup serverStartup.pdf serverStartup.txt balancer-howto.html building.html

	cgi-howto.html changelog.html class-loader-howto.html cluster-howto.html config ajp.html cluster-channel.html cluster-deployer.html colors ColorGameBean.html ColorGameBean.html clr.html clr.html colors.html colors.html colrs.jsp colrs.jsp colrs.jsp.html colrs.jsp.html dates date.html date.html date.jsp date.jsp date.jsp.html date.jsp.html

Tabela 91. Linux OS sa IP adresama 172.23.202.133, 172.23.202.132, 172.23.202.123, 172.23.202.229 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.133		OS: Ubuntu 10.04.2 lts x64 server, ubuntu1004srvx64			30
IP adresa: 172.23.202.132		OS: Ubuntu 10.04.2 lts x86 server, ubuntu1004srvx86			30
IP adresa: 172.23.202.123		OS: Kubuntu 10.04.2 desktop x86, kubuntu1004dskx86			30
IP adresa: 172.23.202.229		OS: Kubuntu 10.04.2 desktop x64, kubuntu1004dskx64			30
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Apache httpd mod_isapi module unload flaw (CVE-2010-0425) (apache-httpd-2_2_x-mod_isapi-moduleunload-flaw-cve-2010-0425)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 U modulu mod_isapi je pronađen propust, koji će pokušati da ukloni ISAPI dll kada naide na greške. To može ostaviti povratne pozive u nedefinisanoj stanju i kao posledica može da se javi segmentation fault. Na Windows platformama koje	BID 38494 ³⁵³⁴ CERT-VN 280613 ³⁵³⁵ CVE CVE-2010-0425 ³⁵³⁶ OVAL OVAL8439 ³⁵³⁷ SECUNIA 38978 ³⁵³⁸ SECUNIA 39628 ³⁵³⁹ URL1 3540 XF apache-http-modisapi-ocp-unspeccified(56624) ³⁵⁴¹	Kritičan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz

³⁵³⁴ <http://www.securityfocus.com/bid/38494>

³⁵³⁵ <http://www.kb.cert.org/vuls/id/280613>

³⁵³⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0425>

³⁵³⁷ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval:def:8439>

³⁵³⁸ <http://secunia.com/advisories/38978/>

³⁵³⁹ <http://secunia.com/advisories/39628/>

³⁵⁴⁰ http://httpd.apache.org/security/vulnerabilities_22.html

³⁵⁴¹ <http://xforce.iss.net/xforce/xfdb/56624>

		koriste mod_isapi, udaljeni napadač bi mogao da pošalje zlonameran zahtev da pokrene ovaj problem, a kako win32 MPM pokreće samo jedan proces, to bi kao ishod imalo odbijanje servisa i potencijalno dozvolilo da se pokrene proizvoljan kôd. Napomena: Zahvaljujući Brett Gervasoni-ju iz "Sense of Security" ovaj problem je prijavljen i za njega je predložena zakrpa.			
2.	Anonymous users can obtain the Windows password policy (cifs-nt-0002)	Korišćenjem CIFS NULL sesije, anonimni korisnik može da dobije uvid u polisu šifri. Polisa šifri sadrži osetljive informacije o najmanjoj mogućoj dužini lozinke, zaključavanje šifre, vremensko trajanje zaključanosti šifre itd.	SANS-01 W5 ³⁵⁴² CVE CVE-2000-1200 ³⁵⁴³ XF nt-lsa-domain-sid(4015) ³⁵⁴⁴ SANS-02 W5 ³⁵⁴⁵ BID 959 ³⁵⁴⁶ SANS-04 W3 ³⁵⁴⁷ SANS-03 W5 ³⁵⁴⁸ BID 87 ³⁵⁴⁹	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost
3.	HTTP Basic Authentication Enabled (http-basic-auth-cleartext)	172.23.202.133:8080 172.23.202.132:8080 172.23.202.123:8080 172.23.202.229:8080 HTTP Basic Authentication šema se ne smatra sigurnom metodom autentifikacije korisnika (ukoliko se ne koristi u kombinaciji sa nekim spoljnim sigurnosnim sistemom, kao TLS/SSL), s obzirom da se korisničko ime i lozinka preko mreže prenose kao običan tekst. Primer: Pokretanje ranjivog HTTP servisa. http://172.23.202.133:8080/manager/html 1: Basic realm="Tomcat Manager Application"	URL1 ³⁵⁵⁰	Kritičan	Koristiti Osnovnu Autentifikaciju preko TLS/SSL (HTTPS). Omogućiti HTTPS na Web serveru. TLS/SSL protokol će zaštititi akreditive osnovne autentifikacije u običnom tekstu. Koristiti Digest Authentication Replace Basic Authentication sa alternativnom Digest Authentication shemom. Po savremenim kriptografskim standardima, Digest Authentication je slaba. Ali za širok spektar namena, ona je korisna zamena za Basic Authentication (osnovnu autentifikaciju). Ona ispravlja neke, ali ne sve, slabosti Basic Authentication (osnovne autentifikacije). Videti RFC 2617 ³⁵⁵¹ (odjeljak 4 Security Considerations) za više informacija.
4.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.133:139 172.23.202.133:445 172.23.202.132:139 172.23.202.132:445 172.23.202.123:139 172.23.202.123:445 172.23.202.229:139 172.23.202.229:445	MSKB 887429 URL1 ³⁵⁵²	Ozbiljan	Metoda za konfigurisanje SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429 ³⁵⁵³ . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru.

³⁵⁴² <http://www.sans.org/critical-security-controls/#w5>³⁵⁴³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2000-1200>³⁵⁴⁴ <http://xforce.iss.net/xforce/xfdb/4015>³⁵⁴⁵ <http://www.sans.org/critical-security-controls/#w5>³⁵⁴⁶ <http://www.securityfocus.com/bid/959>³⁵⁴⁷ <http://www.sans.org/critical-security-controls/#w3>³⁵⁴⁸ <http://www.sans.org/critical-security-controls/#w5>³⁵⁴⁹ <http://www.securityfocus.com/bid/87>³⁵⁵⁰ <http://tools.ietf.org/html/rfc2617>³⁵⁵¹ <http://tools.ietf.org/html/rfc2617#section-4>³⁵⁵² <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>³⁵⁵³ <http://support.microsoft.com/kb/887429>

		Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).			Na Samba serveru (na konfiguracionom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing = auto</i> ili da se zahteva SMB potpisivanje: <i>server signing = mandatory</i>
5.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.133:139 172.23.202.133:445 172.23.202.132:139 172.23.202.132:445 172.23.202.123:139 172.23.202.123:445 172.23.202.229:139 172.23.202.229:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled“)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled“)“ ranjivosti.
6.	Apache httpd expat DoS (CVE-2009-3560) (apache-httpd-2_2_x-cve-2009-3560)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepoverljivi XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	BID 37203 ³⁵⁵⁴ CVE CVE-2009-3560 ³⁵⁵⁵ DEBIAN DSA-1953 ³⁵⁵⁶ OVAL OVAL10613 ³⁵⁵⁷ OVAL OVAL6883 ³⁵⁵⁸ SECUNIA 37537 ³⁵⁵⁹ SECUNIA 38231 ³⁵⁶⁰ SECUNIA 38794 ³⁵⁶¹ SECUNIA 38832 ³⁵⁶² SECUNIA 38834 ³⁵⁶³ SECUNIA 39478 ³⁵⁶⁴ SECUNIA 41701 ³⁵⁶⁵ SECUNIA 43300 ³⁵⁶⁶ URL1 ³⁵⁶⁷	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
7.	Apache httpd expat DoS (CVE-2009-3720) (apache-httpd-2_2_x-cve-2009-3720)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u	CVE CVE-2009-3720 ³⁵⁶⁸ OVAL OVAL11019 ³⁵⁶⁹ OVAL OVAL7112 ³⁵⁷⁰ REDHAT RHSA-2010:0002 ³⁵⁷¹ SECUNIA 37324 ³⁵⁷²	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz

³⁵⁵⁴ <http://www.securityfocus.com/bid/37203>³⁵⁵⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3560>³⁵⁵⁶ <http://www.debian.org/security/2009/dsa-1953>³⁵⁵⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10613>³⁵⁵⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6883>³⁵⁵⁹ <http://secunia.com/advisories/37537/>³⁵⁶⁰ <http://secunia.com/advisories/38231/>³⁵⁶¹ <http://secunia.com/advisories/38794/>³⁵⁶² <http://secunia.com/advisories/38832/>³⁵⁶³ <http://secunia.com/advisories/38834/>³⁵⁶⁴ <http://secunia.com/advisories/39478/>³⁵⁶⁵ <http://secunia.com/advisories/41701/>³⁵⁶⁶ <http://secunia.com/advisories/43300/>³⁵⁶⁷ http://httpd.apache.org/security/vulnerabilities_22.html³⁵⁶⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3720>³⁵⁶⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11019>³⁵⁷⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7112>³⁵⁷¹ <http://rhn.redhat.com/errata/RHSA-2010-0002.html>³⁵⁷² <http://secunia.com/advisories/37324/>

		mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepoverljivi XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	SECUNIA 37537³⁵⁷³ SECUNIA 37925³⁵⁷⁴ SECUNIA 38050³⁵⁷⁵ SECUNIA 38231³⁵⁷⁶ SECUNIA 38794³⁵⁷⁷ SECUNIA 38832³⁵⁷⁸ SECUNIA 38834³⁵⁷⁹ SECUNIA 39478³⁵⁸⁰ SECUNIA 41701³⁵⁸¹ SECUNIA 43300³⁵⁸² URL1³⁵⁸³		
8.	Apache httpd apr_bridage_split_line DoS (CVE-2010-1623) (apache-httpd-2_2_x-cve-2010-1623)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako Apache procesira ne-SSL zahteve. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_brigade_split_line() u sklopu APR-util library, koji se koristi za procesiranje ne-SSL zahteva. Zlonamerni napadač bi mogao da šalje zahteve, pažljivo izrađujući tajming za pojedinačne bajtove, što bi polako zauzimalo memoriju i potencijalno dovelo do odbijanja servisa.	BID 43673³⁵⁸⁴ CVE CVE-2010-1623³⁵⁸⁵ REDHAT RHSA-2010:0950³⁵⁸⁶ SECUNIA 41701³⁵⁸⁷ SECUNIA 42015³⁵⁸⁸ SECUNIA 42361³⁵⁸⁹ SECUNIA 42367³⁵⁹⁰ SECUNIA 42403³⁵⁹¹ SECUNIA 42537³⁵⁹² SECUNIA 43211³⁵⁹³ SECUNIA 43285³⁵⁹⁴ URL1³⁵⁹⁵	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
9.	Apache httpd mod_cache and mod_dav DoS (CVE-2010-1452) (apache-httpd-2_2_x-mod_cache-andmod_	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako web server izvršava jedan od sledećih modula:	APPLE APPLE-SA-2011-03-21³⁵⁹⁶ CVE CVE-2010-1452³⁵⁹⁷ OVAL OVAL11683³⁵⁹⁸ REDHAT RHSA-2010:0659³⁵⁹⁹ SECUNIA 42367³⁶⁰⁰	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.16.tar.gz

³⁵⁷³ <http://secunia.com/advisories/37537/>³⁵⁷⁴ <http://secunia.com/advisories/37925/>³⁵⁷⁵ <http://secunia.com/advisories/38050/>³⁵⁷⁶ <http://secunia.com/advisories/38231/>³⁵⁷⁷ <http://secunia.com/advisories/38794/>³⁵⁷⁸ <http://secunia.com/advisories/38832/>³⁵⁷⁹ <http://secunia.com/advisories/38834/>³⁵⁸⁰ <http://secunia.com/advisories/39478/>³⁵⁸¹ <http://secunia.com/advisories/41701/>³⁵⁸² <http://secunia.com/advisories/43300/>³⁵⁸³ http://httpd.apache.org/security/vulnerabilities_22.html³⁵⁸⁴ <http://www.securityfocus.com/bid/43673>³⁵⁸⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1623>³⁵⁸⁶ <http://rhn.redhat.com/errata/RHSA-2010-0950.html>³⁵⁸⁷ <http://secunia.com/advisories/41701/>³⁵⁸⁸ <http://secunia.com/advisories/42015/>³⁵⁸⁹ <http://secunia.com/advisories/42361/>³⁵⁹⁰ <http://secunia.com/advisories/42367/>³⁵⁹¹ <http://secunia.com/advisories/42403/>³⁵⁹² <http://secunia.com/advisories/42537/>³⁵⁹³ <http://secunia.com/advisories/43211/>³⁵⁹⁴ <http://secunia.com/advisories/43285/>³⁵⁹⁵ http://httpd.apache.org/security/vulnerabilities_22.html³⁵⁹⁶ <http://lists.apple.com/archives/security-announce/2011/Mar/msg00006.html>³⁵⁹⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1452>³⁵⁹⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11683>³⁵⁹⁹ <http://rhn.redhat.com/errata/RHSA-2010-0659.html>³⁶⁰⁰ <http://secunia.com/advisories/42367/>

	dav-dos-cve-2010-1452)	mod_cache, mod_dav. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u obradi zahteva od strane mod_cache i mod_dav. Zlonameran napadač bi mogao da pošalje pažljivo izrađen zahtev i prouzrokuje da httpd child proces krahira. Ovakvo krahiranje bi se manifestovalo samo kao odbijanje servisa ako se koristi Worker MPM. Ovaj problem se dalje može ublažiti ako na mod_dav samo utiču zahtevi za koje postoji mogućnost autentifikovanja, a mod_cache je pod uticajem samo ako se koristi neuobičajena „CacheIgnoreURLSessionIdentifiers“ direktiva, uvedena u verziji 2.2.14. Ovaj problem je prijavio Mark Drayton.	URL1 ³⁶⁰¹		
10.	Apache httpd Timeout detection flaw (mod_proxy_http) (CVE-2010-2068) (apache-httpd-2.2.x-timeoutdetection-flaw-mod_proxy_http-cve-2010-2068)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Propust sa kojim je omogućeno otkrivanje informacija je otkriven u modulu mod_proxy_http na verzijama 2.2.9 do 2.2.15, 2.3.4-alpha i 2.3.5-alpha. Pod određenim tajmout uslovima, server bi mogao da uzvрати odgovorom koji je namenjen drugom korisniku. Ugrožene su one konfiguracije koje pokreću korišćenje proxy worker pool-ova. Na ranijim verzijama nije bilo ranjivosti, jer proxy pool-ovi još nisu bili uvedeni. Zahvaljujući Loren Anderson-u ovaj problem je prijavljen, a najjednostavniji način njegovog izbegavanja jeste opšte konfigurisanje.	APPLE APPLE-SA-2011-03-21 ³⁶⁰² BID 40827 ³⁶⁰³ CVE CVE-2010-2068 ³⁶⁰⁴ OVAL OVAL11491 ³⁶⁰⁵ OVAL OVAL6931 ³⁶⁰⁶ SECUNIA 40206 ³⁶⁰⁷ SECUNIA 41480 ³⁶⁰⁸ SECUNIA 41490 ³⁶⁰⁹ SECUNIA 41722 ³⁶¹⁰ XF apache-modproxyhttp-timeout-info-disc(59413) ³⁶¹¹ URL1 ³⁶¹²	Ozbiljan	Mnoge platforme i mnogi distributeri daju unapred formirane binarne pakete za Apache. Ovi unapred formirani paketi su najčešće standardizovani i optimizirani za određenu distribuciju, pa se zato savetuje korišćenje paketa predefinisanih za određeni OS, ukoliko su dostupni. Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.16.tar.gz
11.	X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch)	172.23.202.133:993 172.23.202.133:995 172.23.202.132:993 172.23.202.132:995 172.23.202.123:993 172.23.202.123:995 172.23.202.229:993 172.23.202.229:995 Rubrika u sertifikatu X.509 sa uobičajenim nazivom subjekta (CN) ne poklapa se sa imenom pojedinca koje je navedeno u sertifikatu.		Ozbiljan	Rubrika sa uobičajenim nazivom subjekta (CN) u sertifikatu X.509 treba da bude podešena da sadrži ime pojedinca koji prikazuje sertifikat (npr. ime hosta). To se postiže izradom novog sertifikata, koji najčešće potpisuje Certification Authority (CA), koji je od poverenja kako za klijenta, tako i za server.

³⁶⁰¹ http://httpd.apache.org/security/vulnerabilities_22.html³⁶⁰² <http://lists.apple.com/archives/security-announce/2011/Mar/msg00006.html>³⁶⁰³ <http://www.securityfocus.com/bid/40827>³⁶⁰⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2068>³⁶⁰⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11491>³⁶⁰⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6931>³⁶⁰⁷ <http://secunia.com/advisories/40206/>³⁶⁰⁸ <http://secunia.com/advisories/41480/>³⁶⁰⁹ <http://secunia.com/advisories/41490/>³⁶¹⁰ <http://secunia.com/advisories/41722/>³⁶¹¹ <http://xforce.iss.net/xforce/xfdb/59413>³⁶¹² http://httpd.apache.org/security/vulnerabilities_22.html

		Pre izdavanja sertifikata, Certification Authority (CA) mora da proveriti identitet pojedinca koji potražuje sertifikat, kako je navedeno u CA-ovom Certification Practice Statement (CPS). Zbog toga, uobičajene procedure validacije sertifikata zahtevaju da rubrika sertifikata sa CN subjektom odgovara pravom imenu pojedinca koji prikazuje sertifikat. Na primer, u sertifikatu prikazanom na „https://www.example.com“, naziv subjekta (CN) treba da bude „www.example.com“. U cilju otkrivanja i sprečavanja napada prisluškivanja, validnost sertifikata mora da bude overena, jer bi u suprotnom napadač mogao da otpočne napad preko posrednika i da stekne potpunu kontrolu nad protokom podataka. Od posebne važnosti je validnost naziva subjekta (CN), koji treba da se poklapa sa imenom pojedinca (imenom host-a). Neodgovarajući CN se najčešće javlja usled greške u konfiguraciji, iako on takođe može da ukazuje na to da se sprovodi napad preko posrednika.			
12.	FTP server does not support AUTH command (ftp-generic-0007)	172.23.202.133:21 172.23.202.132:21 172.23.202.123:21 172.23.202.229:21 FTP klijenti po defaultu šalju FTP server-u poverljive podatke (korisnički ID i šifra) u vidu čitkog teksta. Ova okolnost dozvoljava zlonamernim korisnicima da presreću poverljive podatke ukoliko prisluškuju vezu. Noviji FTP serveri podržavaju AUTH komandu, koja omogućava dodatne opcije autentifikacije, kao što su TLS, Kerberos, GSSAPI itd. Ona se može koristiti za sprečavanje prisluškivanja na FTP vezama.		Ozbiljan	Ažurirati/preći na FTP server koji podržava AUTH komandu.
13.	Apache httpd mod_proxy_ajp DoS (CVE-2010-0408) (http-apache-mod_proxy_ajp-dos)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ajp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Mod_proxy_ajp će vratiti pogrešan kôd statusa ako naiđe na grešku,	BID 38491³⁶¹³ CVE CVE-2010-0408³⁶¹⁴ DEBIAN DSA-2035³⁶¹⁵ OVAL OVAL8619³⁶¹⁶ OVAL OVAL9935³⁶¹⁷ REDHAT RHSA-2010:0168³⁶¹⁸ SECUNIA 39100³⁶¹⁹ SECUNIA 39501³⁶²⁰ SECUNIA 39628³⁶²¹ SECUNIA 39632³⁶²² SECUNIA 39656³⁶²³	Ozbiljan	Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz

³⁶¹³ <http://www.securityfocus.com/bid/38491>³⁶¹⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0408>³⁶¹⁵ <http://www.debian.org/security/2010/dsa-2035>³⁶¹⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8619>³⁶¹⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9935>³⁶¹⁸ <http://rhn.redhat.com/errata/RHSA-2010-0168.html>³⁶¹⁹ <http://secunia.com/advisories/39100/>³⁶²⁰ <http://secunia.com/advisories/39501/>³⁶²¹ <http://secunia.com/advisories/39628/>³⁶²² <http://secunia.com/advisories/39632/>

		prouzrokujući da backend server bude stavljen u status greške dok ne istekne vreme za ponovni pokušaj. Udaljeni napadač bi mogao da pošalje zlonameran zahtev da bi pokrenuo ovaj problem, što bi dovelo do odbijanja servisa. Zahvaljujući Niku Toivola iz Sulake Corporation ovaj problem je prijavljen uz predloženu adekvatnu meru zaštite u vidu zakrpe.	SECUNIA 40096 ³⁶²⁴ URL1 ³⁶²⁵		
14.	Browsable web directory (http-generic-browsable-dir)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Otkriven je direktorijum na web serveru koji može biti pretraživan, što znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice - spajdering (prateći hiperlinkove), ili -kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute force napadom na liste uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skrivena“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice.		Ozbiljan	Za Apache: onemogućiti brauzovanje direktorijuma mreže za sve direktorijume i poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim ako postoji potreba da ovi fajlovi budu dostupni preko web-a. Povremeno proći kroz web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastsareo, kao i nepoznate fajlove i direktorijume. Za Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote: Onemogućiti brauzovanje direktorijuma mreže za sve direktorijume i poddirektorijume. Uključiti Tomcat-ov web.xml file. U odeljku „default“, promeniti parametar „listings“ iz „true“ u „false“. Restartovati server. Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim ako ne postoji potreba da ovi fajlovi budu dostupni preko web-a. Povremeno proći kroz web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastsareo, kao i nepoznate fajlove i

³⁶²³ <http://secunia.com/advisories/39656/>³⁶²⁴ <http://secunia.com/advisories/40096/>³⁶²⁵ http://httpd.apache.org/security/vulnerabilities_22.html

					direktorijume.
15.	Form action submits sensitive data in the clear (http-generic-sensitive-form-data-unencrypted)	172.23.202.133:8080 172.23.202.132:8080 172.23.202.123:8080 172.23.202.229:8080 Web forma sadrži rubrike sa podacima koji su možda po prirodi osetljivi. Ovakvi podaci se prenose preko nezaštićene veze, koja bi mogla da omogući zlonamernim napadačima da prisluškujući mrežu pregledaju podatke u vidu običnog teksta. Formatiranje preko http://localhost:8080/examples/jsp/security/protected/vti_shm/j_security_check prosleđuje sledeće nezaštićene osetljive rubrike: j_password		Ozbiljan	Isključiti HTTPS protokol na serveru. Promeniti „action“ URL na oznaci rubrike da koristi HTTPS protokol („https://...“) umesto samo HTTP protokol („http://...“). Sve osetljive podatke treba slati preko HTTPS umesto preko HTTP.
16.	TLS/SSL Server Supports Weak Cipher Algorithms (ssl-weak-ciphers)	172.23.202.133:993 172.23.202.132:993 172.23.202.123:993 172.23.202.229:993 negotiated the SSL_DHE_RSA_WITH_DES_CBC_SHA cipher suite TLS/SSL server podržava šifre koje se zasnivaju na slabim algoritmima. To napadaču može omogućiti da pokrene napade preko posrednika i da pregleda ili čačka osetljive podatke. Uopšteno, sledeće šifre se smatraju slabim: Tzv. „null“ (nula) šifre, jer ne šifruju podatke. Eksportne šifre koje koriste dužine tajnih ključeva ograničene na 40 bitova. Na to najčešće ukazuje reč EXP/EXPORT u nazivu šifre. Zastareli algoritmi za šifrovanje čije se dužine tajnih ključeva po današnjim standardima smatraju kratkim, npr. DES ili RC4 sa 56-bitnim ključevima.		Ozbiljan	Konfigurisati server tako da onemogući podršku za slabe šifre. Za Apache web servere sa mod_ssl, uključiti fajl Apache konfiguracije i izmeniti liniju SSLCipherSuite tako da u njoj piše: SSLCipherSuite ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
17.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	TCP reset with incorrect sequence number triggered this fault on 172.23.202.133:22 172.23.202.132:22 172.23.202.123:143 172.23.202.229:143 Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hедера i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP	BID: 10183 ³⁶²⁶ CERT-VN: 415294 ³⁶²⁷ CVE CVE-2004-0230 ³⁶²⁸ MS: MS05-019 ³⁶²⁹ MS: MS06-064 ³⁶³⁰ NETBSD: NetBSD-SA2004-006 ³⁶³¹ OVAL: OVAL2689 ³⁶³² OVAL: OVAL270 ³⁶³³ OVAL OVAL3508 ³⁶³⁴ OVAL OVAL4791 ³⁶³⁵ OVAL OVAL5711 ³⁶³⁶	Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC 2385. ³⁶⁴⁴ Ono je napravljeno da smanji opasnost od određenih napada na BGP, kao što su TCP reseti.

³⁶²⁶ <http://www.securityfocus.com/bid/10183>³⁶²⁷ <http://www.kb.cert.org/vuls/id/415294>³⁶²⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>³⁶²⁹ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>³⁶³⁰ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>³⁶³¹ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>³⁶³² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>³⁶³³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>³⁶³⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>³⁶³⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>

		RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	SECUNIA: 11440 ³⁶³⁷ SECUNIA 11458 ³⁶³⁸ SECUNIA: 22341 ³⁶³⁹ SGI 20040403-01-A ³⁶⁴⁰ XF tcp-rst-dos(15886) ³⁶⁴¹ URL1 ³⁶⁴² URL2 ³⁶⁴³		
18.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podesi na jedinstvenu vrednost i da se koristi u rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da fingerprint-uje operativni sistem.	BID 4314 ³⁶⁴⁵ CVE CVE-2002-0510 ³⁶⁴⁶ XF linux-udp-fingerprint(8588) ³⁶⁴⁷	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili pak ranjivost koju treba popravljati, tako da ne postoje rešenja koja se mogu kupiti. Jedino se može postaviti fajervol ili neka druga sprava za filtriranje između napadnutog i neprijateljskog napada koji je u mogućnosti da randomizuje IP ID-jeve.
19.	Apache httpd apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpd-cve-2011-0419)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Skenirani servis je osjetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_autoindex. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_fnmatch() u sklopu APR biblioteke. Ako je omogućen mod_autoindex, a indeksi direktorijuma mod_autoindex su sadržavali fajlove sa dovoljno dugim nazivima, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do preterane upotrebe CPU-a. Ovo bi moglo da bude iskorišćeno u napadu odbijanja servisa. Zahvaljujući Maksymilian Arciemowicz-u prijavljen je ovaj propust.	CVE CVE-2011-0419 ³⁶⁴⁸ REDHAT RHSA-2011:0507 ³⁶⁴⁹ SECUNIA 44490 ³⁶⁵⁰ SECUNIA 44564 ³⁶⁵¹ SECUNIA 44574 ³⁶⁵² URL1 ³⁶⁵³	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.18.tar.gz
20.	Apache Etag Inode Information Leakage (http-apache-etag-inode-leak)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 U određenim konfiguracijama,	BID 6939 ³⁶⁵⁴ BID 6943 ³⁶⁵⁵ CVE CVE-2003-1418 ³⁶⁵⁶ XF apache-mime-information-	Ozbiljan	Onemogućiti Etag mehanizam tipa "inod-based" konfiguraciji Apache-a. Takođe, inod informacije je

³⁶³⁶ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval:def:5711>³⁶⁴⁴ <http://www.ietf.org/rfc/rfc2385.txt>³⁶³⁷ <http://secunia.com/advisories/11440/>³⁶³⁸ <http://secunia.com/advisories/11458/>³⁶³⁹ <http://secunia.com/advisories/22341/>³⁶⁴⁰ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>³⁶⁴¹ <http://xforce.iss.net/xforce/xfdb/15886>³⁶⁴² <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>³⁶⁴³ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>³⁶⁴⁵ <http://www.securityfocus.com/bid/4314>³⁶⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>³⁶⁴⁷ <http://xforce.iss.net/xforce/xfdb/8588>³⁶⁴⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419>³⁶⁴⁹ <http://rhn.redhat.com/errata/RHSA-2011-0507.html>³⁶⁵⁰ <http://secunia.com/advisories/44490/>³⁶⁵¹ <http://secunia.com/advisories/44564/>³⁶⁵² <http://secunia.com/advisories/44574/>³⁶⁵³ http://httpd.apache.org/security/vulnerabilities_22.html³⁶⁵⁴ <http://www.securityfocus.com/bid/6939>³⁶⁵⁵ <http://www.securityfocus.com/bid/6943>³⁶⁵⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-1418>

		Apache HTTP server dozvoljava udaljenim napadačima da dobiju poverljive informacije preko (1) Etag heder-a, koji otkriva broj inoda ili (2) razdvajanje višedelnih MIME-a, koja ukazuje na ID child procesa (PID). Određene verzije Apache-a koriste zahtevani broj čvorova fajla da bi konstruisali 'Etag' heder za odgovor. Iako sama po sebi nije ranjivost, ova informacija olakšava sprovođenje određenih NFS napada. „Running vulnerable HTTP service: Apache 2.2.14. <a a3746-b1-4a774f890d43c\""="" href="http://172.23.202.133/1: \">http://172.23.202.133/1: \"a3746-b1-4a774f890d43c\"”	disclosure(11438) ³⁶⁵⁷		moгуće ukloniti iz Etag heder-a tako što će se dodati direktiva u Apache konfiguraciju: FileETag Mtime Size.
21.	Apache httpd Subrequest handling of request headers (mod_headers) (CVE-2010-0434) (http://apacherequest-header-info-disclosure)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_headers. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust u jezgru "subrequest process code" može dovesti do greške tipa segmentation fault-a ili do otkrivanja podataka iz nekog drugog zahteva na thread-ovima servera, kao što su worker ili winnt MPM-ovi. Zahvaljujući Philip Pickett-u iz Vmware, ovaj propust je prijavljen i predložen je način ispravke.	BID 38494³⁶⁵⁸ CVE CVE-2010-0434³⁶⁵⁹ DEBIAN DSA-2035³⁶⁶⁰ OVAL OVAL10358³⁶⁶¹ OVAL OVAL8695³⁶⁶² REDHAT RHSA-2010:0168³⁶⁶³ REDHAT RHSA-2010:0175³⁶⁶⁴ SECUNIA 39100³⁶⁶⁵ SECUNIA 39115³⁶⁶⁶ SECUNIA 39501³⁶⁶⁷ SECUNIA 39628³⁶⁶⁸ SECUNIA 39632³⁶⁶⁹ SECUNIA 39656³⁶⁷⁰ SECUNIA 40096³⁶⁷¹ XF apache-http-rh-info-disclosure(56625)³⁶⁷² URL1³⁶⁷³	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz
22.	Apache Tomcat v4.x Example Scripts Information Leakage (http://tomcat-0005)	172.23.202.133:8080 172.23.202.132:8080 172.23.202.123:8080 172.23.202.229:8080 Sledeće skripte su navedene kao primeri koji dolaze sa Apache Tomcat-om v4.x, a koje napadači mogu da iskoriste da dobiju informacije o sistemu. Poznato je da su ove skripte ranjive na napad tipa "cross site scripting" (XSS): /examples/jsp/num/numguess.jsp /examples/jsp/dates/date.jsp /examples/jsp/snp/snoop.jsp /examples/jsp/error/error.html		Kritičan	U potpunosti obrisati ove skripte. Primeri skripta nikad ne treba da budu instalirani na serverima koji su u produkciji.

³⁶⁵⁷ <http://xforce.iss.net/xforce/xfdb/11438>³⁶⁵⁸ <http://www.securityfocus.com/bid/38494>³⁶⁵⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0434>³⁶⁶⁰ <http://www.debian.org/security/2010/dsa-2035>³⁶⁶¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10358>³⁶⁶² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8695>³⁶⁶³ <http://rhn.redhat.com/errata/RHSA-2010-0168.html>³⁶⁶⁴ <http://rhn.redhat.com/errata/RHSA-2010-0175.html>³⁶⁶⁵ <http://secunia.com/advisories/39100/>³⁶⁶⁶ <http://secunia.com/advisories/39115/>³⁶⁶⁷ <http://secunia.com/advisories/39501/>³⁶⁶⁸ <http://secunia.com/advisories/39628/>³⁶⁶⁹ <http://secunia.com/advisories/39632/>³⁶⁷⁰ <http://secunia.com/advisories/39656/>³⁶⁷¹ <http://secunia.com/advisories/40096/>³⁶⁷² <http://xforce.iss.net/xforce/xfdb/56625>³⁶⁷³ http://httpd.apache.org/security/vulnerabilities_22.html

		/examples/jsp/sessions/carts.html /examples/jsp/checkbox/check.html /examples/jsp/colors/colors.html /examples/jsp/cal/login.html /examples/jsp/include/include.jsp /examples/jsp/forward/forward.jsp /examples/jsp/plugin/plugin.jsp /examples/jsp/jspServlet/jspServlet.js p /examples/jsp/servlet/foo.jsp /examples/jsp/mail/sendmail.jsp /examples/servlet/HelloWorldExample /examples/servlet/RequestInfoExample /examples/servlet/RequestHeaderExample /examples/servlet/RequestParamExample /examples/servlet/CookieExample /examples/servlet/IndiServlet /examples/servlet/SessionExample /tomcat-docs/appdev/sample/web/hello.jsp			
23.	Self-signed TLS/SSL certificate (ssl-self-signed-certificate)	172.23.202.133:993 172.23.202.133:995 172.23.202.132:993 172.23.202.132:995 172.23.202.123:993 172.23.202.123:995 172.23.202.229:993 172.23.202.229:995 TLS/SSL-a sertifikat servera je samopotpisan. Samopotpisani sertifikati po defaultu nisu od poverenja, naročito zato što napadi na TLS/SSL preko posrednika obično koriste samopotpisane sertifikate da prisluškuju TLS/SSL veze.		Ozbiljan	Nabaviti novi TLS/SSL serverov sertifikat koji NIJE samopotpisan i instalirati ga na server. Precizna uputstva za dobijanje novog sertifikata zavise od zahteva organizacije. Uopšteno, treba napraviti zahtev za sertifikat i taj zahtev sačuvati kao fajl. Ovaj fajl se zatim šalje Certificate Authority-ju (CA) na obradu. Organizacija možda poseduje sopstveni interni Certificate Authority. U suprotnom, potrebno je platiti sertifikat iz spoljnog poverljivog Certificate Authority-ja, kao što su Thawte , Verisign .
24.	Autocomplete enabled for sensitive HTML form fields (spider-sensitive-form-data-autocomplete-enabled)	172.23.202.133:8080 172.23.202.132:8080 172.23.202.123:8080 172.23.202.229:8080 Web forma sadrži lozinke i druge rubrike sa osetljivim tekstom za koje je otvorena mogućnost auto-complete od strane web pretraživača. Funkcija auto-complete skladišti forme popunjenih rubrika i lozinke lokalno, na web pretraživaču, tako da se ove rubrike automatski popunjavaju kada korisnik ponovo poseti sajt. Osetljivi podaci i lozinke mogu biti ukradeni ako je korisnikov sistem kompromitovan. Međutim, treba imati u vidu da forma auto-complete nije standardna i da je to karakteristika web pretraživača koju svaki web pretraživač tretira na različit način. Na primer Opera zanemaruje ovu opciju i zahteva od korisnika da unese poverljive podatke		Umeren	Za svaku osetljivu rubriku u HTML, stavku „autocomplete“ potrebno je podesiti na „off“. Na primer: <input type=“password“ autocomplete=“off“ name=“pw“> Ako ima previše rubrika, možda je brže podesiti stavku „autocomplete“ na „off“ u spoljnom tagu <form>. Na primer: <form action=“/login.jsp“ autocomplete=“off“ name=“pw“> <input type=“password“ name=“pw“> </form>

		svaki put kada posećuje određeni web sajt.			
25.	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server. Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko poziva udaljenih procedura (RPC). Ovi servisi su i u prošlosti bili skloni ranjivostima.. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinjenije napade.	BID: 494³⁶⁷⁴ CVE: CVE-1999-0519³⁶⁷⁵ MSKB: 143474³⁶⁷⁶ URL1³⁶⁷⁷	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost.
26.	Apache default installation/welcome page installed (http://apache-default-install-page)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Apache difoltna instalacija ili „Welcome“ stranica je instalirana na serveru. To obično ukazuje na novoinstalirani server. U mnogim slučajevima, Apache se instalira zajedno sa drugim aplikacijama i korisnik možda nije svestan da je web server pokrenut. Ovakvi serveri se retko patch-uju i još ređe nadgledaju, što zlonamernim napadačima postaje pogodna meta koja najverovatnije neće pokrenuti nikakvo upozorenje. Primer : Running vulnerable HTTP service: Apache 2.2.14. http://172.23.202.133/ 1: <html><body><h1>It works!</h1>	OSVDB 2117 ³⁶⁷⁸	Umeren	Ako se od servera zahteva da obezbedi neophodnu funkcionalnost, onda difoltnu stranicu treba zameniti odgovarajućim sadržajem. U suprotnom, ovakav server treba ukloniti sa mreže, prateći bezbednosni princip minimalne složenosti (više složenosti = manja bezbednost). Ako server nije potreban, treba ga ukloniti iz svih startup fajlova (npr. /etc/rc*) ili skripti, a zatim prekinuti servis. Proveriti da li se on ponovo pokreće kada se mašina reboot-uje. Apache se uglavnom instalira kao /usr/sbin/httpd na UNIX mašinama ili kao C:\Program Files\Apache Group na Windows mašinama. Razmotriti uklanjanje binara i svih srodnih biblioteka iz sistema.
27.	Apache Tomcat default installation/welcome page installed (http://tomcat-default-install-page)	172.23.202.133:8080 172.23.202.132:8080 172.23.202.123:8080 172.23.202.229:8080 Tomcat difoltna instalacija ili „Welcome“ stranica je instalirana na serveru. To obično ukazuje na novoinstalirani server. U mnogim slučajevima, Tomcat se instalira zajedno sa drugim aplikacijama i korisnik možda nije	OSVDB 2117 ³⁶⁷⁹	Umeren	Ako se od servera zahteva da obezbedi neophodnu funkcionalnost, onda difoltnu stranicu treba zameniti odgovarajućim sadržajem. U suprotnom, ovakav server treba ukloniti sa mreže, prateći bezbednosni princip minimalne složenosti (više složenosti = manja bezbednost).

³⁶⁷⁴ <http://www.securityfocus.com/bid/494>³⁶⁷⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>³⁶⁷⁶ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>³⁶⁷⁷ http://www.hsc.fr/ressources/presentations/null_sessions/³⁶⁷⁸ http://www.osvdb.org/displayvuln.php?osvdb_id=2117 pristupljeno 11.12.2011³⁶⁷⁹ http://www.osvdb.org/displayvuln.php?osvdb_id=2117 pristupljeno 11.12.2011

		svestan da je web server pokrenut. Ovakvi serveri se retko patch-uju i još ređe nadgledaju, što zlonamernim napadačima postaje pogodna meta koja najverovatnije neće pokrenuti nikakvo upozorenje. Running vulnerable HTTP service: Apache Tomcat. http://172.23.202.122:8080/ 8: 9: <body> 10: <h1>It works !</h1> 11: 12: ... means you've setup Tomcat successfully. Congratulations!</p>			
28.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	CVE CVE-1999-0524³⁶⁸⁰ OSVDB 95³⁶⁸¹ XF icmp-netmask(306)³⁶⁸² XF icmp-timestamp(322)³⁶⁸³	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
29.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1³⁶⁸⁴ URL2³⁶⁸⁵ URL3³⁶⁸⁶	Umeren	Onemogućavanje TCP timestamp odgovora na Linux OS. Podesiti <code>net.ipv4.tcp_timestamps</code> vrednost na sledećem ključu na 0 pokretanjem sledeće komande: <pre>sysctl -w net.ipv4.tcp_timestamps=0</pre> Dodatno, sledeću vrednost u difoltnom <code>sysctl</code> konfiguracionom fajlu, <code>generally sysctl.conf</code>: <pre>net.ipv4.tcp_timestamps=0</pre>
30.	Database Open Access (database-open-access)	172.23.202.133:3306 172.23.202.132:3306 172.23.202.123:3306 172.23.202.229:3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim	URL1³⁶⁸⁷	Umeren	Konfigurisati server baze podataka tako da dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.

³⁶⁸⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>

³⁶⁸¹ <http://www.osvdb.org/95>

³⁶⁸² <http://xforce.iss.net/xforce/xfdb/306>

³⁶⁸³ <http://xforce.iss.net/xforce/xfdb/322>

³⁶⁸⁴ http://www.forensicswiki.org/wiki/TCP_timestamps

³⁶⁸⁵ <http://www.ietf.org/rfc/rfc1323.txt>

³⁶⁸⁶ <http://uptime.netcraft.com/>

³⁶⁸⁷ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf

		mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7			

Tabela 92. Linux OS – Pronađeni servisi na IP adresi 172.23.202.133 (2011. godina)

SERVISI	SAMBA 172.23.202.133 tcp 139 Samba 3.5.8 172.23.202.133 tcp 445 Samba 3.5.8 CIFS Name Service 172.23.202.133 udp 137 FTP 172.23.202.133 tcp 21 vsFTPD 2.2.2 ftp.banner: 220 (vsFTPD 2.2.2) HTTP 172.23.202.133 tcp 80 Apache 2.2.14 http.banner: Apache/2.2.14 (Ubuntu) http.banner.server: Apache/2.2.14 (Ubuntu) 172.23.202.133 tcp 8080 Apache Tomcat Coyote: 1.1 http.banner: Apache-Coyote/1.1 IMAP 172.23.202.133 tcp 143 Dovecot imap.banner: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE STARTTLS LOGINDISABLED] Dovecot ready. IMAPS³⁶⁸⁸ 172.23.202.133 tcp 993 Dovecot imap.banner: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE AUTH=PLAIN] Dovecot ready. POP 172.23.202.133 tcp 110 Dovecot pop.banner: +OK Dovecot ready. POPS³⁶⁸⁹ 172.23.202.133 tcp 995 Dovecot pop.banner: +OK Dovecot ready. MySQL 172.23.202.133 tcp 3306 SSH 172.23.202.133 tcp 22 OpenSSH 5.3p1 ssh.banner: SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu6 ssh.protocol.version: 2.0
Spidered Web site	http://172.23.202.133:80 Common Default URLs: <i>Access Error (403)</i> cgi-bin doc <i>Successful (200)</i>

³⁶⁸⁸ Internet Message Access Protocol (IMAPS) preko TLS/SSL-a se koristi za pristupanje i obradu elektronske pošte (e-mail) korišćenjem dešifrovanih (TLS/SSL) konekcija. Kada se uspostavi TLS/SSL konekcija, koristi se standardni IMAP protokol. IMAP serveri mogu sadržavati nekoliko foldera, aka mailbox-ova, koji sadrže poruke (e-mails) za korisnike.

³⁶⁸⁹ Post Office Protocol (POP) omogućava radnim stanicama da dinamički iz mailbox servera uzvraćaju elektronsku poštu (e-mail). POPS dodaje SSLpodršku POP3.

	Icons Guessed URLs <i>Access Error (403)</i> cgi-bin ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-doc %3f.jsp .svn Entries ADw-script AD4-alert(42) Adw scriptAD4- CVS Entries Root DEADJOE Trace.axd WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config <i>Redirect (301)</i> icons small <i>Successful (200)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-script+AD4- icons small index.html Linked URLs <i>Successful (200)</i> icons README README.html Small <u>http://172.23.202.133:8080</u> Common Default URLs <i>Successful (200)</i> docs examples Guessed URLs <i>Error (400)</i> examples jsp cal cal1.jsp%00 cal1.jsp%5C checkbox checkresult.jsp%00 checkresult.jsp%5C colors

	colrs.jsp%00 colrs.jsp%5C dates date.jsp%00 date.jsp%5C error err.jsp%00 err.jsp%5C forward forward.jsp%00 forward.jsp%5C include include.jsp%00 include.jsp%5C jsp2 el basic-arithmetic.jsp%00 basic-arithmetic.jsp%5C basic-comparisons.jsp%00 basic-comparisons.jsp%5C functions.jsp%00 functions.jsp%5C implicit-objects.jsp%00 jspattribute jspattribute.jsp%00 jspattribute.jsp%5C shuffle.jsp%00 shuffle.jsp%5C misc config.jsp%00 config.jsp%5C dynamicattrs.jsp%00 dynamicattrs.jsp%5C simpletag book.jsp%00 book.jsp%5C hello.jsp%00 hello.jsp%5C repeat.jsp%00 repeat.jsp%5C foo.jsp%00 foo.jsp%5C tagfiles hello.jsp%00 hello.jsp%5C panel.jsp%00 panel.jsp%5C products.jsp%00 products.jsp%5C jsptoserv jsptoservlet.jsp%00 num numguess.jsp%00 numguess.jsp%5C plugin plugin.jsp%00 plugin.jsp%5C sessions carts.jsp%00 carts.jsp%5C snp snoop.jsp%00 snoop.jsp%5C tagplugin choose.jsp%00 choose.jsp%5C foreach.jsp%00

	foreach.jsp%5C if.jsp%00 if.jsp%5C xml xml.jsp%00 xml.jsp%5C Error (500) examples jsp error errorpage.jsp Redirect (302) examples examples manager Requires Authentication (401) manager jmxproxy %3f.jsp .svn entries ?P=+ADw-script+AD4-alert(42)+Adw script+AD4- ADw-script AD4-alert(42) Adw scriptAD4- CVS Entries Root DEADJOE WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config Successful (200) ?P=+ADw-script+AD4-alert(42)+ADwscript+ AD4- script+AD4- script+AD4- script+AD4- script+AD4- script+AD4- docs api appdev sample index.html architecture Linked URLs Error (500) examples jsp jsp2 el functions.jsp?foo=JSP+2.0 functions.jsp?foo=JSP+2.0 implicit-objects.jsp?foo=bar implicit-objects.jsp?foo=bar jspx textRotate.jspx textRotate.jspx?name=JSPX

	tagfiles products.jsp <i>Redirect (302)</i> examples jsp jsp jsp servlets servlets servlets manager <i>Requires Authentication (401)</i> host-manager html manager deploy?path= foo findleaks html jmxproxy list reload?path= examples roles serverinfo sessions?path= examples <i>Successful (200)</i> docs RELEASE-NOTES.txt aio.html api index.html appdev build.xml.txt deployment.html index.html installation.html introduction.html processes.html sample sample.war source.html web.xml.txt apr.html architecture index.html overview.html requestProcess.html requestProcess requestProcess.pdf startup.html startup serverStartup.pdf serverStartup.txt balancer-howto.html building.html cgi-howto.html changelog.html class-loader-howto.html cluster-howto.html config ajp.html cluster-channel.html

	cluster-deployer.html colors ColorGameBean.html ColorGameBean.html clr.html clr.html colors.html colors.html colrs.jsp colrs.jsp colrs.jsp.html colrs.jsp.html dates date.html date.html date.jsp date.jsp date.jsp.html date.jsp.html

Tabela 93. Linux OS – Pronađeni servisi na IP adresi 172.23.202.132 (2011. godina)

SERVISI	SAMBA 172.23.202.132 tcp 139 Samba 3.5.8 172.23.202.132 tcp 445 Samba 3.5.8 CIFS Name Service 172.23.202.132 udp 137 FTP 172.23.202.132 tcp 21 vsFTPD 2.2.2 ftp.banner: 220 (vsFTPD 2.2.2) HTTP 172.23.202.132 tcp 80 Apache 2.2.14 http.banner: Apache/2.2.14 (Ubuntu) http.banner.server: Apache/2.2.14 (Ubuntu) 172.23.202.132 tcp 8080 Apache Tomcat Coyote: 1.1 http.banner: Apache-Coyote/1.1 IMAP 172.23.202.132 tcp 143 Dovecot imap.banner: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE STARTTLS LOGINDISABLED] Dovecot ready. IMAPS³⁶⁹⁰ 172.23.202.132 tcp 993 Dovecot imap.banner: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE AUTH=PLAIN] Dovecot ready. POP 172.23.202.132 tcp 110 Dovecot pop.banner: +OK Dovecot ready. POPS³⁶⁹¹ 172.23.202.132 tcp 995 Dovecot

³⁶⁹⁰ Internet Message Access Protocol (IMAPS) preko TLS/SSL-a se koristi za pristupanje i obradu elektronske pošte (e-mail) korišćenjem dešifrovanih (TLS/SSL) konekcija. Kada se uspostavi TLS/SSL konekcija, koristi se standardni IMAP protokol. IMAP serveri mogu sadržavati nekoliko foldera, aka mailbox-ova, koji sadrže poruke (e-mails) za korisnike.

³⁶⁹¹ Post Office Protocol (POP) omogućava radnim stanicama da dinamički iz mailbox servera uzvraćaju elektronsku poštu (e-mail). POPS dodaje SSLpodršku POP3.

	pop.banner: +OK Dovecot ready. MySQL 172.23.202.132 tcp 3306 SSH 172.23.202.132 tcp 22 OpenSSH 5.3p1 ssh.banner: SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu6 ssh.protocol.version: 2.0
Spidered Web site	http://172.23.202.132:80 Common Default URLs: <i>Access Error (403)</i> cgi-bin doc <i>Successful (200)</i> Icons Guessed URLs <i>Access Error (403)</i> cgi-bin ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-doc%3f.jsp .svn Entries ADw-script AD4-alert(42) AdwscriptAD4-CVS Entries Root DEADJOE Trace.axd WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config <i>Redirect (301)</i> icons small <i>Successful (200)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-script+AD4-icons small index.html Linked URLs <i>Successful (200)</i> icons README README.html Small http://172.23.202.132:8080

	Common Default URLs <i>Successful (200)</i> docs examples Guessed URLs <i>Error (400)</i> examples jsp cal cal1.jsp%00 cal1.jsp%5C checkbox checkresult.jsp%00 checkresult.jsp%5C colors colrs.jsp%00 colrs.jsp%5C dates date.jsp%00 date.jsp%5C error err.jsp%00 err.jsp%5C forward forward.jsp%00 forward.jsp%5C include include.jsp%00 include.jsp%5C jsp2 el basic-arithmetic.jsp%00 basic-arithmetic.jsp%5C basic-comparisons.jsp%00 basic-comparisons.jsp%5C functions.jsp%00 functions.jsp%5C implicit-objects.jsp%00 jspattribute jspattribute.jsp%00 jspattribute.jsp%5C shuffle.jsp%00 shuffle.jsp%5C misc config.jsp%00 config.jsp%5C dynamicattrs.jsp%00 dynamicattrs.jsp%5C simpletag book.jsp%00 book.jsp%5C hello.jsp%00 hello.jsp%5C repeat.jsp%00 repeat.jsp%5C foo.jsp%00 foo.jsp%5C tagfiles hello.jsp%00 hello.jsp%5C panel.jsp%00 panel.jsp%5C products.jsp%00 products.jsp%5C

	jsptoserv jsptoservlet.jsp%00 num numguess.jsp%00 numguess.jsp%5C plugin plugin.jsp%00 plugin.jsp%5C sessions carts.jsp%00 carts.jsp%5C snp snoop.jsp%00 snoop.jsp%5C tagplugin choose.jsp%00 choose.jsp%5C foreach.jsp%00 foreach.jsp%5C if.jsp%00 if.jsp%5C xml xml.jsp%00 xml.jsp%5C Error (500) examples jsp error errorpge.jsp Redirect (302) examples examples manager Requires Authentication (401) manager jmxproxy %3f.jsp .svn entries ?P=+ADw-script+AD4-alert(42)+Adw script+AD4- ADw-script AD4-alert(42) Adw scriptAD4- CVS Entries Root DEADJOE WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config Successful (200) ?P=+ADw-script+AD4-alert(42)+ADwscript+ AD4- script+AD4- script+AD4- script+AD4- script+AD4- script+AD4- docs api appdev

	sample index.html architecture Linked URLs <i>Error (500)</i> examples jsp jsp2 el functions.jsp?foo=JSP+2.0 functions.jsp?foo=JSP+2.0 implicit-objects.jsp?foo=bar implicit-objects.jsp?foo=bar jspx textRotate.jspx textRotate.jspx?name=JSPX tagfiles products.jsp <i>Redirect (302)</i> examples jsp jsp jsp servlets servlets servlets manager <i>Requires Authentication (401)</i> host-manager html manager deploy?path= foo findleaks html jmxproxy list reload?path= examples roles serverinfo sessions?path= examples <i>Successful (200)</i> docs RELEASE-NOTES.txt aio.html api index.html appdev build.xml.txt deployment.html index.html installation.html introduction.html processes.html sample sample.war source.html web.xml.txt apr.html architecture

	index.html overview.html requestProcess.html requestProcess requestProcess.pdf startup.html startup serverStartup.pdf serverStartup.txt balancer-howto.html building.html cgi-howto.html changelog.html class-loader-howto.html cluster-howto.html config ajp.html cluster-channel.html cluster-deployer.html colors ColorGameBean.html ColorGameBean.html clr.html clr.html colors.html colors.html colrs.jsp colrs.jsp colrs.jsp.html colrs.jsp.html dates date.html date.html date.jsp date.jsp date.jsp.html date.jsp.html

Tabela 94. Linux OS – Pronađeni servisi na IP adresi 172.23.202.123 (2011. godina)

SERVISI	SAMBA 172.23.202.123 tcp 139 Samba 3.5.8 172.23.202.123 tcp 445 Samba 3.5.8 CIFS Name Service 172.23.202.123 udp 137 FTP 172.23.202.123 tcp 21 vsFTPD 2.2.2 ftp.banner: 220 (vsFTPD 2.2.2) HTTP 172.23.202.123 tcp 80 Apache 2.2.14 http.banner: Apache/2.2.14 (Ubuntu) http.banner.server: Apache/2.2.14 (Ubuntu) 172.23.202.123 tcp 8080 Apache Tomcat Coyote: 1.1 http.banner: Apache-Coyote/1.1 IMAP 172.23.202.123 tcp 143 Dovecot imap.banner: * OK [CAPABILITY IMAP4rev1 LITERAL+

	SASL-IR LOGIN-REFERRALS ID ENABLE STARTTLS LOGINDISABLED] Dovecot ready. IMAPS³⁶⁹² 172.23.202.123 tcp 993 Dovecot imap.banner: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE AUTH=PLAIN] Dovecot ready. POP 172.23.202.123 tcp 110 Dovecot pop.banner: +OK Dovecot ready. POPS³⁶⁹³ 172.23.202.123 tcp 995 Dovecot pop.banner: +OK Dovecot ready. MySQL 172.23.202.123 tcp 3306 SSH 172.23.202.123 tcp 22 OpenSSH 5.3p1 ssh.banner: SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu6 ssh.protocol.version: 2.0
Spidered Web site	http://172.23.202.123:80 Common Default URLs: <i>Access Error (403)</i> cgi-bin doc <i>Successful (200)</i> Icons Guessed URLs <i>Access Error (403)</i> cgi-bin ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-doc%3f.jsp .svn Entries ADw-script AD4-alert(42) AdwscriptAD4-CVS Entries Root DEADJOE Trace.axd WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config <i>Redirect (301)</i> icons small

³⁶⁹² Internet Message Access Protocol (IMAPS) preko TLS/SSL-a se koristi za pristupanje i obradu elektronske pošte (e-mail) korišćenjem dešifrovanih (TLS/SSL) konekcija. Kada se uspostavi TLS/SSL konekcija, koristi se standardni IMAP protokol. IMAP serveri mogu sadržavati nekoliko foldera, aka mailbox-ova, koji sadrže poruke (e-mails) za korisnike.

³⁶⁹³ Post Office Protocol (POP) omogućava radnim stanicama da dinamički iz mailbox servera uzvraćaju elektronsku poštu (e-mail). POPS dodaje SSLpodršku POP3.

	<i>Successful (200)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-script+AD4-icons small index.html Linked URLs <i>Successful (200)</i> icons README README.html Small http://172.23.202.123:8080 Common Default URLs <i>Successful (200)</i> docs examples Guessed URLs <i>Error (400)</i> examples jsp cal cal1.jsp%00 cal1.jsp%5C checkbox checkresult.jsp%00 checkresult.jsp%5C colors colrs.jsp%00 colrs.jsp%5C dates date.jsp%00 date.jsp%5C error err.jsp%00 err.jsp%5C forward forward.jsp%00 forward.jsp%5C include include.jsp%00 include.jsp%5C jsp2 el basic-arithmetic.jsp%00 basic-arithmetic.jsp%5C basic-comparisons.jsp%00 basic-comparisons.jsp%5C functions.jsp%00 functions.jsp%5C implicit-objects.jsp%00 jspattribute jspattribute.jsp%00 jspattribute.jsp%5C shuffle.jsp%00 shuffle.jsp%5C misc config.jsp%00

	config.jsp%5C dynamicattrs.jsp%00 dynamicattrs.jsp%5C simpletag book.jsp%00 book.jsp%5C hello.jsp%00 hello.jsp%5C repeat.jsp%00 repeat.jsp%5C foo.jsp%00 foo.jsp%5C tagfiles hello.jsp%00 hello.jsp%5C panel.jsp%00 panel.jsp%5C products.jsp%00 products.jsp%5C jsptoserv jsptoservlet.jsp%00 num numguess.jsp%00 numguess.jsp%5C plugin plugin.jsp%00 plugin.jsp%5C sessions carts.jsp%00 carts.jsp%5C snp snoop.jsp%00 snoop.jsp%5C tagplugin choose.jsp%00 choose.jsp%5C foreach.jsp%00 foreach.jsp%5C if.jsp%00 if.jsp%5C xml xml.jsp%00 xml.jsp%5C Error (500) examples jsp error errorpage.jsp Redirect (302) examples examples manager Requires Authentication (401) manager jmxproxy %3f.jsp .svn entries ?P=+ADw-script+AD4-alert(42)+Adw script+AD4- ADw-script AD4-alert(42) Adw scriptAD4- CVS Entries Root

	DEADJOE WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config <i>Successful (200)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-script+AD4-script+AD4-script+AD4-script+AD4-docs api appdev sample index.html architecture Linked URLs <i>Error (500)</i> examples jsp jsp2 el functions.jsp?foo=JSP+2.0 functions.jsp?foo=JSP+2.0 implicit-objects.jsp?foo=bar implicit-objects.jsp?foo=bar jspx textRotate.jspx textRotate.jspx?name=JSPX tagfiles products.jsp <i>Redirect (302)</i> examples jsp jsp jsp servlets servlets servlets manager <i>Requires Authentication (401)</i> host-manager html manager deploy?path=foo findleaks html jmxproxy list reload?path=examples roles serverinfo sessions?path=examples

	<i>Successful (200)</i> docs RELEASE-NOTES.txt aio.html api index.html appdev build.xml.txt deployment.html index.html installation.html introduction.html processes.html sample sample.war source.html web.xml.txt apr.html architecture index.html overview.html requestProcess.html requestProcess requestProcess.pdf startup.html startup serverStartup.pdf serverStartup.txt balancer-howto.html building.html cgi-howto.html changelog.html class-loader-howto.html cluster-howto.html config ajp.html cluster-channel.html cluster-deployer.html colors ColorGameBean.html ColorGameBean.html clr.html clr.html colors.html colors.html colrs.jsp colrs.jsp colrs.jsp.html colrs.jsp.html dates date.html date.html date.jsp date.jsp date.jsp.html date.jsp.html

Tabela 95. Linux OS – Pronađeni servisi na IP adresi 172.23.202.229 (2011. godina)

SERVISI	SAMBA 172.23.202.229 tcp 139 Samba 3.5.8 172.23.202.229 tcp 445 Samba 3.5.8 CIFS Name Service 172.23.202.229 udp 137

	FTP 172.23.202.229 tcp 21 vsFTPD 2.2.2 ftp.banner: 220 (vsFTPD 2.2.2) HTTP 172.23.202.229 tcp 80 Apache 2.2.14 http.banner: Apache/2.2.14 (Ubuntu) http.banner.server: Apache/2.2.14 (Ubuntu) 172.23.202.229 tcp 8080 Apache Tomcat Coyote: 1.1 http.banner: Apache-Coyote/1.1 IMAP 172.23.202.229 tcp 143 Dovecot imap.banner: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE STARTTLS LOGINDISABLED] Dovecot ready. IMAPS³⁶⁹⁴ 172.23.202.229 tcp 993 Dovecot imap.banner: * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE AUTH=PLAIN] Dovecot ready. POP 172.23.202.229 tcp 110 Dovecot pop.banner: +OK Dovecot ready. POPS³⁶⁹⁵ 172.23.202.133 tcp 995 Dovecot pop.banner: +OK Dovecot ready. MySQL 172.23.202.229 tcp 3306 SSH 172.23.202.229 tcp 22 OpenSSH 5.3p1 ssh.banner: SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu6 ssh.protocol.version: 2.0
Spidered Web site	http://172.23.202.229:80 Common Default URLs: <i>Access Error (403)</i> cgi-bin doc <i>Successful (200)</i> Icons Guessed URLs <i>Access Error (403)</i> cgi-bin ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-doc%3f.jsp .svn Entries

³⁶⁹⁴ Internet Message Access Protocol (IMAPS) preko TLS/SSL-a se koristi za pristupanje i obradu elektronske pošte (e-mail) korišćenjem dešifrovanih (TLS/SSL) konekcija. Kada se uspostavi TLS/SSL konekcija, koristi se standardni IMAP protokol. IMAP serveri mogu sadržavati nekoliko foldera, aka mailbox-ova, koji sadrže poruke (e-mails) za korisnike.

³⁶⁹⁵ Post Office Protocol (POP) omogućava radnim stanicama da dinamički iz mailbox servera uzvraćaju elektronsku poštu (e-mail). POPS dodaje SSLpodršku POP3.

	ADw-script AD4-alert(42) Adw scriptAD4- CVS Entries Root DEADJOE Trace.axd WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config <i>Redirect (301)</i> icons small <i>Successful (200)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+ AD4- script+AD4- script+AD4- icons small index.html Linked URLs <i>Successful (200)</i> icons README README.html Small http://172.23.202.229:8080 Common Default URLs <i>Successful (200)</i> docs examples Guessed URLs <i>Error (400)</i> examples jsp cal cal1.jsp%00 cal1.jsp%5C checkbox checkresult.jsp%00 checkresult.jsp%5C colors colrs.jsp%00 colrs.jsp%5C dates date.jsp%00 date.jsp%5C error err.jsp%00 err.jsp%5C forward forward.jsp%00 forward.jsp%5C include include.jsp%00

	include.jsp%5C jsp2 el basic-arithmetic.jsp%00 basic-arithmetic.jsp%5C basic-comparisons.jsp%00 basic-comparisons.jsp%5C functions.jsp%00 functions.jsp%5C implicit-objects.jsp%00 jspattribute jspattribute.jsp%00 jspattribute.jsp%5C shuffle.jsp%00 shuffle.jsp%5C misc config.jsp%00 config.jsp%5C dynamicattrs.jsp%00 dynamicattrs.jsp%5C simpletag book.jsp%00 book.jsp%5C hello.jsp%00 hello.jsp%5C repeat.jsp%00 repeat.jsp%5C foo.jsp%00 foo.jsp%5C tagfiles hello.jsp%00 hello.jsp%5C panel.jsp%00 panel.jsp%5C products.jsp%00 products.jsp%5C jsptoserv jsptoservlet.jsp%00 num numguess.jsp%00 numguess.jsp%5C plugin plugin.jsp%00 plugin.jsp%5C sessions carts.jsp%00 carts.jsp%5C snp snoop.jsp%00 snoop.jsp%5C tagplugin choose.jsp%00 choose.jsp%5C foreach.jsp%00 foreach.jsp%5C if.jsp%00 if.jsp%5C xml xml.jsp%00 xml.jsp%5C Error (500) examples jsp error errorpge.jsp Redirect (302)

	examples examples manager <i>Requires Authentication (401)</i> manager jmxproxy %3f.jsp .svn entries ?P=+ADw-script+AD4-alert(42)+Adw script+AD4- ADw-script AD4-alert(42) Adw scriptAD4- CVS Entries Root DEADJOE WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config <i>Successful (200)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+ AD4- script+AD4- script+AD4- script+AD4- script+AD4- script+AD4- script+AD4- docs api appdev sample index.html architecture Linked URLs <i>Error (500)</i> examples jsp jsp2 el functions.jsp?foo=JSP+2.0 functions.jsp?foo=JSP+2.0 implicit-objects.jsp?foo=bar implicit-objects.jsp?foo=bar jspx textRotate.aspx textRotate.aspx?name=JSPX tagfiles products.jsp <i>Redirect (302)</i> examples jsp jsp jsp servlets servlets servlets manager

	<i>Requires Authentication (401)</i> host-manager html manager deploy?path= foo findleaks html jmxproxy list reload?path= examples roles serverinfo sessions?path= examples <i>Successful (200)</i> docs RELEASE-NOTES.txt aio.html api index.html appdev build.xml.txt deployment.html index.html installation.html introduction.html processes.html sample sample.war source.html web.xml.txt apr.html architecture index.html overview.html requestProcess.html requestProcess requestProcess.pdf startup.html startup serverStartup.pdf serverStartup.txt balancer-howto.html building.html cgi-howto.html changelog.html class-loader-howto.html cluster-howto.html config ajp.html cluster-channel.html cluster-deployer.html colors ColorGameBean.html ColorGameBean.html clr.html clr.html colors.html colors.html colrs.jsp colrs.jsp colrs.jsp.html colrs.jsp.html dates

	date.html date.html date.jsp date.jsp date.jsp.html date.jsp.html

Tabela 96. Linux OS sa IP adresama 172.23.202.197 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.197		OS: Debian 60 x86, debian60x86			23
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Anonymous users can obtain the Windows password policy (cifs-nt-0002)	Korišćenjem CIFS NULL sesije, anonimni korisnik može da dobije uvid u polisu šifri. Polisa šifri sadrži osetljive informacije o najmanjoj mogućoj dužini lozinke, zaključavanje šifre, vremensko trajanje zaključanosti šifre itd.	SANS-01 W5 ³⁶⁹⁶ CVE CVE-2000-1200 ³⁶⁹⁷ XF nt-lsa-domain-sid(4015) ³⁶⁹⁸ SANS-02 W5 ³⁶⁹⁹ BID 959 ³⁷⁰⁰ SANS-04 W3 ³⁷⁰¹ SANS-03 W5 ³⁷⁰² BID 87 ³⁷⁰³	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost
2.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.197:139 172.23.202.197:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB 887429 URL1 ³⁷⁰⁴	Ozbiljan	Metoda za konfiguiranje SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429 ³⁷⁰⁵ . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracionom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing = auto</i> ili da se zahteva SMB potpisivanje: <i>server signing = mandatory</i>
3.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.197:139 172.23.202.197:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti
4.	Apache httpd expat DoS (CVE-2009-3560) (apache-httpd-2_2_x-cve-2009-3560)	172.23.202.197:80 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML	BID 37203 ³⁷⁰⁶ CVE CVE-2009-3560 ³⁷⁰⁷ DEBIAN DSA-1953 ³⁷⁰⁸ OVAL OVAL10613 ³⁷⁰⁹ OVAL OVAL6883 ³⁷¹⁰	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz

³⁶⁹⁶ <http://www.sans.org/critical-security-controls/#w5>³⁶⁹⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2000-1200>³⁶⁹⁸ <http://xforce.iss.net/xforce/xfdb/4015>³⁶⁹⁹ <http://www.sans.org/critical-security-controls/#w5>³⁷⁰⁰ <http://www.securityfocus.com/bid/959>³⁷⁰¹ <http://www.sans.org/critical-security-controls/#w3>³⁷⁰² <http://www.sans.org/critical-security-controls/#w5>³⁷⁰³ <http://www.securityfocus.com/bid/87>³⁷⁰⁴ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>³⁷⁰⁵ <http://support.microsoft.com/kb/887429>³⁷⁰⁶ <http://www.securityfocus.com/bid/37203>³⁷⁰⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3560>³⁷⁰⁸ <http://www.debian.org/security/2009/dsa-1953>³⁷⁰⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10613>

		dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepoverljivi XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	SECUNIA 37537 ³⁷¹¹ SECUNIA 38231 ³⁷¹² SECUNIA 38794 ³⁷¹³ SECUNIA 38832 ³⁷¹⁴ SECUNIA 38834 ³⁷¹⁵ SECUNIA 39478 ³⁷¹⁶ SECUNIA 41701 ³⁷¹⁷ SECUNIA 43300 ³⁷¹⁸ URL1 ³⁷¹⁹		
5.	Apache httpd expat DoS (CVE-2009-3720) (apache-httpd-2_2_x-cve-2009-3720)	172.23.202. 197:80 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepoverljivi XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	CVE CVE-2009-3720 ³⁷²⁰ OVAL OVAL11019 ³⁷²¹ OVAL OVAL7112 ³⁷²² REDHAT RHSA-2010:0002 ³⁷²³ SECUNIA 37324 ³⁷²⁴ SECUNIA 37537 ³⁷²⁵ SECUNIA 37925 ³⁷²⁶ SECUNIA 38050 ³⁷²⁷ SECUNIA 38231 ³⁷²⁸ SECUNIA 38794 ³⁷²⁹ SECUNIA 38832 ³⁷³⁰ SECUNIA 38834 ³⁷³¹ SECUNIA 39478 ³⁷³² SECUNIA 41701 ³⁷³³ SECUNIA 43300 ³⁷³⁴ URL1 ³⁷³⁵	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
6.	Apache httpd apr_bridage_split_line DoS (CVE-2010-1623) (apache-httpd-2_2_x-cve-2010-1623)	172.23.202. 197:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako Apache procesira ne-SSL zahteve. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti.	BID 43673 ³⁷³⁶ CVE CVE-2010-1623 ³⁷³⁷ REDHAT RHSA-2010:0950 ³⁷³⁸ SECUNIA 41701 ³⁷³⁹ SECUNIA 42015 ³⁷⁴⁰	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz

³⁷¹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6883>³⁷¹¹ <http://secunia.com/advisories/37537/>³⁷¹² <http://secunia.com/advisories/38231/>³⁷¹³ <http://secunia.com/advisories/38794/>³⁷¹⁴ <http://secunia.com/advisories/38832/>³⁷¹⁵ <http://secunia.com/advisories/38834/>³⁷¹⁶ <http://secunia.com/advisories/39478/>³⁷¹⁷ <http://secunia.com/advisories/41701/>³⁷¹⁸ <http://secunia.com/advisories/43300/>³⁷¹⁹ http://httpd.apache.org/security/vulnerabilities_22.html³⁷²⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3720>³⁷²¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11019>³⁷²² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7112>³⁷²³ <http://rhn.redhat.com/errata/RHSA-2010-0002.html>³⁷²⁴ <http://secunia.com/advisories/37324/>³⁷²⁵ <http://secunia.com/advisories/37537/>³⁷²⁶ <http://secunia.com/advisories/37925/>³⁷²⁷ <http://secunia.com/advisories/38050/>³⁷²⁸ <http://secunia.com/advisories/38231/>³⁷²⁹ <http://secunia.com/advisories/38794/>³⁷³⁰ <http://secunia.com/advisories/38832/>³⁷³¹ <http://secunia.com/advisories/38834/>³⁷³² <http://secunia.com/advisories/39478/>³⁷³³ <http://secunia.com/advisories/41701/>³⁷³⁴ <http://secunia.com/advisories/43300/>³⁷³⁵ http://httpd.apache.org/security/vulnerabilities_22.html³⁷³⁶ <http://www.securityfocus.com/bid/43673>³⁷³⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1623>³⁷³⁸ <http://rhn.redhat.com/errata/RHSA-2010-0950.html>³⁷³⁹ <http://secunia.com/advisories/41701/>

		Propust je otkriven u funkciji <code>apr_brigade_split_line()</code> u sklopu APR-util library, koji se koristi za procesiranje ne-SSL zahteva. Zlonamerni napadač bi mogao da šalje zahteve, pažljivo izrađujući tajming za pojedinačne bajtove, što bi polako zauzimalo memoriju i potencijalno dovelo do odbijanja servisa.	SECUNIA 42361 ³⁷⁴¹ SECUNIA 42367 ³⁷⁴² SECUNIA 42403 ³⁷⁴³ SECUNIA 42537 ³⁷⁴⁴ SECUNIA 43211 ³⁷⁴⁵ SECUNIA 43285 ³⁷⁴⁶ URL1 ³⁷⁴⁷		
7.	X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch)	172.23.202. 197:993 Rubrika u sertifikatu X.509 sa uobičajenim nazivom subjekta (CN) ne poklapa se sa imenom pojedinca koje je navedeno u sertifikatu. Pre izdavanja sertifikata, Certification Authority (CA) mora da proveriti identitet pojedinca koji potražuje sertifikat, kako je navedeno u CA-ovom Certification Practice Statement (CPS). Zbog toga, uobičajene procedure validacije sertifikata zahtevaju da rubrika sertifikata sa CN subjektom odgovara pravom imenu pojedinca koji prikazuje sertifikat. Na primer, u sertifikatu prikazanom na „https://www.example.com/“, naziv subjekta (CN) treba da bude „www.example.com“. U cilju otkrivanja i sprečavanja napada prisluškivanja, validnost sertifikata mora da bude overena, jer bi u suprotnom napadač mogao da otpočne napad preko posrednika i da stekne potpunu kontrolu nad protokom podataka. Od posebne važnosti je validnost naziva subjekta (CN), koji treba da se poklapa sa imenom pojedinca (imenom host-a). Neodgovarajući CN se najčešće javlja usled greške u konfiguraciji, iako on takođe može da ukazuje na to da se sprovodi napad preko posrednika.		Ozbiljan	Rubrika sa uobičajenim nazivom subjekta (CN) u sertifikatu X.509 treba da bude podešena da sadrži ime pojedinca koji prikazuje sertifikat (npr. ime hosta). To se postiže izradom novog sertifikata, koji najčešće potpisuje Certification Authority (CA), koji je od poverenja kako za klijenta, tako i za server.
8.	FTP access with ftp account (ftp-generic-0001)	172.23.202. 197:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisnikovim ID-jem (identifikacijom) "ftp" i šifrom "ftp". Dosadašnja praksa je pokazala da je najbolje ukloniti difoltnu naloge, ukoliko je to moguće. Za naloge koje sistem zahteva treba izmeniti difoltnu šifru.	CVE CVE-1999-0497 ³⁷⁴⁸	Ozbiljan	Ukloniti ili onemogućiti nalog, ukoliko to nije kritično za funkcionisanje sistema. U suprotnom, lozinku treba promeniti u onu koja nije po difoltu.
9.	FTP access with anonymous account	172.23.202. 197:21 Mnogi FTP serveri podržavaju	CVE CVE-1999-0497 ³⁷⁴⁹	Ozbiljan	Ukloniti ili onemogućiti nalog, ukoliko to nije

³⁷⁴⁰ <http://secunia.com/advisories/42015/>³⁷⁴¹ <http://secunia.com/advisories/42361/>³⁷⁴² <http://secunia.com/advisories/42367/>³⁷⁴³ <http://secunia.com/advisories/42403/>³⁷⁴⁴ <http://secunia.com/advisories/42537/>³⁷⁴⁵ <http://secunia.com/advisories/43211/>³⁷⁴⁶ <http://secunia.com/advisories/43285/>³⁷⁴⁷ http://httpd.apache.org/security/vulnerabilities_22.html³⁷⁴⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>³⁷⁴⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>

	(ftp-generic-0002)	difoltni nalog sa korisnikovim ID-jem (identifikacijom) "anonymous" i lozinkom "ftp@". Dosadašnja praksa je pokazala da je najbolje ukloniti difoltna naloge, ukoliko je to moguće. Za naloge koje sistem zahteva treba izmeniti difoltnu šifru.			kritično za funkcionisanje sistema. U suprotnom, lozinku treba promeniti u onu koja nije po difoltu.
10.	FTP server does not support AUTH command (ftp-generic-0007)	172.23.202. 197:21 FTP klijenti po difoltu šalju FTP server-u poverljive podatke (korisnički ID i šifra) u vidu čitkog teksta. Ova okolnost dozvoljava zlonamernim korisnicima da presreću poverljive podatke ukoliko prisluškuju vezu. Noviji FTP serveri podržavaju AUTH komandu, koja omogućava dodatne opcije autentifikacije, kao što su TLS, Kerberos, GSSAPI itd. Ona se može koristiti za sprečavanje prisluškivanja na FTP vezama.		Ozbiljan	Ažurirati/preći na FTP server koji podržava AUTH komandu.
11.	Browsable web directory (http-generic-browsable-dir)	172.23.202. 197:80 Otkriven je direktorijum na web serveru koji može biti pretraživan, što znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice - spajdering (prateći hiperlinkove), ili -kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute force napadom na liste uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skrivena“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice. http://172.23.202.197/icons/small/ 4: <title>Index of /icons/small</title> 5: </head> 6: <body> 7: Index of /icons/small 8: ...CO]“</th><th>Name</th><th><a href=“?C=M;O=A...</th>		Ozbiljan	Za Apache: onemogućiti brauzovanje direktorijuma mreže za sve direktorijume i poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim ako postoji potreba da ovi fajlovi budu dostupni preko web-a. Povremeno proći kroz web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume.
12.	TLS/SSL Server Supports Weak Cipher Algorithms (ssl-weak-ciphers)	172.23.202. 197:993 negotiated the SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA cipher suite TLS/SSL server podržava šifre koje se zasnivaju na slabim algoritmima. To napadaču može omogućiti da pokrene napade preko posrednika i da pregleda ili čačka osetljive podatke. Uopšteno, sledeće šifre se smatraju slabim: Tzv. „null“ (nula) šifre, jer ne šifruju podatke. Eksportne šifre koje koriste dužine tajnih ključeva ograničene na 40 bitova. Na to najčešće ukazuje reč EXP/EXPORT u nazivu šifre.		Ozbiljan	Konfigurisati server tako da onemogući podršku za slabe šifre. Za Apache web servere sa mod_ssl, uključiti fajl Apache konfiguracije i izmeniti liniju SSLCipherSuite tako da u njoj piše: SSLCipherSuite ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM

		Zastareli algoritmi za šifrovanje čije se dužine tajnih ključeva po današnjim standardima smatraju kratkim, npr. DES ili RC4 sa 56-bitnim ključevima.			
13.	TLS/SSL Server Supports SSLv2 (sslv2-and-up-enabled)	172.23.202. 197:993 Iako server prihvata klijente koji koriste TLS ili SSLv3, on takođe prihvata klijente koji koriste SSLv2. SSLv2 je starija implementacija Secure Sockets Layer protokola. Ima veliki broj bezbednosnih propusta koji omogućavaju zlonamenrim napadačima da preuzmu i menjaju informacije koje razmenjuju klijent i server, uključujući i slabosti koje se odnose na posredne napade (eng. man in the middle) tokom handshake postupka. Eksportovani setovi šifara nepotrebno oslabljuju MAC-ove. Istovetni kriptografski ključevi se koriste za autentifikaciju poruke i kriptovanje. S obzirom da je ranjiv na napade koji uzrokuju falsifikovanje i odsecanje TCP FIN paketa, SSLv2 je postao nepoželjan i više se ne preporučuje. Ni SSLv2, ni SSLv3 ne odgovaraju U.S. FIPS 140-2 standardima, koji važe u kriptografskim modulima u upotrebi unutar federalnih informacionih sistema. Samo noviji TLS (Transport Layer Security) protokol odgovara FIPS 140-2 zahtevima. Osim toga, isključivo prisustvo SSLv2-a se smatra greškom od strane PCI-a (Payment Card Industry) Data Security Standard. Ova ranjivost će biti prijavljena ako udaljeni server podržava SSLv2, ne uzimajući u obzir da se takođe podržavaju TLS ili SSLv3.	URL1³⁷⁵⁰ URL2³⁷⁵¹	Ozbiljan	Konfigurisati server tako da se od klijenta zahteva upotreba najmanje SSLv3 ili TLS. Kada je reč o Microsoft IIS web serverima konsultovati Microsoft Knowledgebase odeljak Q187498 za instrukcije koje se odnose na onemogućavanje SSL 2.0. Za Apache web servere sa omogućenim mod_ssl, izmeniti Apache konfiguracioni fajl da za sekciju SSLCipherSuite piše: SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:!SSLv2 Znak ! (znak uzvika) ispred SSLv2 je ono što onemogućava ovaj protokol.
14.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	172.23.202. 197:139 Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hедера i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183³⁷⁵² CERT-VN: 415294³⁷⁵³ CVE CVE-2004-0230³⁷⁵⁴ MS: MS05-019³⁷⁵⁵ MS: MS06-064³⁷⁵⁶ NETBSD: NetBSD-SA2004-006³⁷⁵⁷ OVAL: OVAL2689³⁷⁵⁸ OVAL: OVAL270³⁷⁵⁹ OVAL OVAL3508³⁷⁶⁰ OVAL OVAL4791³⁷⁶¹ OVAL OVAL5711³⁷⁶²	Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC 2385³⁷⁷⁰. Ono je napravljeno da smanji opasnost od određenih napada na BGP, kao što su TCP reseti.

³⁷⁵⁰ https://www.pcisecuritystandards.org/pdfs/pcissc_assessors_nl_2008-11.pdf

³⁷⁵¹ www.eucybervote.org/Reports/MSI-WP2-D7V1-V1.0-02.htm pristupljeno 11.12.2011

³⁷⁵² <http://www.securityfocus.com/bid/10183>

³⁷⁵³ <http://www.kb.cert.org/vuls/id/415294>

³⁷⁵⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>

³⁷⁵⁵ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>

³⁷⁵⁶ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>

³⁷⁵⁷ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>

³⁷⁵⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>

³⁷⁵⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>

³⁷⁶⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>

³⁷⁶¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>

			SECUNIA: 11440 ³⁷⁶³ SECUNIA 11458 ³⁷⁶⁴ SECUNIA: 22341 ³⁷⁶⁵ SGI 20040403-01-A ³⁷⁶⁶ XF tcp-rst-dos(15886) ³⁷⁶⁷ URL1 ³⁷⁶⁸ URL2 ³⁷⁶⁹		
15.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podesi na jedinstvenu vrednost i da se koristi u rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da fingerprint-uje operativni sistem.	BID 4314 ³⁷⁷¹ CVE CVE-2002-0510 ³⁷⁷² XF linux-udp-fingerprint(8588) ³⁷⁷³	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili pak ranjivost koju treba popravljati, tako da ne postoje rešenja koja se mogu kupiti. Jedino se može postaviti fajervol ili neka druga sprava za filtriranje između napadnutog i neprijateljskog napada koji je u mogućnosti da randomizuje IP ID-jeve.
16.	Apache httpd apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpd-cve-2011-0419)	172.23.202. 197:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_autoindex. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_fnmatch() u sklopu APR biblioteke. Ako je omogućen mod_autoindex, a indeksi direktorijuma mod_autoindex su sadržavali fajlove sa dovoljno dugim nazivima, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do preterane upotrebe CPU-a. Ovo bi moglo da bude iskorišćeno u napadu odbijanja servisa. Zahvaljujući Maksymilian Arciemowicz prijavljen je ovaj propust.	CVE CVE-2011-0419 ³⁷⁷⁴ REDHAT RHSA-2011:0507 ³⁷⁷⁵ SECUNIA 44490 ³⁷⁷⁶ SECUNIA 44564 ³⁷⁷⁷ SECUNIA 44574 ³⁷⁷⁸ URL1 ³⁷⁷⁹	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.18.tar.gz
17.	Apache Etag Inode Information Leakage (http-apache-etag-inode-leak)	172.23.202. 197:80 U određenim konfiguracijama, Apache HTTP server dozvoljava udaljenim napadačima da dobiju poverljive informacije preko (1) Etag heder-a, koji otkriva broj inoda ili (2) razdvajace višedelnih MIME-a, koja ukazuje na ID child procesa (PID).	BID 6939 ³⁷⁸⁰ BID 6943 ³⁷⁸¹ CVE CVE-2003-1418 ³⁷⁸² XF apache-mime-information-disclosure(11438) ³⁷⁸³	Ozbiljan	Onemogućiti Etag mehanizam tipa "inod-based" konfiguraciji Apache-a. Takođe, inod informacije je moguće ukloniti iz Etag heder-a tako što će se dodati direktiva u Apache

³⁷⁶² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>³⁷⁷⁰ <http://www.ietf.org/rfc/rfc2385.txt>³⁷⁶³ <http://secunia.com/advisories/11440/>³⁷⁶⁴ <http://secunia.com/advisories/11458/>³⁷⁶⁵ <http://secunia.com/advisories/22341/>³⁷⁶⁶ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>³⁷⁶⁷ <http://xforce.iss.net/xforce/xfdb/15886>³⁷⁶⁸ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>³⁷⁶⁹ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>³⁷⁷¹ <http://www.securityfocus.com/bid/4314>³⁷⁷² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>³⁷⁷³ <http://xforce.iss.net/xforce/xfdb/8588>³⁷⁷⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419>³⁷⁷⁵ <http://rhn.redhat.com/errata/RHSA-2011-0507.html>³⁷⁷⁶ <http://secunia.com/advisories/44490/>³⁷⁷⁷ <http://secunia.com/advisories/44564/>³⁷⁷⁸ <http://secunia.com/advisories/44574/>³⁷⁷⁹ http://httpd.apache.org/security/vulnerabilities_22.html³⁷⁸⁰ <http://www.securityfocus.com/bid/6939>³⁷⁸¹ <http://www.securityfocus.com/bid/6943>³⁷⁸² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-1418>³⁷⁸³ <http://xforce.iss.net/xforce/xfdb/11438>

		Određene verzije Apache-a koriste zahtevani broj čvorova fajla da bi konstruisali 'Etag' heder za odgovor. Iako sama po sebi nije ranjivost, ova informacija olakšava sprovođenje određenih NFS napada. „Running vulnerable HTTP service: Apache 2.2.16. <a 684d7-b1-4a74aec9d6880\""="" href="http://172.23.202.197/1: \">http://172.23.202.197/1: \"684d7-b1-4a74aec9d6880\"”			konfiguraciju: <i>FileETag Mtime Size</i>
18.	Self-signed TLS/SSL certificate (ssl-self-signed-certificate)	172.23.202. 197:993 TLS/SSL-a sertifikat servera je samopotpisan. Samopotpisani sertifikati po difoltu nisu od poverenja, naročito zato što napadi na TLS/SSL preko posrednika obično koriste samopotpisane sertifikate da prisluškuju TLS/SSL veze.		Ozbiljan	Nabaviti novi TLS/SSL serverov sertifikat koji NIJE samopotpisan i instalirati ga na server. Precizna uputstva za dobijanje novog sertifikata zavise od zahteva organizacije. Uopšteno, treba napraviti zahtev za sertifikat i taj zahtev sačuvati kao fajl. Ovaj fajl se zatim šalje Certificate Authority-ju (CA) na obradu. Organizacija možda poseduje sopstveni interni Certificate Authority. U suprotnom, potrebno je platiti sertifikat iz spoljnog poverljivog Certificate Authority-ja, kao što su Thawte, Verisign.
19.	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server. Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko poziva udaljenih procedura (RPC). Ovi servisi su i u prošlosti bili skloni ranjivostima.. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinjenije napade. Primer: Found user(s): nobody root vanja Found server name: UBUNT1104DSKX64 Found local group(s): Found policy for domain(s): UBUNT1104DSKX64 Builtin	BID: 494³⁷⁸⁴ CVE: CVE-1999-0519³⁷⁸⁵ MSKB: 143474³⁷⁸⁶ URL1³⁷⁸⁷	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost
20.	Apache default installation/welcome page installed (http-apache-default-install-page)	172.23.202.197:80 Apache difoltna instalacija ili „Welcome“ stranica je instalirana na serveru. To obično ukazuje na novoinstalirani server. U mnogim slučajevima, Apache se	OSVDB 2117 ³⁷⁸⁸	Umeren	Ako se od servera zahteva da obezbedi neophodnu funkcionalnost, onda difoltnu stranicu treba zameniti odgovarajućim sadržajem. U suprotnom,

³⁷⁸⁴ <http://www.securityfocus.com/bid/494>³⁷⁸⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>³⁷⁸⁶ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>³⁷⁸⁷ http://www.hsc.fr/ressources/presentations/null_sessions/³⁷⁸⁸ http://www.osvdb.org/displayvuln.php?osvdb_id=2117 pristupljeno 11.12.2011

		instalira zajedno sa drugim aplikacijama i korisnik možda nije svestan da je web server pokrenut. Ovakvi serveri se retko patch-uju i još ređe nadgledaju, što zlonamernim napadačima postaje pogodna meta koja najverovatnije neće pokrenuti nikakvo upozorenje. Primer: Running vulnerable HTTP service: Apache 2.2.16. http://172.23.202.197/ 1: <code><html><body><h1>It works!</h1></code>			ovakav server treba ukloniti sa mreže, prateći bezbednosni princip minimalne složenosti (više složenosti = manja bezbednost). Ako server nije potreban, treba ga ukloniti iz svih startup fajlova (npr. <code>/etc/rc*</code>) ili skripti, a zatim prekinuti servis. Proveriti da li se on ponovo pokreće kada se mašina reboot-uje. Apache se uglavnom instalira kao <code>/usr/sbin/httpd</code> na UNIX mašinama ili kao <code>C:\Program Files\Apache Group</code> na Windows mašinama. Razmotriti uklanjanje binara i svih srodnih biblioteka iz sistema.
21.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	CVE CVE-1999-0524³⁷⁸⁹ OSVDB 95³⁷⁹⁰ XF icmp-netmask(306)³⁷⁹¹ XF icmp-timestamp(322)³⁷⁹²	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost
22.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1³⁷⁹³ URL2³⁷⁹⁴ URL3³⁷⁹⁵	Umeren	Onemogućiti TCP vremenske pečate na Linux-u. Podesiti vrednost <code>net.ipv4.tcp_timestamps</code> na 0 pokretanjem sledeće komande: <code>sysctl -w net.ipv4.tcp_timestamps=0</code> Uz to, sledeću vrednost staviti u difoltni <code>sysctl</code> konfiguracioni fajl, uopšteno <code>sysctl.conf</code>: <code>net.ipv4.tcp_timestamps=0</code>
23.	Database Open Access (database-open-access)	172.23.202.197:3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju.	URL1³⁷⁹⁶	Umeren	Konfigurisati server baze podataka tako da dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.

³⁷⁸⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>

³⁷⁹⁰ <http://www.osvdb.org/95>

³⁷⁹¹ <http://xforce.iss.net/xforce/xfdb/306>

³⁷⁹² <http://xforce.iss.net/xforce/xfdb/322>

³⁷⁹³ http://www.forensicswiki.org/wiki/TCP_timestamps

³⁷⁹⁴ <http://www.ietf.org/rfc/rfc1323.txt>

³⁷⁹⁵ <http://uptime.netcraft.com/>

³⁷⁹⁶ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf

		Iz ovog razloga, posedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7.			

Tabela 97. Linux OS – Pronađeni servisi na IP adresi 172.23.202.197 (2011. godina)

SERVISI	SAMBA 172.23.202.197 tcp 139 Samba 3.5.6 172.23.202.197 tcp 445 Samba 3.5.6 CIFS Name Service 172.23.202.197 udp 137 FTP 172.23.202.197 tcp 21 vsFTPD 2.3.2 ftp.banner: 220 (vsFTPD 2.3.2) HTTP 172.23.202.197 tcp 80 3 Apache 2.2.16 http.banner: Apache/2.2.16 (Debian) http.banner.server: Apache/2.2.16 (Debian) IMAP 172.23.202.197 tcp 143 imap.banner: * OK [CAPABILITY IMAP4REV1 I18NLEVEL=1 LITERAL+ SASL-IR LOGIN-REFERRALS STARTTLS LOGINDISABLED] IMAP4rev1 2007e.404 at Sat, 20 Aug 2011 07:32:44 -0400 (EDT) IMAPS³⁷⁹⁷ 172.23.202.197 tcp 993 imap.banner: * OK [CAPABILITY IMAP4REV1 I18NLEVEL=1 LITERAL+ SASL-IR LOGIN-REFERRALS AUTH=PLAIN AUTH=LOGIN] IMAP4rev1 2007e.404 at Sat, 20 Aug 2011 07:32:49 -0400 (EDT) POP 172.23.202.197 tcp 110 0 Qualcomm Qpopper 4.0.9 pop.banner: +OK Qpopper (version 4.0.9) MySQL 172.23.202.197 tcp 3306 SSH 172.23.202.197 tcp 22 0 OpenSSH 5.5p1 ssh.banner: SSH-2.0-OpenSSH_5.5p1 Debian-6 ssh.protocol.version: 2.0 PORTMAPPER 172.23.202.197 tcp 111 program-number: 100000 program-version: 2 172.23.202.197 udp 111 program-number: 100000 program-version: 2 STATUS 172.23.202.197 udp 33361 0 program-number: 100024 program-version: 1 172.23.202.197 tcp 59752 0 program-number: 100024

³⁷⁹⁷ Internet Message Access Protocol (IMAPS) preko TLS/SSL-a se koristi za pristupanje i obradu elektronske pošte (e-mail) korišćenjem dešifrovanih (TLS/SSL) konekcija. Kada se uspostavi TLS/SSL konekcija, koristi se standardni IMAP protokol. IMAP serveri mogu sadržavati nekoliko foldera, aka mailbox-ova, koji sadrže poruke (e-mails) za korisnike.

Spidered Web site	program-version: 1 http://172.23.202.197:80 Common Default URLs: <i>Access Error (403)</i> cgi-bin doc Guessed URLs <i>Access Error (403)</i> cgi-bin ?P=+ADw-script+AD4-alert(42)+Adw-script+AD4- doc %3f.jsp .svn Entries ADw-script AD4-alert(42) ADwscript AD4- CVS Entries Root DEADJOE Trace.axd WS_FTP.LOG Web.sitemap adojavas.inc adovbs.inc web.config <i>Redirect (301)</i> icons small <i>Successful (200)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-script+AD4- icons small index.html Linked URLs <i>Successful (200)</i> icons README README.html Small manual de bind.html caching.html configuring.html content-negotiation.html custom-error.html developer API.html debugging.html documenting.html filters.html hooks.html index.html

Tabela 98. Linux OS sa IP adresama 172.23.202.199, 172.23.202.224 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.199		OS: Scilinux 60 x64, scilinux60x64			19
IP adresa: 172.23.202.224		OS: Scilinux 60 x86, scilinux60x86			19
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Apache httpd expat DoS (CVE-2009-3560) (apache-httpd-2_2_x-cve-2009-3560)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepoverljivi XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	BID 37203 ³⁷⁹⁸ CVE CVE-2009-3560 ³⁷⁹⁹ DEBIAN DSA-1953 ³⁸⁰⁰ OVAL OVAL10613 ³⁸⁰¹ OVAL OVAL6883 ³⁸⁰² SECUNIA 37537 ³⁸⁰³ SECUNIA 38231 ³⁸⁰⁴ SECUNIA 38794 ³⁸⁰⁵ SECUNIA 38832 ³⁸⁰⁶ SECUNIA 38834 ³⁸⁰⁷ SECUNIA 39478 ³⁸⁰⁸ SECUNIA 41701 ³⁸⁰⁹ SECUNIA 43300 ³⁸¹⁰ URL1 ³⁸¹¹	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
2.	Apache httpd expat DoS (CVE-2009-3720) (apache-httpd-2_2_x-cve-2009-3720)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument.	CVE CVE-2009-3720 ³⁸¹² OVAL OVAL11019 ³⁸¹³ OVAL OVAL7112 ³⁸¹⁴ REDHAT RHSA-2010:0002 ³⁸¹⁵ SECUNIA 37324 ³⁸¹⁶ SECUNIA 37537 ³⁸¹⁷ SECUNIA 37925 ³⁸¹⁸ SECUNIA 38050 ³⁸¹⁹ SECUNIA 38231 ³⁸²⁰	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz

³⁷⁹⁸ <http://www.securityfocus.com/bid/37203>³⁷⁹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3560>³⁸⁰⁰ <http://www.debian.org/security/2009/dsa-1953>³⁸⁰¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10613>³⁸⁰² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6883>³⁸⁰³ <http://secunia.com/advisories/37537/>³⁸⁰⁴ <http://secunia.com/advisories/38231/>³⁸⁰⁵ <http://secunia.com/advisories/38794/>³⁸⁰⁶ <http://secunia.com/advisories/38832/>³⁸⁰⁷ <http://secunia.com/advisories/38834/>³⁸⁰⁸ <http://secunia.com/advisories/39478/>³⁸⁰⁹ <http://secunia.com/advisories/41701/>³⁸¹⁰ <http://secunia.com/advisories/43300/>³⁸¹¹ http://httpd.apache.org/security/vulnerabilities_22.html³⁸¹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3720>³⁸¹³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11019>³⁸¹⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7112>³⁸¹⁵ <http://rhn.redhat.com/errata/RHSA-2010-0002.html>³⁸¹⁶ <http://secunia.com/advisories/37324/>³⁸¹⁷ <http://secunia.com/advisories/37537/>³⁸¹⁸ <http://secunia.com/advisories/37925/>³⁸¹⁹ <http://secunia.com/advisories/38050/>³⁸²⁰ <http://secunia.com/advisories/38231/>

		Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepoverljivi XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	SECUNIA 38794 ³⁸²¹ SECUNIA 38832 ³⁸²² SECUNIA 38834 ³⁸²³ SECUNIA 39478 ³⁸²⁴ SECUNIA 41701 ³⁸²⁵ SECUNIA 43300 ³⁸²⁶ URL1 ³⁸²⁷		
3.	Apache httpd apr_bridage_split_line DoS (CVE-2010-1623) (apache-httpd-2_2_x-cve-2010-1623)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Skenirani servis je osjetljiv na ovu ranjivost SAMO ako Apache procesira ne-SSL zahteve. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_brigade_split_line() u sklopu APR-util library, koji se koristi za procesiranje ne-SSL zahteva. Zlonamerni napadač bi mogao da šalje zahteve, pažljivo izrađujući tajming za pojedinačne bajtove, što bi polako zauzimalo memoriju i potencijalno dovelo do odbijanja servisa.	BID 43673 ³⁸²⁸ CVE CVE-2010-1623 ³⁸²⁹ REDHAT RHSA-2010:0950 ³⁸³⁰ SECUNIA 41701 ³⁸³¹ SECUNIA 42015 ³⁸³² SECUNIA 42361 ³⁸³³ SECUNIA 42367 ³⁸³⁴ SECUNIA 42403 ³⁸³⁵ SECUNIA 42537 ³⁸³⁶ SECUNIA 43211 ³⁸³⁷ SECUNIA 43285 ³⁸³⁸ URL1 ³⁸³⁹	Ozbiljan	Apache >= 2.2 and < 2.3 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
4.	Apache httpd Timeout detection flaw (mod_proxy_http) (CVE-2010-2068) (apache-httpd-2_2_x-timeoutdetection-flaw-mod_proxy_http-cve-2010-2068)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Propust sa kojim je omogućeno otkrivanje informacija je otkriven u modulu mod_proxy_http na verzijama 2.2.9 do 2.2.15, 2.3.4-alpha i 2.3.5-alpha. Pod određenim tajmaut	APPLE APPLE-SA-2011-03-21 ³⁸⁴⁰ BID 40827 ³⁸⁴¹ CVE CVE-2010-2068 ³⁸⁴² OVAL OVAL11491 ³⁸⁴³ OVAL OVAL6931 ³⁸⁴⁴ SECUNIA 40206 ³⁸⁴⁵ SECUNIA 41480 ³⁸⁴⁶ SECUNIA 41490 ³⁸⁴⁷ SECUNIA 41722 ³⁸⁴⁸	Ozbiljan	Mnoge platforme i mnogi distributeri daju unapred formirane binarne pakete za Apache. Ovi unapred formirani paketi su najčešće standardizovani i optimizirani za određenu distribuciju, pa se zato savetuje korišćenje paketa predefinisanih za određeni

³⁸²¹ <http://secunia.com/advisories/38794/>³⁸²² <http://secunia.com/advisories/38832/>³⁸²³ <http://secunia.com/advisories/38834/>³⁸²⁴ <http://secunia.com/advisories/39478/>³⁸²⁵ <http://secunia.com/advisories/41701/>³⁸²⁶ <http://secunia.com/advisories/43300/>³⁸²⁷ http://httpd.apache.org/security/vulnerabilities_22.html³⁸²⁸ <http://www.securityfocus.com/bid/43673>³⁸²⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1623>³⁸³⁰ <http://rhn.redhat.com/errata/RHSA-2010-0950.html>³⁸³¹ <http://secunia.com/advisories/41701/>³⁸³² <http://secunia.com/advisories/42015/>³⁸³³ <http://secunia.com/advisories/42361/>³⁸³⁴ <http://secunia.com/advisories/42367/>³⁸³⁵ <http://secunia.com/advisories/42403/>³⁸³⁶ <http://secunia.com/advisories/42537/>³⁸³⁷ <http://secunia.com/advisories/43211/>³⁸³⁸ <http://secunia.com/advisories/43285/>³⁸³⁹ http://httpd.apache.org/security/vulnerabilities_22.html³⁸⁴⁰ <http://lists.apple.com/archives/security-announce/2011/Mar/msg00006.html>³⁸⁴¹ <http://www.securityfocus.com/bid/40827>³⁸⁴² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2068>³⁸⁴³ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:11491>³⁸⁴⁴ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:6931>³⁸⁴⁵ <http://secunia.com/advisories/40206/>³⁸⁴⁶ <http://secunia.com/advisories/41480/>³⁸⁴⁷ <http://secunia.com/advisories/41490/>³⁸⁴⁸ <http://secunia.com/advisories/41722/>

		uslovima, server bi mogao da uzvрати odgovorom koji je namenjen drugom korisniku. Ugrožene su one konfiguracije koje pokreću korišćenje proxy worker pool-ova. Na ranijim verzijama nije bilo ranjivosti, jer proxy pool-ovi još nisu bili uvedeni. Zahvaljujući Loren Anderson-u ovaj problem je prijavljen, a najjednostavniji način njegovog izbegavanja jeste opšte konfigurisanje.	XF modproxyhttp-timeout-info-disc(59413) ³⁸⁴⁹ URL1 ³⁸⁵⁰		OS, ukoliko su dostupni. Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.16.tar.gz
5.	X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch)	172.23.202.199:443 172.23.202.224:443 Rubrika u sertifikatu X.509 sa uobičajenim nazivom subjekta (CN) ne poklapa se sa imenom pojedinca koje je navedeno u sertifikatu. Pre izdavanja sertifikata, Certification Authority (CA) mora da proveri identitet pojedinca koji potražuje sertifikat, kako je navedeno u CA-ovom Certification Practice Statement (CPS). Zbog toga, uobičajene procedure validacije sertifikata zahtevaju da rubrika sertifikata sa CN subjektom odgovara pravom imenu pojedinca koji prikazuje sertifikat. Na primer, u sertifikatu prikazanom na „https://www.example.com/“, naziv subjekta (CN) treba da bude „www.example.com“. U cilju otkrivanja i sprečavanja napada prisluškivanja, validnost sertifikata mora da bude overena, jer bi u suprotnom napadač mogao da otpočne napad preko posrednika i da stekne potpunu kontrolu nad protokom podataka. Od posebne važnosti je validnost naziva subjekta (CN), koji treba da se poklapa sa imenom pojedinca (imenom host-a). Neodgovarajući CN se najčešće javlja usled greške u konfiguraciji, iako on takođe može da ukazuje na to da se sprovodi napad preko posrednika.		Ozbiljan	Rubrika sa uobičajenim nazivom subjekta (CN) u sertifikatu X.509 treba da bude podešena da sadrži ime pojedinca koji prikazuje sertifikat (npr. ime hosta). To se postiže izradom novog sertifikata, koji najčešće potpisuje Certification Authority (CA), koji je od poverenja kako za klijenta, tako i za server.
6.	FTP access with ftp account (ftp-generic-0001)	172.23.202.199:21 172.23.202.224:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisničkim ID-jem „ftp“ i šifrom „ftp“. Dosadašnja praksa je pokazala da treba ukloniti difoltnu naloge, ako je to moguće. Za naloge koje zahteva sistem, treba promeniti difoltnu šifru.	CVE CVE-1999-0497 ³⁸⁵¹	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko to nije kritično za dalje funkcionisanje sistema. U suprotnom, treba promeniti lozinku u nedifoltnu vrednost.
7.	FTP access with anonymous account (ftp-generic-0002)	172.23.202.199:21 172.23.202.224:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisničkim ID-jem „anonymous“ i šifrom „ftp@“. Dosadašnja praksa je pokazala da	CVE CVE-1999-0497 ³⁸⁵²	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko to nije kritično za dalje funkcionisanje sistema. U suprotnom, treba promeniti lozinku u nedifoltnu

³⁸⁴⁹ <http://xforce.iss.net/xforce/xfdb/59413>³⁸⁵⁰ http://httpd.apache.org/security/vulnerabilities_22.html³⁸⁵¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>³⁸⁵² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>

		treba ukloniti difoltne naloge, ako je to moguće. Za naloge koje zahteva sistem, treba promeniti difoltnu šifru.			vrednost.
8.	FTP server does not support AUTH command (ftp-generic-0007)	172.23.202.199:21 172.23.202.224:21 Klijenti na FTP server po difoltu šalju poverljive podatke (korisnički ID i šifru) u vidu čitkog teksta. Ova okolnost dozvoljava zlonamernim korisnicima omogućava da presreću poverljive podatke ukoliko prisluškuju vezu. Noviji FTP serveri podržavaju komandu AUTH, koja daje veće opcije autentifikacije, kao TLS, Kerberos, GSSAPI, itd. Njih treba koristiti da bi se sprečilo prisluškivanje na FTP vezama.		Ozbiljan	Nadograditi/Ažurirati na a FTP server koji podržava komandu AUTH.
9.	Browsable web directory (http-generic-browsable-dir)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Otkriven je direktorijum na web serveru koji može biti pretraživan, što znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice - spajdering (prateći hiperlinkove), ili -kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute force napadom na liste uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skrivena“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice.		Ozbiljan	Za Apache: onemogućiti brauzovanje direktorijuma mreže za sve direktorijume i poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim ako postoji potreba da ovi fajlovi budu dostupni preko web-a. Povremeno proći kroz web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume.
10.	TLS/SSL Server Supports Weak Cipher Algorithms (ssl-weak-ciphers)	172.23.202.199:443 172.23.202.224:443 negotiated the SSL_DHE_RSA_WITH_DES_CBC_SHA cipher suite TLS/SSL server podržava šifre koje se zasnivaju na slabim algoritmima. To napadaču može omogućiti da pokrene napade preko posrednika i da pregleda ili čačka osetljive podatke. Uopšteno, sledeće šifre se smatraju slabim: Tzv. „null“ (nula) šifre, jer ne šifruju podatke. Eksportne šifre koje koriste dužine tajnih ključeva ograničene na 40 bitova. Na to najčešće ukazuje reč EXP/EXPORT u nazivu šifre. Zastareli algoritmi za šifrovanje čije se dužine tajnih ključeva po današnjim standardima smatraju kratkim, npr. DES ili RC4 sa 56-bitnim ključevima.		Ozbiljan	Konfigurisati server tako da onemogući podršku za slabe šifre. Za Apache web servere sa mod_ssl, uključiti fajl Apache konfiguracije i izmeniti liniju SSLCipherSuite tako da u njoj piše: SSLCipherSuite ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM

11.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	TCP reset with incorrect sequence number triggered this fault on 172.23.202.199:21 172.23.202.224:21 Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183 ³⁸⁵³ CERT-VN: 415294 ³⁸⁵⁴ CVE CVE-2004-0230 ³⁸⁵⁵ MS: MS05-019 ³⁸⁵⁶ MS: MS06-064 ³⁸⁵⁷ NETBSD: NetBSD-SA2004-006 ³⁸⁵⁸ OVAL: OVAL2689 ³⁸⁵⁹ OVAL: OVAL270 ³⁸⁶⁰ OVAL OVAL3508 ³⁸⁶¹ OVAL OVAL4791 ³⁸⁶² OVAL OVAL5711 ³⁸⁶³ SECUNIA: 11440 ³⁸⁶⁴ SECUNIA 11458 ³⁸⁶⁵ SECUNIA: 22341 ³⁸⁶⁶ SGI 20040403-01-A ³⁸⁶⁷ XF tcp-rst-dos(15886) ³⁸⁶⁸ URL1 ³⁸⁶⁹ URL2 ³⁸⁷⁰	Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC 2385 ³⁸⁷¹ . Ono je napravljeno da smanji opasnost od određenih napada na BGP, kao što su TCP reseti.
12.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podesi na jedinstvenu vrednost i da se koristi u rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da fingerprint-uje operativni sistem.	BID 4314 ³⁸⁷² CVE CVE-2002-0510 ³⁸⁷³ XF linux-udp-fingerprint(8588) ³⁸⁷⁴	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili pak ranjivost koju treba popravljati, tako da ne postoje rešenja koja se mogu kupiti. Jedino se može postaviti fajervol ili neka druga sprava za filtriranje između napadnutog i neprijateljskog napada koji je u mogućnosti da randomizuje IP ID-jeve.
13.	Apache httpd apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpd-cve-2011-0419)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_autoindex. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji	CVE CVE-2011-0419 ³⁸⁷⁵ REDHAT RHSA-2011-0507 ³⁸⁷⁶ SECUNIA 44490 ³⁸⁷⁷ SECUNIA 44564 ³⁸⁷⁸ SECUNIA 44574 ³⁸⁷⁹ URL1 ³⁸⁸⁰	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.18.tar.gz

³⁸⁵³ <http://www.securityfocus.com/bid/10183>³⁸⁵⁴ <http://www.kb.cert.org/vuls/id/415294>³⁸⁵⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>³⁸⁵⁶ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>³⁸⁵⁷ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>³⁸⁵⁸ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>³⁸⁵⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>³⁸⁶⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>³⁸⁶¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>³⁸⁶² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>³⁸⁶³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>³⁸⁶⁴ <http://secunia.com/advisories/11440/>³⁸⁶⁵ <http://secunia.com/advisories/11458/>³⁸⁶⁶ <http://secunia.com/advisories/22341/>³⁸⁶⁷ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>³⁸⁶⁸ <http://xforce.iss.net/xforce/xfdb/15886>³⁸⁶⁹ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>³⁸⁷⁰ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>³⁸⁷¹ <http://www.ietf.org/rfc/rfc2385.txt>³⁸⁷² <http://www.securityfocus.com/bid/4314>³⁸⁷³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>³⁸⁷⁴ <http://xforce.iss.net/xforce/xfdb/8588>³⁸⁷⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419>³⁸⁷⁶ <http://rhn.redhat.com/errata/RHSA-2011-0507.html>³⁸⁷⁷ <http://secunia.com/advisories/44490/>³⁸⁷⁸ <http://secunia.com/advisories/44564/>³⁸⁷⁹ <http://secunia.com/advisories/44574/>³⁸⁸⁰ http://httpd.apache.org/security/vulnerabilities_22.html

		apr_fnmatch() u sklopu APR biblioteke. Ako je omogućen mod_autoindex, a indeksi direktorijuma mod_autoindex su sadržavali fajlove sa dovoljno dugim nazivima, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do preterane upotrebe CPU-a. Ovo bi moglo da bude iskorišćeno u napadu odbijanja servisa. Zahvaljujući Maksymilian Arciemowicz prijavljen je ovaj propust.			
14.	Self-signed TLS/SSL certificate (ssl-self-signed-certificate)	172.23.202.199:443 172.23.202.224:443 TLS/SSL-a sertifikat servera je samopotpisan. Samopotpisani sertifikati po defaultu nisu od poverenja, naročito zato što napadi na TLS/SSL preko posrednika obično koriste samopotpisane sertifikate da prisluškuju TLS/SSL veze.		Ozbiljan	Nabaviti novi TLS/SSL serverov sertifikat koji NIJE samopotpisan i instalirati ga na server. Precizna uputstva za dobijanje novog sertifikata zavise od zahteva organizacije. Uopšteno, treba napraviti zahtev za sertifikat i taj zahtev sačuvati kao fajl. Ovaj fajl se zatim šalje Certificate Authority-ju (CA) na obradu. Organizacija možda poseduje sopstveni interni Certificate Authority. U suprotnom, potrebno je platiti sertifikat iz spoljnog poverljivog Certificate Authority-ja, kao što su Thawte, Verisign.
15.	HTTP TRACE Method Enabled (http-trace-method-enabled)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 HTTP TRACE metoda se obično koristi da uzvрати potpuni HTTP zahtev klijentu koji ga zahteva, u cilju debagovanja proxy servera. Napadač bi mogao da kreira web stranicu koristeći XMLHTTP, ActiveX ili XMLDOM da natera klijenta da pošalje TRACE zahtev i da sačuva klijenove kolačiće. Kao posledica može da se javi XSS napad. Primer: Running vulnerable HTTP service. http://172.23.202.199/ 1: TRACE / HTTP/1.1 2: Host: 172.23.202.199 3: Cookie: vulnerable=yes	CVE CVE-2004-2320 ³⁸⁸¹ CVE CVE-2004-2763 ³⁸⁸² CVE CVE-2005-3398 ³⁸⁸³ CVE CVE-2006-4683 ³⁸⁸⁴ CVE CVE-2007-3008 ³⁸⁸⁵ CVE CVE-2008-7253 ³⁸⁸⁶ CVE CVE-2009-2823 ³⁸⁸⁷ CVE CVE-2010-0386 ³⁸⁸⁸ OSVDB 877 ³⁸⁸⁹ SUN 50603 ³⁸⁹⁰ BID 9561 ³⁸⁹¹ URL1 ³⁸⁹² URL2 ³⁸⁹³	Ozbiljan	Apache Onemogućiti HTTP TRACE metodu za Apache. Novije verzije Apache-a (1.3.34 i 2.0.55 i novije) omogućuju konfiguracionu direktivu koja se zove TraceEnable. Da bi se odbili TRACE zahtevi, dodaje se sledeći red u konfiguraciju servera: TraceEnable off Za starije verzije Apache web servera, koristiti modul mod_rewrite da bi se odbili TRACE zahteve: RewriteEngine On RewriteCond %{REQUEST_METHOD} ^TRACE RewriteRule .* - [F]

³⁸⁸¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2320>³⁸⁸² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2763>³⁸⁸³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-3398>³⁸⁸⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-4683>³⁸⁸⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3008>³⁸⁸⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-7253>³⁸⁸⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2823>³⁸⁸⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0386>³⁸⁸⁹ <http://osvdb.org/887>³⁸⁹⁰ <https://sunsolve.sun.com/search/document.do?assetkey=1-22-50603-1> pristupljeno 18.12.2011³⁸⁹¹ <http://www.securityfocus.com/bid/9561>³⁸⁹² <http://www.apacheweek.com/issues/03-01-24#news>³⁸⁹³ <http://www.kb.cert.org/vuls/id/867593>

16.	Database Open Access (database-open-access)	172.23.202.199:3306 172.23.202.224:3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7.	URL1 ³⁸⁹⁴	Umeren	Konfigurisati server baze podataka tako da dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.
17.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatišu slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	CVE CVE-1999-0524 ³⁸⁹⁵ OSVDB 95 ³⁸⁹⁶ XF netmask(306) ³⁸⁹⁷ icmp- XF timestamp(322) ³⁸⁹⁸ icmp-	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
18.	WebDAV Extensions are Enabled (http-generic-webdav-enabled)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 WebDAV je skup ekstenzija za HTTP protokol koji omogućava korisnicima da zajednički edituju i obrađuju fajlove na udaljenim web serverima. Mnogi web serveri po defaultu omogućavaju WebDAV ekstenzije, čak i kada nisu potrebne. S obzirom na dodatnu složenost, dosadašnja praksa je pokazala da treba onemogućiti WebDAV ukoliko se trenutno ne koristi.		Umeren	Apache: Potrebno je onemogućiti WebDAV (eng. Web-based Distributed Authoring and Versioning) za Apache. Proveriti da li je mod_dav modul isključen ili utvrditi da li postoji zahtevana autentifikacija na direktorijumima nad kojima se zahteva DAV.
19.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1 ³⁸⁹⁹ URL2 ³⁹⁰⁰ URL3 ³⁹⁰¹	Umeren	Onemogućiti TCP vremenske pečate na Linux-u. Podesiti vrednost net.ipv4.tcp_timestamps na 0 pokretanjem sledeće komande: sysctl -w net.ipv4.tcp_timestamps=0 Uz to, sledeću vrednost staviti u defaultni sysctl konfiguracioni fajl, uopšteno sysctl.conf:

³⁸⁹⁴ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf³⁸⁹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>³⁸⁹⁶ <http://www.osvdb.org/95>³⁸⁹⁷ <http://xforce.iss.net/xforce/xfdb/306>³⁸⁹⁸ <http://xforce.iss.net/xforce/xfdb/322>³⁸⁹⁹ http://www.forensicswiki.org/wiki/TCP_timestamps³⁹⁰⁰ <http://www.ietf.org/rfc/rfc1323.txt>³⁹⁰¹ <http://uptime.netcraft.com/>

					net.ipv4.tcp_timestamps=0

Tabela 99. Linux OS – Pronađeni servisi na IP adresi 172.23.202.199 (2011. godina)

SERVISI	FTP 172.23.202.199 tcp 21 vsFTPd 2.2.2 ftp.banner: 220 (vsFTPd 2.2.2) HTTP 172.23.202.199 tcp 80 Apache 2.2.15 WebDAV: http.banner: Apache/2.2.15 (Scientific Linux) http.banner.server: Apache/2.2.15 (Scientific Linux) 172.23.202.199 tcp 443 Apache 2.2.15 WebDAV: http.banner: Apache/2.2.15 (Scientific Linux) http.banner.server: Apache/2.2.15 (Scientific Linux) MySQL 172.23.202.199 tcp 3306 NTP 172.23.202.199 udp 123 SSH 172.23.202.199 tcp 22 0 OpenSSH 5.3 ssh.banner: SSH-2.0-OpenSSH_5.3 ssh.protocol.version: 2.0 Portmapper³⁹⁰² : 172.23.202.199 tcp 111 program-number: 100000 program-version: 2 172.23.202.199 udp 111 program-number: 100000 program-version: 2 STATUS: 172.23.202.199 udp 36250 program-number: 100024 program-version: 1 172.23.202.199 tcp 59180 program-number: 100024 program-version: 1
Spidered Web site	http://172.23.202.199:80 http://172.23.202.199:443 Common Default URLs: <i>Access Error (403)</i> cgi-bin error <i>Successful (200)</i> icons manual howto Guessed URLs <i>Access Error (403)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-

³⁹⁰² Port mapper poziva udaljene procedure je servis koji mapira RPC programe ka specifičnim portovima i daje tu informaciju klijentskim programima. S obzirom da većina RPC programa nema dobro definisan broj portova, njima se dinamički dodeljuje broj porta kada prvi put budu pokrenuti. Bilo koji klijentski program koji poželi da koristi određeni RPC program najpre stupa u kontakt sa port mapperom da bi odredio port i protokol specifikovanog RPC programa. Nakon toga, klijent koristi tu informaciju da direktno stupi u kontakt sa RPC programom. Neke implementacije port mapera dodatno omogućavaju prolazak komandi ka RPC programima kroz port mapper.

	script+AD4- script+AD4- cgi-bin error Redirect (301) icons small manual Successful (200) icons ?P=+ADw-script+AD4-alert(42)+Adw script+AD4- manual de developer index.html faq index.html index.html howto index.html index.html images index.html misc index.html mod index.html platform index.html programs index.html rewrite index.html ssl index.html style css vhosts index.html en images index.html Linked URLs Access Error (403) Successful (200) icons small manual bind.html caching.html configuring.html content-negotiation.html de bind.html caching.html configuring.html content-negotiation.html custom-error.html developer API.html debugging.html documenting.html filters.html hooks.html

	modules.html request.html thread_safety.html dns-caveats.html howto access.html auth.html cgi.html htaccess.html public_html.html ssi.html install.html invoking.html license.html logs.html misc password_encryptions.html perf-tuning.htm programs ab.html apachectl.html apxs.html configure.html dbmmanage.html htcacheclean.html htdbm.html htdigest.html htpasswd.html httpd.html httpd2dbm.html logresolve.html other.html rotatelogs.html suexec.html rewrite rewrite_flags.html rewrite_guide.html rewrite_guide_advanced.html rewrite_intro.html rewrite_tech.html sections.html server-wide.html sitemap.html ssl ssl_compat.html ssl_faq.html ssl_howto.html ssl_intro.html stopping.html

Tabela 100. Linux OS – Pronađeni servisi na IP adresi 172.23.202.224 (2011. godina)

SERVISI	FTP 172.23.202.224 tcp 21 vsFTPD 2.2.2 ftp.banner: 220 (vsFTPD 2.2.2) HTTP 172.23.202.224 tcp 80 Apache 2.2.15 WebDAV: http.banner: Apache/2.2.15 (Scientific Linux) http.banner.server: Apache/2.2.15 (Scientific Linux)

	172.23.202.224 tcp 443 Apache 2.2.15 WebDAV: http.banner: Apache/2.2.15 (Scientific Linux) http.banner.server: Apache/2.2.15 (Scientific Linux) MySQL 172.23.202.224 tcp 3306 NTP 172.23.202.224 udp 123 SSH 172.23.202.224 tcp 22 0 OpenSSH 5.3 ssh.banner: SSH-2.0-OpenSSH_5.3 ssh.protocol.version: 2.0 Portmapper³⁹⁰³ : 172.23.202.224 tcp 111 program-number: 100000 program-version: 2 172.23.202.224 udp 111 program-number: 100000 program-version: 2 STATUS: 172.23.202.224 udp 36250 program-number: 100024 program-version: 1 172.23.202.224 tcp 59180 program-number: 100024 program-version: 1
Spidered Web site	http://172.23.202.224:80 http://172.23.202.224:443 Common Default URLs: <i>Access Error (403)</i> cgi-bin error <i>Successful (200)</i> icons manual howto Guessed URLs <i>Access Error (403)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-script+AD4-cgi-bin error <i>Redirect (301)</i> icons small manual <i>Successful (200)</i> icons ?P=+ADw-script+AD4-alert(42)+Adwscript+AD4-manual de developer

³⁹⁰³ Port mapper pōziva udaljene procedure je servis koji mapira RPC programe ka specifičnim portovima i daje tu informaciju klijentskim programima. S obzirom da većina RPC programa nema dobro definisan broj portova, njima se dinamički dodeljuje broj porta kada prvi put budu pokrenuti. Bilo koji klijentski program koji poželi da koristi određeni RPC program najpre stupa u kontakt sa port mapperom da bi odredio port i protokol specifikovanog RPC programa. Nakon toga, klijent koristi tu informaciju da direktno stupi u kontakt sa RPC programom. Neke implementacije port mapera dodatno omogućavaju prolazak komandi ka RPC programima kroz port mapper.

	index.html faq index.html index.html howto index.html index.html images index.html misc index.html mod index.html platform index.html programs index.html rewrite index.html ssl index.html style css vhosts index.html en images index.html Linked URLs Access Error (403) Successful (200) icons small manual bind.html caching.html configuring.html content-negotiation.html de bind.html caching.html configuring.html content-negotiation.html custom-error.html developer API.html debugging.html documenting.html filters.html hooks.html modules.html request.html thread_safety.html dns-caveats.html howto access.html auth.html cgi.html htaccess.html public_html.html ssi.html install.html invoking.html license.html logs.html

	misc password_encryptions.html perf-tuning.htm programs ab.html apachectl.html apxs.html configure.html dbmmanage.html htcacheclean.html htdbm.html htdigest.html htpasswd.html httpd.html httpd2dbm.html logresolve.html other.html rotatelogs.html suexec.html rewrite rewrite_flags.html rewrite_guide.html rewrite_guide_advanced.html rewrite_intro.html rewrite_tech.html sections.html server-wide.html sitemap.html ssl ssl_compat.html ssl_faq.html ssl_howto.html ssl_intro.html stopping.html

Tabela 101. Linux OS sa IP adresama 172.23.202.198, 172.23.202.223 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.198		OS: Fedora 15 x86, fedora15x86			14
IP adresa: 172.23.202.223		OS: Fedora 15 x64, fedora15x64			14
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch)	172.23.202.198:443 172.23.202.223:443 Rubrika u sertifikatu X.509 sa uobičajenim nazivom subjekta (CN) ne poklapa se sa imenom pojedinca koje je navedeno u sertifikatu. Pre izdavanja sertifikata, Certification Authority (CA) mora da proveri identitet pojedinca koji potražuje sertifikat, kako je navedeno u CA-ovom Certification Practice Statement (CPS). Zbog toga, uobičajene procedure validacije sertifikata zahtevaju da rubrika sertifikata sa CN subjektom odgovara pravom imenu pojedinca koji prikazuje sertifikat. Na primer, u sertifikatu prikazanom na „https://www.example.com/“, naziv subjekta (CN) treba da bude		Ozbiljan	Rubrika sa uobičajenim nazivom subjekta (CN) u sertifikatu X.509 treba da bude podešena da sadrži ime pojedinca koji prikazuje sertifikat (npr. ime hosta). To se postiže izradom novog sertifikata, koji najčešće potpisuje Certification Authority (CA), koji je od poverenja kako za klijenta, tako i za server.

		„www.example.com“. U cilju otkrivanja i sprečavanja napada prisluškivanja, validnost sertifikata mora da bude overena, jer bi u suprotnom napadač mogao da otpočne napad preko posrednika i da stekne potpunu kontrolu nad protokom podataka. Od posebne važnosti je validnost naziva subjekta (CN), koji treba da se poklapa sa imenom pojedinca (imenom host-a). Neodgovarajući CN se najčešće javlja usled greške u konfiguraciji, iako on takođe može da ukazuje na to da se sprovodi napad preko posrednika.			
2.	FTP access with ftp account (ftp-generic-0001)	172.23.202.198:21 172.23.202.223:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisničkim ID-jem „ftp“ i šifrom „ftp“. Dosadašnja praksa je pokazala da treba ukloniti difoltnu naloge, ako je to moguće. Za naloge koje zahteva sistem, treba promeniti difoltnu šifru.	CVE CVE-1999-0497 ³⁹⁰⁴	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko to nije kritično za dalje funkcionisanje sistema. U suprotnom, treba promeniti lozinku u nedifoltnu vrednost.
3.	FTP access with anonymous account (ftp-generic-0002)	172.23.202.198:21 172.23.202.223:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisničkim ID-jem „anonymous“ i šifrom „ftp@“. Dosadašnja praksa je pokazala da treba ukloniti difoltnu naloge, ako je to moguće. Za naloge koje zahteva sistem, treba promeniti difoltnu šifru.	CVE CVE-1999-0497 ³⁹⁰⁵	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko to nije kritično za dalje funkcionisanje sistema. U suprotnom, treba promeniti lozinku u nedifoltnu vrednost.
4.	FTP server does not support AUTH command (ftp-generic-0007)	172.23.202.198:21 172.23.202.223:21 Klijenti na FTP server po difoltu šalju poverljive podatke (korisnički ID i šifru) u vidu čitkog teksta. Ova okolnost dozvoljava zlonamernim korisnicima omogućava da presreću poverljive podatke ukoliko prisluškuju vezu. Noviji FTP serveri podržavaju komandu AUTH, koja daje veće opcije autentifikacije, kao TLS, Kerberos, GSSAPI, itd. Njih treba koristiti da bi se sprečilo prisluškivanje na FTP vezama.		Ozbiljan	Nadograditi/Ažurirati na a FTP server koji podržava komandu AUTH.
5.	Browsable web directory (http-generic-browsable-dir)	172.23.202.198:80 172.23.202.223:80 172.23.202.198:443 172.23.202.223:443 Otkriven je direktorijum na web serveru koji može biti pretraživan, što znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice - spajdering (prateći hiperlinkove), ili -kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute force napadom na liste		Ozbiljan	Za Apache: onemogućiti brauzovanje direktorijuma mreže za sve direktorijume i poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove

³⁹⁰⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>³⁹⁰⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>

		uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skriven“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice. http://172.23.202.198/icons/ 4: <title>Index of /icons</title> 5: </head> 6: <body> 7: <h1>Index of /icons</h1> 8: ...CO]"></th><th>Name</th><th><a href="?C=M;O=A...			u web root, osim ako postoji potreba da ovi fajlovi budu dostupni preko web-a. Povremeno proći kroz web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastsareo, kao i nepoznate fajlove i direktorijume. Za Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote: Onemogućiti brauzovanje direktorijuma mreže za sve direktorijume i poddirektorijume. Uključiti Tomcat-ov web.xml file. U odeljku „default“, promeniti parametar „listings“ iz „true“ u „false“. Restartovati server. Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim ako ne postoji potreba da ovi fajlovi budu dostupni preko web-a. Povremeno proći kroz web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastsareo, kao i nepoznate fajlove i direktorijume.
6.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	TCP reset with incorrect sequence number triggered this fault on 172.23.202.198:80 172.23.202.223:80 Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183³⁹⁰⁶ CERT-VN: 415294³⁹⁰⁷ CVE CVE-2004-0230³⁹⁰⁸ MS: MS05-019³⁹⁰⁹ MS: MS06-064³⁹¹⁰ NETBSD: NetBSD-SA2004-006³⁹¹¹ OVAl: OVAL2689³⁹¹² OVAl: OVAL270³⁹¹³ OVAl OVAL3508³⁹¹⁴ OVAl OVAL4791³⁹¹⁵ OVAl OVAL5711³⁹¹⁶ SECUNIA: 11440³⁹¹⁷ SECUNIA 11458³⁹¹⁸ SECUNIA: 22341³⁹¹⁹	Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC 2385³⁹²⁴. Ono je napravljeno da smanji opasnost od određenih napada na BGP, kao što su TCP reseti.

³⁹⁰⁶ <http://www.securityfocus.com/bid/10183>

³⁹⁰⁷ <http://www.kb.cert.org/vuls/id/415294>

³⁹⁰⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>

³⁹⁰⁹ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>

³⁹¹⁰ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>

³⁹¹¹ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>

³⁹¹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>

³⁹¹³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>

³⁹¹⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>

³⁹¹⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>

³⁹¹⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>

³⁹¹⁷ <http://secunia.com/advisories/11440/>

³⁹¹⁸ <http://secunia.com/advisories/11458/>

³⁹¹⁹ <http://secunia.com/advisories/22341/>

			SGI 20040403-01-A ³⁹²⁰ XF tcp-rst-dos(15886) ³⁹²¹ URL1 ³⁹²² URL2 ³⁹²³		
7.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podese na jedinstvenu vrednost i da se koristi u rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da fingerprint-uje operativni sistem.	BID 4314 ³⁹²⁵ CVE CVE-2002-0510 ³⁹²⁶ XF linux-udp-fingerprint(8588) ³⁹²⁷	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili pak ranjivost koju treba popravljati, tako da ne postoje rešenja koja se mogu kupiti. Jedino se može postaviti fajervol ili neka druga sprava za filtriranje između napadnutog i neprijateljskog napada koji je u mogućnosti da randomizuje IP ID-jeve.
8.	Apache httpd apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpd-cve-2011-0419)	172.23.202.198:80 172.23.202.198:443 172.23.202.223:80 172.23.202.223:443 The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_autoindex. Review your web server configuration for validation. A flaw was found in the apr_fnmatch() function of the bundled APR library. Where mod_autoindex is enabled, and a directory indexed by mod_autoindex contained files with sufficiently long names, a remote attacker could send a carefully crafted request which would cause excessive CPU usage. This could be used in a denial of service attack. Acknowledgements: This issue was reported by Maksymilian Arciemowicz	CVE CVE-2011-0419 ³⁹²⁸ REDHAT RHSA-2011:0507 ³⁹²⁹ SECUNIA 44490 ³⁹³⁰ SECUNIA 44564 ³⁹³¹ SECUNIA 44574 ³⁹³² URL1 ³⁹³³	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.18.tar.gz
9.	Self-signed TLS/SSL certificate (ssl-self-signed-certificate)	172.23.202.198:443 172.23.202.223:443 TLS/SSL-a sertifikat servera je samopotpisan. Samopotpisani sertifikati po defaultu nisu od poverenja, naročito zato što napadi na TLS/SSL preko posrednika obično koriste samopotpisane sertifikate da prisluškuju TLS/SSL veze.		Ozbiljan	Nabaviti novi TLS/SSL serverov sertifikat koji NIJE samopotpisan i instalirati ga na server. Precizna uputstva za dobijanje novog sertifikata zavise od zahteva organizacije. Uopšteno, treba napraviti zahtev za sertifikat i taj zahtev sačuvati kao fajl. Ovaj fajl se zatim šalje Certificate Authority-ju (CA) na obradu. Organizacija možda poseduje sopstveni interni Certificate Authority. U suprotnom, potrebno je

³⁹²⁴ <http://www.ietf.org/rfc/rfc2385.txt>³⁹²⁰ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>³⁹²¹ <http://xforce.iss.net/xforce/xfdb/15886>³⁹²² <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>³⁹²³ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>³⁹²⁵ <http://www.securityfocus.com/bid/4314>³⁹²⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>³⁹²⁷ <http://xforce.iss.net/xforce/xfdb/8588>³⁹²⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419>³⁹²⁹ <http://rhn.redhat.com/errata/RHSA-2011-0507.html>³⁹³⁰ <http://secunia.com/advisories/44490/>³⁹³¹ <http://secunia.com/advisories/44564/>³⁹³² <http://secunia.com/advisories/44574/>³⁹³³ http://httpd.apache.org/security/vulnerabilities_22.html

					platiti sertifikat iz spolnog poverljivog Certificate Authority-ja, kao što su Thawte, Verisign.
10.	HTTP TRACE Method Enabled (http-trace-method-enabled)	172.23.202.198:80 172.23.202.223:80 172.23.202.198:443 172.23.202.223:443 HTTP TRACE metoda se obično koristi da uzvрати potpuni HTTP zahtev klijentu koji ga zahteva, u cilju debugovanja proxy servera. Napadač bi mogao da kreira web stranicu koristeći XMLHTTP, ActiveX ili XMLDOM da natera klijenta da pošalje TRACE zahtev i da sačuva klijenove kolačiće. Kao posledica može da se javi XSS napad. Primer : 172.23.202.198:443 Running vulnerable HTTPS service. https://172.23.202.198/ 1: TRACE / HTTP/1.1 2: Host: 172.23.202.198:443 3: Cookie: vulnerable=yes	CVE CVE-2004-2320³⁹³⁴ CVE CVE-2004-2763³⁹³⁵ CVE CVE-2005-3398³⁹³⁶ CVE CVE-2006-4683³⁹³⁷ CVE CVE-2007-3008³⁹³⁸ CVE CVE-2008-7253³⁹³⁹ CVE CVE-2009-2823³⁹⁴⁰ CVE CVE-2010-0386³⁹⁴¹ OSVDB 877³⁹⁴² SUN 50603³⁹⁴³ BID 9561³⁹⁴⁴ URL1³⁹⁴⁵ URL2³⁹⁴⁶	Ozbiljan	Apache Onemogućiti HTTP TRACE metodu za Apache. Novije verzije Apache-a (1.3.34 i 2.0.55 i novije) omogućuju konfiguracionu direktivu koja se zove TraceEnable. Da bi se odbili TRACE zahtevi, dodaje se sledeći red u konfiguraciju servera: TraceEnable off Za starije verzije Apache web servera, koristiti modul mod_rewrite da bi se odbili TRACE zahteve: RewriteEngine On RewriteCond %{REQUEST_METHOD} ^TRACE RewriteRule .* - [F]
11.	Database Open Access (database-open-access)	172.23.202.198:3306 172.23.202.223:3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posjedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7.	URL1 ³⁹⁴⁷	Umeren	Konfigurisati server baze podataka tako da dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.
12.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatišu slabe time-based generatore slučajnih	CVE CVE-1999-0524³⁹⁴⁸ OSVDB 95³⁹⁴⁹ XF icmp-netmask(306)³⁹⁵⁰ XF icmp-timestamp(322)³⁹⁵¹	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti

³⁹³⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2320>³⁹³⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2763>³⁹³⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-3398>³⁹³⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-4683>³⁹³⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3008>³⁹³⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-7253>³⁹⁴⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2823>³⁹⁴¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0386>³⁹⁴² <http://osvdb.org/877>³⁹⁴³ <https://sunsolve.sun.com/search/document.do?assetkey=1-22-50603-1> pristupljeno 18.12.2011³⁹⁴⁴ <http://www.securityfocus.com/bid/9561>³⁹⁴⁵ <http://www.apacheweek.com/issues/03-01-24#news>³⁹⁴⁶ <http://www.kb.cert.org/vuls/id/867593>³⁹⁴⁷ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf³⁹⁴⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>³⁹⁴⁹ <http://www.osvdb.org/95>³⁹⁵⁰ <http://xforce.iss.net/xforce/xfdb/306>³⁹⁵¹ <http://xforce.iss.net/xforce/xfdb/322>

		brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.			detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
13.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1³⁹⁵² URL2³⁹⁵³ URL3³⁹⁵⁴	Umeren	Onemogućiti TCP vremenske pečate na Linux-u. Podesiti vrednost <code>net.ipv4.tcp_timestamps</code> na 0 pokretanjem sledeće komande: <code>sysctl -w net.ipv4.tcp_timestamps=0</code> Uz to, sledeću vrednost staviti u difoltni <code>sysctl</code> konfiguracioni fajl, uopšteno <code>sysctl.conf</code> : <code>net.ipv4.tcp_timestamps=0</code>
14.	WebDAV Extensions are Enabled (http-generic-webdav-enabled)	172.23.202.198:80 172.23.202.223:80 172.23.202.198:443 172.23.202.223:443 WebDAV je skup ekstenzija za HTTP protokol koji omogućava korisnicima da zajednički edituju i obrađuju fajlove na udaljenim web serverima. Mnogi web serveri po difoltu omogućavaju WebDAV ekstenzije, čak i kada nisu potrebne. S obzirom na dodatnu složenost, dosadašnja praksa je pokazala da treba onemogućiti WebDAV ukoliko se trenutno ne koristi.		Umeren	Apache: Potrebno je onemogućiti WebDAV (eng. Web-based Distributed Authoring and Versioning) za Apache. Proveriti da li je <code>mod_dav</code> modul isključen ili utvrditi da li postoji zahtevana autentifikacija na direktorijumima nad kojima se zahteva DAV.

Tabela 102. Linux OS – Pronađeni servisi na IP adresi 172.23.202.198 (2011. godina)

SERVISI	
	FTP 172.23.202.198 tcp 21 vsFTPD 2.3.4 ftp.banner: 220 (vsFTPD 2.3.4)
	HTTP 172.23.202.198 tcp 80 Apache 2.2.17 WebDAV: http.banner: Apache/2.2.17 (Fedora) http.banner.server: Apache/2.2.17 (Fedora) 172.23.202.198 tcp 443 Apache 2.2.17 WebDAV: http.banner: Apache/2.2.17 (Fedora) http.banner.server: Apache/2.2.17 (Fedora)
	NTP 172.23.202.198 udp 123
	MySQL 172.23.202.198 tcp 3306
	SSH 172.23.202.198 tcp 22 OpenSSH 5.6 ssh.banner: SSH-2.0-OpenSSH_5.6 ssh.protocol.version: 2.0

³⁹⁵² http://www.forensicswiki.org/wiki/TCP_timestamps³⁹⁵³ <http://www.ietf.org/rfc/rfc1323.txt>³⁹⁵⁴ <http://uptime.netcraft.com/>

	Portmapper³⁹⁵⁵ : 172.23.202.198 tcp 111 program-number: 100000 program-version: 2 172.23.202.198 udp 111 program-number: 100000 program-version: 2 STATUS: 172.23.202.198 udp 40338 0 program-number: 100024 program-version: 1 172.23.202.198 tcp 43110 0 program-number: 100024 program-version: 1
Spidered Web site	http://172.23.202.198:80 http://172.23.202.198:443 Common Default URLs: <i>Access Error (403)</i> cgi-bin error <i>Successful (200)</i> icons manual howto Guessed URLs <i>Access Error (403)</i> ?P=+Adw-script+AD4-alert(42)+Adwscript+AD4- script+AD4- script+AD4- cgi-bin error <i>Redirect (301)</i> icons small manual <i>Successful (200)</i> icons ?P=+Adw-script+AD4-alert(42)+Adwscript+AD4- script+AD4- README small README manual de developer index.html index.html index.html faq index.html index.html howto index.html

³⁹⁵⁵ Port mapper poziva udaljene procedure je servis koji mapira RPC programe ka specifičnim portovima i daje tu informaciju klijentskim programima. S obzirom da većina RPC programa nema dobro definisan broj portova, njima se dinamički dodeljuje broj porta kada prvi put budu pokrenuti. Bilo koji klijentski program koji poželi da koristi određeni RPC program najpre stupa u kontakt sa port mapperom da bi odredio port i protokol specifikovanog RPC programa. Nakon toga, klijent koristi tu informaciju da direktno stupi u kontakt sa RPC programom. Neke implementacije port mapera dodatno omogućavaju prolazak komandi ka RPC programima kroz port mapper.

	index.html images index.html misc index.html mod index.html Linked URLs Access Error (403) Successful (200) icons small bind.html caching.html configuring.html content-negotiation.html de bind.html caching.html configuring.html content-negotiation.html custom-error.html developer API.html howto access.html auth.html cgi.html htaccess.html public_html.html ssi.html install.html invoking.html license.html logs.html misc password_encryptions.html perf-tuning.html relevant_standards.html rewriteguide.html security_tips.html

Tabela 103. Linux OS – Pronađeni servisi na IP adresi 172.23.202.223 (2011. godina)

SERVISI	FTP 172.23.202.223 tcp 21 vsFTPd 2.3.4 ftp.banner: 220 (vsFTPd 2.3.4) HTTP 172.23.202.223 tcp 80 Apache 2.2.17 WebDAV: http.banner: Apache/2.2.17 (Fedora) http.banner.server: Apache/2.2.17 (Fedora) 172.23.202.223 tcp 443 Apache 2.2.17 WebDAV: http.banner: Apache/2.2.17 (Fedora) http.banner.server: Apache/2.2.17 (Fedora) NTP 172.23.202.223 udp 123

	MySQL 172.23.202.223 tcp 3306 SSH 172.23.202.223 tcp 22 OpenSSH 5.6 ssh.banner: SSH-2.0-OpenSSH_5.6 ssh.protocol.version: 2.0 Portmapper³⁹⁵⁶ : 172.23.202.223 tcp 111 program-number: 100000 program-version: 2 172.23.202.223 udp 111 program-number: 100000 program-version: 2 STATUS: 172.23.202.223 udp 40338 0 program-number: 100024 program-version: 1 172.23.202.223 tcp 43110 0 program-number: 100024 program-version: 1
Spidered Web site	http://172.23.202.223:80 http://172.23.202.223:443 Common Default URLs: <i>Access Error (403)</i> cgi-bin error <i>Successful (200)</i> icons manual howto Guessed URLs <i>Access Error (403)</i> ?P=+Adw-script+AD4-alert(42)+Adwscript+AD4- script+AD4- script+AD4- cgi-bin error <i>Redirect (301)</i> icons small manual <i>Successful (200)</i> icons ?P=+Adw-script+AD4-alert(42)+Adwscript+AD4- script+AD4- README small README manual de developer

³⁹⁵⁶ Port mapper poziva udaljene procedure je servis koji mapira RPC programe ka specifičnim portovima i daje tu informaciju klijentskim programima. S obzirom da većina RPC programa nema dobro definisan broj portova, njima se dinamički dodeljuje broj porta kada prvi put budu pokrenuti. Bilo koji klijentski program koji poželi da koristi određeni RPC program najpre stupa u kontakt sa port mapperom da bi odredio port i protokol specifikovanog RPC programa. Nakon toga, klijent koristi tu informaciju da direktno stupi u kontakt sa RPC programom. Neke implementacije port mapera dodatno omogućavaju prolazak komandi ka RPC programima kroz port mapper.

	index.html index.html index.html faq index.html index.html howto index.html index.html images index.html misc index.html mod index.html Linked URLs Access Error (403) Successful (200) icons small bind.html caching.html configuring.html content-negotiation.html de bind.html caching.html configuring.html content-negotiation.html custom-error.html developer API.html howto access.html auth.html cgi.html htaccess.html public_html.html ssi.html install.html invoking.html license.html logs.html misc password_encryptions.html perf-tuning.html relevant_standards.html rewriteguide.html security_tips.html

Tabela 104. Linux OS sa IP adresama 172.23.202.131 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.131		OS: Slackware 13.37 x86, slackware1337			11
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Browsable web directory (http-generic-	172.23.202.131:80 Otkriven je direktorijum na web		Ozbiljan	Za Apache: onemogućiti brauzovanje direktorijuma

	browsable-dir)	serveru koji može biti pretraživan, što znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice -spajdering (prateći hiperlinkove), ili -kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute force napadom na liste uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skrivenne“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice.			mreže za sve direktorijume i poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim ako postoji potreba da ovi fajlovi budu dostupni preko web-a. Povremeno proći kroz web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume.
2.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	172.23.202.131:113: Kada se kod TCP paketa koristi Large Window Size, olakšava se spolnom napadaču da otkrije sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183 ³⁹⁵⁷ CERT-VN: 415294 ³⁹⁵⁸ CVE CVE-2004-0230 ³⁹⁵⁹ MS: MS05-019 ³⁹⁶⁰ MS: MS06-064 ³⁹⁶¹ NETBSD: NetBSD-SA2004-006 ³⁹⁶² OVAL: OVAL2689 ³⁹⁶³ OVAL: OVAL270 ³⁹⁶⁴ OVAL OVAL3508 ³⁹⁶⁵ OVAL OVAL4791 ³⁹⁶⁶ OVAL OVAL5711 ³⁹⁶⁷ SECUNIA: 11440 ³⁹⁶⁸ SECUNIA 11458 ³⁹⁶⁹ SECUNIA: 22341 ³⁹⁷⁰ SGI 20040403-01-A ³⁹⁷¹ XF tcp-rst-dos(15886) ³⁹⁷² URL1 ³⁹⁷³ URL2 ³⁹⁷⁴	Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC 2385 ³⁹⁷⁵ . Ono je napravljeno da smanji opasnost od određenih napada na BGP, kao što su TCP reseti.
3.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podesi na jedinstvenu vrednost i da se koristi u	BID 4314 ³⁹⁷⁶ CVE CVE-2002-0510 ³⁹⁷⁷ XF linux-udp-fingerprint(8588) ³⁹⁷⁸	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili pak ranjivost koju treba popravljati, tako da ne

³⁹⁵⁷ <http://www.securityfocus.com/bid/10183>³⁹⁵⁸ <http://www.kb.cert.org/vuls/id/415294>³⁹⁵⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>³⁹⁶⁰ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>³⁹⁶¹ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>³⁹⁶² <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>³⁹⁶³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>³⁹⁶⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>³⁹⁶⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>³⁹⁶⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>³⁹⁶⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>³⁹⁶⁸ <http://secunia.com/advisories/11440/>³⁹⁶⁹ <http://secunia.com/advisories/11458/>³⁹⁷⁰ <http://secunia.com/advisories/22341/>³⁹⁷¹ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>³⁹⁷² <http://xforce.iss.net/xforce/xfdb/15886>³⁹⁷³ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>³⁹⁷⁴ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>³⁹⁷⁵ <http://www.ietf.org/rfc/rfc2385.txt>³⁹⁷⁶ <http://www.securityfocus.com/bid/4314>³⁹⁷⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>

		rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da fingerprint-uje operativni sistem.			postoje rešenja koja se mogu kupiti. Jedino se može postaviti fajervol ili neka druga sprava za filtriranje između napadnutog i neprijateljskog napada koji je u mogućnosti da randomizuje IP ID-jeve.
4.	Apache httpd apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpd-cve-2011-0419)	172.23.202.131:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_autoindex. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_fnmatch() u sklopu APR biblioteke. Ako je omogućen mod_autoindex, a indeksi direktorijuma mod_autoindex su sadržavali fajlove sa dovoljno dugim nazivima, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do preterane upotrebe CPU-a. Ovo bi moglo da bude iskorišćeno u napadu odbijanja servisa. Zahvaljujući Maksymilian Arciemowicz prijavljen je ovaj propust.	CVE CVE-2011-0419 ³⁹⁷⁹ REDHAT RHSA-2011:0507 ³⁹⁸⁰ SECUNIA 44490 ³⁹⁸¹ SECUNIA 44564 ³⁹⁸² SECUNIA 44574 ³⁹⁸³ URL1 ³⁹⁸⁴	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.18.tar.gz
5.	Apache Etag Inode Information Leakage (http-apache-etag-inode-leak)	172.23.202.131:80 U određenim konfiguracijama, Apache HTTP server dozvoljava udaljenim napadačima da dobiju poverljive informacije preko (1) Etag heder-a, koji otkriva broj inoda ili (2) razdvajajuće višedelnih MIME-a, koja ukazuje na ID child procesa (PID). Određene verzije Apache-a koriste zahtevani broj čvorova fajla da bi konstruisali 'Etag' heder za odgovor. Iako sama po sebi nije ranjivost, ova informacija olakšava sprovođenje određenih NFS napada. „Running vulnerable HTTP service: Apache 2.2.17. http://172.23.202.131/1: "27231-2c-3e9564c23b600"“	BID 6939 ³⁹⁸⁵ BID 6943 ³⁹⁸⁶ CVE CVE-2003-1418 ³⁹⁸⁷ XF apache-mime-information-disclosure(11438) ³⁹⁸⁸	Ozbiljan	Onemogućiti Etag mehanizam tipa "inod-based" konfiguraciji Apache-a. Takođe, inod informacije je moguće ukloniti iz Etag heder-a tako što će se dodati direktiva u Apache konfiguraciju: <i>FileETag Mtime Size</i>
6.	Apache default installation/welcome page installed (http-apache-default-install-page)	172.23.202.131:80 Apache difoltna instalacija ili „Welcome“ stranica je instalirana na serveru. To obično ukazuje na novoinstalirani server. U mnogim slučajevima, Apache se instalira zajedno sa drugim aplikacijama i korisnik možda nije svestan da je web server pokrenut. Ovakvi serveri se retko patch-uju i još	OSVDB 2117 ³⁹⁸⁹	Umeren	Ako se od servera zahteva da obezbedi neophodnu funkcionalnost, onda difoltnu stranicu treba zameniti odgovarajućim sadržajem. U suprotnom, ovakav server treba ukloniti sa mreže, prateći bezbednosni princip minimalne složenosti (više

³⁹⁷⁸ <http://xforce.iss.net/xforce/xfdb/8588>³⁹⁷⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419>³⁹⁸⁰ <http://rhn.redhat.com/errata/RHSA-2011-0507.html>³⁹⁸¹ <http://secunia.com/advisories/44490/>³⁹⁸² <http://secunia.com/advisories/44564/>³⁹⁸³ <http://secunia.com/advisories/44574/>³⁹⁸⁴ http://httpd.apache.org/security/vulnerabilities_22.html³⁹⁸⁵ <http://www.securityfocus.com/bid/6939>³⁹⁸⁶ <http://www.securityfocus.com/bid/6943>³⁹⁸⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-1418>³⁹⁸⁸ <http://xforce.iss.net/xforce/xfdb/11438>³⁹⁸⁹ http://www.osvdb.org/displayvuln.php?osvdb_id=2117 pristupljeno 11.12.2011

		rede nadgledaju, što zlonamernim napadačima postaje pogodna meta koja najverovatnije neće pokrenuti nikakvo upozorenje. Primer: Running vulnerable HTTP service: Apache 2.2.17. http://172.23.202.131/ 1: <code><html><body><h1>It works!</h1></body></html></code>			složenosti = manja bezbednost). Ako server nije potreban, treba ga ukloniti iz svih startup fajlova (npr. /etc/rc*) ili skripti, a zatim prekinuti servis. Proveriti da li se on ponovo pokreće kada se mašina reboot-uje. Apache se uglavnom instalira kao /usr/sbin/httpd na UNIX mašinama ili kao C:\Program Files\Apache Group na Windows mašinama. Razmotriti uklanjanje binara i svih srodnih biblioteka iz sistema.
7.	HTTP TRACE Method Enabled (http-trace-method-enabled)	172.23.202.131:80 HTTP TRACE metoda se obično koristi da uzvрати potpuni HTTP zahtev klijentu koji ga zahteva, u cilju debagovanja proxy servera. Napadač bi mogao da kreira web stranicu koristeći XMLHTTP, ActiveX ili XMLHttpRequest da natera klijenta da pošalje TRACE zahtev i da sačuva klijenove kolačiće. Kao posledica može da se javi XSS napad. Primer : Running vulnerable HTTP service. http://172.23.202.131/ 1: TRACE / HTTP/1.1 2: Host: 172.23.202.209 3: Cookie: vulnerable=yes	CVE CVE-2004-2320³⁹⁹⁰ CVE CVE-2004-2763³⁹⁹¹ CVE CVE-2005-3398³⁹⁹² CVE CVE-2006-4683³⁹⁹³ CVE CVE-2007-3008³⁹⁹⁴ CVE CVE-2008-7253³⁹⁹⁵ CVE CVE-2009-2823³⁹⁹⁶ CVE CVE-2010-0386³⁹⁹⁷ OSVDB 877³⁹⁹⁸ SUN 50603³⁹⁹⁹ BID 9561⁴⁰⁰⁰ URL1⁴⁰⁰¹ URL2⁴⁰⁰²	Ozbiljan	Apache Onemogućiti HTTP TRACE metodu za Apache. Novije verzije Apache-a (1.3.34 i 2.0.55 i novije) omogućuju konfiguracionu direktivu koja se zove TraceEnable. Da bi se odbili TRACE zahtevi, dodaje se sledeći red u konfiguraciju servera: TraceEnable off Za starije verzije Apache web servera, koristiti modul mod_rewrite da bi se odbili TRACE zahteve: RewriteEngine On RewriteCond %{REQUEST_METHOD} ^TRACE RewriteRule .* - [F]
8.	Database Open Access (database-open-access)	172.23.202.131:3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim mehanizmima autorizacije, predstavlja povredu standarda PCI	URL1 ⁴⁰⁰³	Umeren	Konfigurisati server baze podataka tako da se dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.

³⁹⁹⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2320>

³⁹⁹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2763>

³⁹⁹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-3398>

³⁹⁹³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-4683>

³⁹⁹⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3008>

³⁹⁹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-7253>

³⁹⁹⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2823>

³⁹⁹⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0386>

³⁹⁹⁸ <http://osvdb.org/887>

³⁹⁹⁹ <https://sunsolve.sun.com/search/document.do?assetkey=1-22-50603-1> pristupljeno 18.12.2011

⁴⁰⁰⁰ <http://www.securityfocus.com/bid/9561>

⁴⁰⁰¹ <http://www.apacheweek.com/issues/03-01-24#news>

⁴⁰⁰² <http://www.kb.cert.org/vuls/id/867593>

⁴⁰⁰³ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf

		DSS sekcija 1.3.7.			
9.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	CVE CVE-1999-0524 ⁴⁰⁰⁴ OSVDB 95 ⁴⁰⁰⁵ XF netmask(306) ⁴⁰⁰⁶ icmp- XF timestamp(322) ⁴⁰⁰⁷ icmp-	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
10.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1 ⁴⁰⁰⁸ URL2 ⁴⁰⁰⁹ URL3 ⁴⁰¹⁰	Umeren	Onemogućiti TCP vremenske pečate na Linux-u. Podesiti vrednost net.ipv4.tcp_timestamps na 0 pokretanjem sledeće komande: sysctl -w net.ipv4.tcp_timestamps=0 Uz to, sledeću vrednost staviti u difoltni sysctl konfiguracioni fajl, uopšteno sysctl.conf: net.ipv4.tcp_timestamps=0
11.	WebDAV Extensions are Enabled (http-generic-webdav-enabled)	172.23.202.131:80 WebDAV je skup ekstenzija za HTTP protokol koji omogućava korisnicima da zajednički edituju i obrađuju fajlove na udaljenim web serverima. Mnogi web serveri po difoltu omogućavaju WebDAV ekstenzije, čak i kada nisu potrebne. S obzirom na dodatnu složenost, dosadašnja praksa je pokazala da treba onemogućiti WebDAV ukoliko se trenutno ne koristi.		Umeren	Apache: Potrebno je onemogućiti WebDAV (eng. Web-based Distributed Authoring and Versioning) za Apache. Proveriti da li je mod_dav modul isključen ili utvrditi da li postoji zahtevana autentifikacija na direktorijumima nad kojima se zahteva DAV.

Tabela 105. Linux OS – Pronađeni servisi na IP adresi 172.23.202.131 (2011. godina)

SERVISI	FTP 172.23.202.198 tcp 21 vsFTPD 2.3.4 ftp.banner: 220 (vsFTPD 2.3.4) HTTP 172.23.202.131 tcp 80 Apache 2.2.17 DAV: 2 WebDAV: http.banner: Apache/2.2.17 (Unix) DAV/2 http.banner.server: Apache/2.2.17 (Unix) DAV/2 NTP 172.23.202.131 udp 123

⁴⁰⁰⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁴⁰⁰⁵ <http://www.osvdb.org/95>⁴⁰⁰⁶ <http://xforce.iss.net/xforce/xfdb/306>⁴⁰⁰⁷ <http://xforce.iss.net/xforce/xfdb/322>⁴⁰⁰⁸ http://www.forensicswiki.org/wiki/TCP_timestamps⁴⁰⁰⁹ <http://www.ietf.org/rfc/rfc1323.txt>⁴⁰¹⁰ <http://uptime.netcraft.com/>

	SMTP 172.23.202.131 tcp 25 Sendmail 8.14.4 advertise-esmtp: 1 172.23.202.131 tcp 587 Sendmail 8.14.4 advertise-esmtp: 1 MySQL 172.23.202.131 tcp 3306 SSH 172.23.202.131 tcp 22 0 OpenSSH 5.8 ssh.banner: SSH-2.0-OpenSSH_5.8 ssh.protocol.version: 2.0 IDENT⁴⁰¹¹ 172.23.202.131 tcp 113 Timeserver⁴⁰¹² 172.23.202.131 tcp 37 server-time: 18750714T064149000 172.23.202.131 udp 37 server-time: 18750714T063949000
Spidered Web site	http://172.23.202.131:80 Common Default URLs: <i>Access Error (403)</i> cgi-bin <i>Error (500)</i> cgi-bin printenv test-cgi <i>Successful (200)</i> manual howto images misc mod programs vhosts Guessed URLs <i>Access Error (403)</i> cgi-bin ?P=+ADw-script+AD4-alert(42)+ADwscript+ AD4- <i>Error (400)</i> never found %0 cgi-bin \$1 docs docs cgi-bin docs sites %1 \$1

⁴⁰¹¹ Ident ili protokol identifikacije obezbeđuje servis kojim se određuje identitet vlasnika određene TCP veze. Da bi identifikovao vezu, klijent TCP portu šalje par brojeva (port na serveru, port klijentu) u formi čitkog teksta. Ako postoji veza između servera i klijenta, onda server povratno šalje korisničku identifikaciju koja zavisi od sistema, koja je zapravo string čiji format određuje operativni sistem na ident serveru. S obzirom da je ovo protokol čitkog teksta, a ident server zapravo može da snabdeva bilo koji identifikator po želji, ovaj protokol nije namenjen da bude autentifikacioni nit autorizatorski mehanizam. Njegova osnovna namena je da daje dodatnu revizorsku informaciju o određenim TCPO vezama.

⁴⁰¹² Ovaj servis daje standardan datum i vreme koji mašina može da čita. Pretraživanis ervis će prvatiti svoje trenutno vreme za nekoliko sekundi, počev od ponoći 1. januara 1900. Ovaj servis se može koristiti za ispravku ili overu vremena određenog hosta, a može se koristiti da sinhronizuje satove na celoj mreži.

	%2 %3 %4 cgi-bin docs docs usr local apache vhosts <i>Redirect (301)</i> manual manual images <i>Successful (200)</i> ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4- manual developer index.html faq index.html howto index.html images index.html misc index.html mod Linked URLs <i>Successful (200)</i> manual bind.html caching.html configuring.html content-negotiation.html custom-error.html developer API.html debugging.html documenting.html filters.html hooks.html modules.html request.html thread_safety.html mod beos.html core.html directive-dict.html directives.html event.html mod_actions.html mod_alias.html mod_asis.html mod_auth_basic.html mod_auth_digest.html mod_authn_alias.html mod_authn_anon.html vhosts details.html examples.html fd-limits.html

	ip-based.html mass.html name-based.html

Tabela 106. Linux OS sa IP adresama 172.23.202.125 (2011. godina)

Datum: 20.08.2011		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.125		OS: Opensuse 11.4 x86, opensuse1104x86			8
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Browsable web directory (http-generic-browsable-dir)	172.23.202.125:80 Otkriven je direktorijum na web serveru koji može biti pretraživan, što znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice - spajdering (prateći hiperlinkove), ili -kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute force napadom na liste uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skrivenne“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice.		Ozbiljan	Za Apache: onemogućiti pretraživanje direktorijuma mreže za sve direktorijume i poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume. Za Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote: Onemogućiti pretraživanje direktorijuma za sve direktorijume i poddirektorijume. Uključiti Tomcat-ov web.xml file. U odeljku „default“, promeniti parametar „listings“ iz „true“ u „false“. Restartovati server. Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skriptu i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i

					direktorijume.
2.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	TCP reset with incorrect sequence number triggered this fault on 172.23.202.125:80: Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hедера i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183 ⁴⁰¹³ CERT-VN: 415294 ⁴⁰¹⁴ CVE CVE-2004-0230 ⁴⁰¹⁵ MS: MS05-019 ⁴⁰¹⁶ MS: MS06-064 ⁴⁰¹⁷ NETBSD: NetBSD-SA2004-006 ⁴⁰¹⁸ OVAL: OVAL2689 ⁴⁰¹⁹ OVAL: OVAL270 ⁴⁰²⁰ OVAL OVAL3508 ⁴⁰²¹ OVAL OVAL4791 ⁴⁰²² OVAL OVAL5711 ⁴⁰²³ SECUNIA: 11440 ⁴⁰²⁴ SECUNIA 11458 ⁴⁰²⁵ SECUNIA: 22341 ⁴⁰²⁶ SGI 20040403-01-A ⁴⁰²⁷ XF tcp-rst-dos(15886) ⁴⁰²⁸ URL1 ⁴⁰²⁹ URL2 ⁴⁰³⁰	Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC 2385 ⁴⁰³¹ . Ono je napravljeno da smanji opasnost od određenih napada na BGP, kao što su TCP reseti.
3.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podesi na jedinstvenu vrednost i da se koristi u rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da fingerprint-uje operativni sistem.	BID 4314 ⁴⁰³² CVE CVE-2002-0510 ⁴⁰³³ XF linux-udp-fingerprint(8588) ⁴⁰³⁴	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili pak ranjivost koju treba popravljati, tako da ne postoje rešenja koja se mogu kupiti. Jedino se može postaviti fajervol ili neka druga sprava za filtriranje između napadnutog i neprijateljskog napada koji je u mogućnosti da randomizuje IP ID-jeve.
4.	Apache httpd apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpd-cve-2011-0419)	172.23.202.125:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_autoindex. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_fnmatch() u sklopu APR biblioteke. Ako je omogućen	CVE CVE-2011-0419 ⁴⁰³⁵ REDHAT RHSA-2011-0507 ⁴⁰³⁶ SECUNIA 44490 ⁴⁰³⁷ SECUNIA 44564 ⁴⁰³⁸ SECUNIA 44574 ⁴⁰³⁹ URL1 ⁴⁰⁴⁰	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.18.tar.gz

⁴⁰¹³ <http://www.securityfocus.com/bid/10183>⁴⁰¹⁴ <http://www.kb.cert.org/vuls/id/415294>⁴⁰¹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁴⁰¹⁶ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁴⁰¹⁷ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁴⁰¹⁸ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁴⁰¹⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>⁴⁰²⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>⁴⁰²¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>⁴⁰²² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>⁴⁰²³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>⁴⁰²⁴ <http://secunia.com/advisories/11440/>⁴⁰²⁵ <http://secunia.com/advisories/11458/>⁴⁰²⁶ <http://secunia.com/advisories/22341/>⁴⁰²⁷ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>⁴⁰²⁸ <http://xforce.iss.net/xforce/xfdb/15886>⁴⁰²⁹ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁴⁰³⁰ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>⁴⁰³¹ <http://www.ietf.org/rfc/rfc2385.txt>⁴⁰³² <http://www.securityfocus.com/bid/4314>⁴⁰³³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>⁴⁰³⁴ <http://xforce.iss.net/xforce/xfdb/8588>⁴⁰³⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419>⁴⁰³⁶ <http://rhn.redhat.com/errata/RHSA-2011-0507.html>⁴⁰³⁷ <http://secunia.com/advisories/44490/>⁴⁰³⁸ <http://secunia.com/advisories/44564/>⁴⁰³⁹ <http://secunia.com/advisories/44574/>⁴⁰⁴⁰ http://httpd.apache.org/security/vulnerabilities_22.html

		mod_autoindex, a indksi direktorijuma mod_autoindex su sadržavali fajlove sa dovoljno dugim nazivima, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do preterane upotrebe CPU-a. Ovo bi moglo da bude iskorišćeno u napadu odbijanja servisa. Zahvaljujući Maksymilian Arciemowicz prijavljen je ovaj propust.			
5.	HTTP TRACE Method Enabled (http-trace-method-enabled)	172.23.202.125:80 HTTP TRACE metoda se obično koristi da uzvрати potpuni HTTP zahtev klijentu koji ga zahteva, u cilju debugovanja proxy servera. Napadač bi mogao da kreira web stranicu koristeći XMLHTTP, ActiveX ili XMLHttpRequest da natera klijenta da pošalje TRACE zahtev i da sačuva klijenove kolačiće. Kao posledica može da se javi XSS napad. Primer : 172.23.202.125:80 Running vulnerable HTTP service. http://172.23.202.125/1:TRACE/HTTP/1.1 2: Host: 172.23.202.125 3: Cookie: vulnerable=yes	CVE CVE-2004-2320 ⁴⁰⁴¹ CVE CVE-2004-2763 ⁴⁰⁴² CVE CVE-2005-3398 ⁴⁰⁴³ CVE CVE-2006-4683 ⁴⁰⁴⁴ CVE CVE-2007-3008 ⁴⁰⁴⁵ CVE CVE-2008-7253 ⁴⁰⁴⁶ CVE CVE-2009-2823 ⁴⁰⁴⁷ CVE CVE-2010-0386 ⁴⁰⁴⁸ OSVDB 877 ⁴⁰⁴⁹ SUN 50603 ⁴⁰⁵⁰ BID 9561 ⁴⁰⁵¹ URL1 ⁴⁰⁵² URL2 ⁴⁰⁵³	Ozbiljan	Apache Onemogućiti HTTP TRACE metodu za Apache. Novije verzije Apache-a (1.3.34 i 2.0.55 i novije) omogućuju konfiguracionu direktivu koja se zove TraceEnable. Da bi se odbili TRACE zahtevi, dodaje se sledeći red u konfiguraciju servera: TraceEnable off Za starije verzije Apache web servera, koristiti modul mod_rewrite da bi se odbili TRACE zahteve: RewriteEngine On RewriteCond %{REQUEST_METHOD} ^TRACE RewriteRule .* - [F]
6.	Database Open Access (database-open-access)	172.23.202.125:3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7.	URL1 ⁴⁰⁵⁴	Umeren	Konfigurisati server baze podataka tako da se dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.
7.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme	CVE CVE-1999-0524 ⁴⁰⁵⁵ OSVDB 95 ⁴⁰⁵⁶ XF icmp-netmask(306) ⁴⁰⁵⁷	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp

⁴⁰⁴¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2320>⁴⁰⁴² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2763>⁴⁰⁴³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-3398>⁴⁰⁴⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-4683>⁴⁰⁴⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3008>⁴⁰⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-7253>⁴⁰⁴⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2823>⁴⁰⁴⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0386>⁴⁰⁴⁹ <http://osvdb.org/877>⁴⁰⁵⁰ <https://sunsolve.sun.com/search/document.do?assetkey=1-22-50603-1> pristupljeno 18.12.2011⁴⁰⁵¹ <http://www.securityfocus.com/bid/9561>⁴⁰⁵² <http://www.apacheweek.com/issues/03-01-24#news>⁴⁰⁵³ <http://www.kb.cert.org/vuls/id/867593>⁴⁰⁵⁴ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf⁴⁰⁵⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁴⁰⁵⁶ <http://www.osvdb.org/95>

		udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	XF timestamp(322) ⁴⁰⁵⁸ icmp-		request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
8.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1 ⁴⁰⁵⁹ URL2 ⁴⁰⁶⁰ URL3 ⁴⁰⁶¹	Umeren	Onemogućiti TCP vremenske pečate na Linux-u. Podesiti vrednost net.ipv4.tcp_timestamps na 0 pokretanjem sledeće komande: sysctl -w net.ipv4.tcp_timestamps=0 Uz to, sledeću vrednost staviti u difoltni sysctl konfiguracioni fajl, uopšteno sysctl.conf: net.ipv4.tcp_timestamps=0

Tabela 107. Linux OS – Pronađeni servisi na IP adresi 172.23.202.125 (2011. godina)

SERVISI	HTTP 172.23.202.125 tcp 80 Apache 2.2.17 http.banner: Apache/2.2.17 (Linux/SUSE) http.banner.server: Apache/2.2.17 (Linux/SUSE) MySQL 172.23.202.125 tcp 3306 SSH 172.23.202.125 tcp 22 OpenSSH 5.8 ssh.banner: SSH-2.0-OpenSSH_5.8 ssh.protocol.version: 2.0 ssh.rsa.pubkey.fingerprint: 3742BD5F5C962CA56AD0CAEB8D640633 Portmapper 172.23.202.125 tcp 111 program-number: 100000 program-version: 2 172.23.202.125 udp 111 program-number: 100000 program-version: 2
Spidered Web site	http://172.23.202.125:80 Common Default URLs: Access Error (403) cgi-bin error Successful (200) icons Guessed URLs

⁴⁰⁵⁷ <http://xforce.iss.net/xforce/xfdb/306>⁴⁰⁵⁸ <http://xforce.iss.net/xforce/xfdb/322>⁴⁰⁵⁹ http://www.forensicswiki.org/wiki/TCP_timestamps⁴⁰⁶⁰ <http://www.ietf.org/rfc/rfc1323.txt>⁴⁰⁶¹ <http://uptime.netcraft.com/>

	Access Error (403) ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-script+AD4-cgi-bin error Redirect (301) icons small Successful (200) icons ?P=+ADw-script+AD4-alert(42)+ADwscript+AD4-script+AD4-small Linked URLs The following URLs were found as links in the content of other web pages. Access Error (403) Successful (200) icons README README.html small

4.3.3 WINDOWS OPERATIVNI SISTEMI - SKENIRANJE SERVISA NA RANJIVOSTI U 2013.

Tabela 108. Windows OS sa IP adresama 172.23.202.109, 172.23.202.106, 172.23.202.69 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.109		OS: Microsoft Windows XP tablet edition SP1 x86, WINXPTabX86sp1			15
IP adresa: 172.23.202.106		OS: Microsoft Windows XP pro sp1 x86, WINXPproSP1x86			15
IP adresa: 172.23.202.69		OS: Microsoft Windows XP pro sp1 x64 WINXPproSP1x64			15
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti

1.	Microsoft Server Service / CanonicalizePathName() Remote Code Execution Vulnerability (dcerpc-msnetapi-netpathcanonicalize-dos)	Određene verzije Microsoft Windows-a su ranjive na daljinsko preopterećenje bafera (privremene memorije) koje bi moglo da kompromituje određeni računar. Posebno izrađen paket se može koristiti sa pozivom ka NetPathCanonicalize RPC ruti na servisu servera, pri čemu bi napadač mogao da izvrši kôd pod sistemskim nivoom pristupa.	BID: 19409 ⁴⁰⁶² CERT: TA06-220A ⁴⁰⁶³ CERT-VN: 650769 ⁴⁰⁶⁴ OVAL OVAL492 ⁴⁰⁶⁵ SECUNIA 21388 ⁴⁰⁶⁶ XF ms-server-service-bo(28002) ⁴⁰⁶⁷ CVE: CVE-2006-3439 ⁴⁰⁶⁸ , MS: MS06-040 ⁴⁰⁶⁹ ,	Kritičan	Uraditi download a zatim instalirati Microsoft patch za 32-bitnu verziju : WindowsXP-KB921883-x86-ENU.EXE ⁴⁰⁷⁰ ili za 64-bitnu verziju Windowsa : WindowsServer2003.WindowsXP-KB921883-v2-x64-ENU.exe ⁴⁰⁷¹
2.	MS03-039: Buffer Overrun In RPCSS Service Could Allow Code Execution (824146) (windows-hotfix-ms03-039)	Napadač koji bi uspešno iskoristio ove ranjivosti mogao bi da pokrene kôd sa privilegijama lokalnog sistema na napadnutom sistemu, ili bi mogao da prouzrokuje isključenje RPCSS servisa. Napadač bi tada bio u mogućnosti da preduzme bilo kakvu akciju na sistemu, uključujući instaliranje programa, pregledanje, menjanje ili brisanje podataka ili otvaranje novih naloga sa svih privilegijama. Da bi iskoristio ove ranjivosti, napadač bi mogao da kreira program koji bi poslao malicioznu RPC poruku ranjivom sistemu, ciljajući na RPCSS servis.	CERT CA-2003-19 ⁴⁰⁷² CERT CA-2003-23 ⁴⁰⁷³ CERT-VN 254236 ⁴⁰⁷⁴ CERT-VN 326746 ⁴⁰⁷⁵ CERT-VN 483492 ⁴⁰⁷⁶ OVAL OVAL1118 ⁴⁰⁷⁷ OVAL OVAL1202 ⁴⁰⁷⁸ OVAL OVAL127 ⁴⁰⁷⁹ OVAL OVAL1813 ⁴⁰⁸⁰ OVAL OVAL20 ⁴⁰⁸¹ OVAL OVAL264 ⁴⁰⁸² OVAL OVAL2884 ⁴⁰⁸³ OVAL OVAL2968 ⁴⁰⁸⁴ OVAL OVAL3966 ⁴⁰⁸⁵ OVAL OVAL4224 ⁴⁰⁸⁶ OVAL OVAL494 ⁴⁰⁸⁷ XF win2k-message-queue-bo(13131) ⁴⁰⁸⁸ CVE: CVE-2003-0528 ⁴⁰⁸⁹ , CVE: CVE-2003-0605 ⁴⁰⁹⁰ , CVE: CVE-2003-0715 ⁴⁰⁹¹ , CVE CVE-2003-0995 ⁴⁰⁹²	Kritičan	Uraditi download a zatim instalirati Microsoft patch za 32-bitnu verziju : WindowsXP-KB824146-x86-ENU.exe (1543456 bytes) ⁴⁰⁹⁵ , ili za 64-bitnu verziju Windowsa : WindowsXP-KB824146-ia64-ENU.exe ⁴⁰⁹⁶ Uraditi download a zatim instalirati Microsoft patch DirectX9-KB819696-x86-ENU.exe (970312 bytes) ⁴⁰⁹⁷

⁴⁰⁶² <http://www.securityfocus.com/bid/19409>⁴⁰⁶³ <http://www.us-cert.gov/ncas/alerts/ta06-220a>⁴⁰⁶⁴ <http://www.kb.cert.org/vuls/id/650769>⁴⁰⁶⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:492>⁴⁰⁶⁶ <http://secunia.com/advisories/21388/>⁴⁰⁶⁷ <http://xforce.iss.net/xforce/xfdb/28002>⁴⁰⁶⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-3439>⁴⁰⁶⁹ <http://technet.microsoft.com/en-us/security/bulletin/ms06-040>⁴⁰⁷⁰ download.microsoft.com/download/c/2/b/c2b41862-1113-4e40-a81a-d6971733e361/WindowsXP-KB921883-x86-ENU.exe⁴⁰⁷¹ <http://download.microsoft.com/download/0/f/9/0f9eb45e-cb70-40dd-8506-8cdf226731f7/WindowsServer2003.WindowsXP-KB921883-v2-x64-ENU.exe>⁴⁰⁷² <http://www.us-cert.gov/ncas/alerts/ca-2003-19>⁴⁰⁷³ <http://www.us-cert.gov/ncas/alerts/ca-2003-23>⁴⁰⁷⁴ <http://www.kb.cert.org/vuls/id/254236>⁴⁰⁷⁵ <http://www.kb.cert.org/vuls/id/326746>⁴⁰⁷⁶ <http://www.kb.cert.org/vuls/id/483492>⁴⁰⁷⁷ oval.mitre.org/oval/definitions/data/OVAL1118.html⁴⁰⁷⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1202>⁴⁰⁷⁹ oval.mitre.org/oval/definitions/data/OVAL127.html⁴⁰⁸⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1813>⁴⁰⁸¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:20>⁴⁰⁸² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:264>⁴⁰⁸³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2884>⁴⁰⁸⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2968>⁴⁰⁸⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3966>⁴⁰⁸⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4224>⁴⁰⁸⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:494>⁴⁰⁸⁸ <http://xforce.iss.net/xforce/xfdb/13131>⁴⁰⁸⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0528>⁴⁰⁹⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0605>⁴⁰⁹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0715>

			MSKB: 824146 ⁴⁰⁹³ , MS:MS03-039 ⁴⁰⁹⁴		
3.	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (windows-hotfix-ms08-067)	172.23.202.109:139 172.23.202.109:445 172.23.202.106:139 172.23.202.106:445 172.23.202.69:139 172.23.202.69:445 Ovo ažuriranje bezbednosti rešava ranjivost koja je prijavljena od strane privatnog lica. Ranjivost bi mogla da omogući daljinsko izvršavanje koda ukoliko je napadnuti sistem primio posebno izrađen RPC zahtev. Na sistemima Microsoft Windows 2000, Windows XP, i Windows Server 2003, napadač bi mogao da iskoristi ovu ranjivost bez proveravanja autentičnosti i da pokrene proizvoljan kôd. Moguće je da ova ranjivost može biti upotrebljena za intenziviranje skrivenog korišćenja exploit-a. Praksa je pokazala da upotreba zaštitnog zida može da pomogne u zaštiti mrežnih resursa od napada koji potiču izvan okvira organizacije.	BID 31874 ⁴⁰⁹⁸ CERT TA08-297A ⁴⁰⁹⁹ CERT TA09-088A ⁴¹⁰⁰ CERT-VN 827267 ⁴¹⁰¹ IAVM 2008-A-0081 ⁴¹⁰² OVAL OVAL6093 ⁴¹⁰³ XF 46040 ⁴¹⁰⁴ MS: MS08-067 ⁴¹⁰⁵ MSKB: 958644 ⁴¹⁰⁶ CVE: CVE-2008-4250 ⁴¹⁰⁷ SECUNIA: 32326 ⁴¹⁰⁸ URL1 ⁴¹⁰⁹ URL2 ⁴¹¹⁰ URL3 ⁴¹¹¹ URL4 ⁴¹¹²	Kritičan	Uraditi download a zatim instalirati Microsoft patch za 32-bitnu verziju : WindowsXP-KB958644-x86-ENU.exe (648560 bytes) ⁴¹¹³ ili za 64-bitnu verziju Windowsa : WindowsServer2003.WindowsXP-KB958644-x64-ENU.exe ⁴¹¹⁴
4.	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (windows-hotfix-ms09-001)	172.23.202.109:139 172.23.202.109:445 172.23.202.106:139 172.23.202.106:445 172.23.202.69:139 172.23.202.69:445 Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti koje su privatno	BID 31179 ⁴¹¹⁵ BID 33121 ⁴¹¹⁶ BID 33122 ⁴¹¹⁷ OVAL OVAL5248 ⁴¹¹⁸ OVAL OVAL5262 ⁴¹¹⁹ OVAL OVAL5863 ⁴¹²⁰ OVAL OVAL6044 ⁴¹²¹ XF 45146 ⁴¹²²	Kritičan	Uraditi download a zatim instalirati Microsoft patch za 32-bitnu verziju : WindowsXP-KB958687-x86-ENU.exe (658288 bytes) ⁴¹³² ili za 64-bitnu verziju Windowsa :

⁴⁰⁹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0995>⁴⁰⁹⁵ www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb824146-x86-enu_b957699c7365c462446bd552cd6d203.exe⁴⁰⁹⁶ <http://download.microsoft.com/download/a/c/e/ace7fe00-4bf7-4421-8ccf-2913395500aa/WindowsXP-KB824146-ia64-ENU.exe>⁴⁰⁹⁷ http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/directx9-kb819696-x86-enu_977f8cc86c1e151a0168d1296210913.exe⁴⁰⁹³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;824146>⁴⁰⁹⁴ <http://technet.microsoft.com/en-us/security/bulletin/ms03-039>⁴⁰⁹⁸ <http://www.securityfocus.com/bid/31874>⁴⁰⁹⁹ <http://www.us-cert.gov/ncas/alerts/ta08-297a>⁴¹⁰⁰ <http://www.us-cert.gov/ncas/alerts/ta09-088a>⁴¹⁰¹ <http://www.kb.cert.org/vuls/id/827267>⁴¹⁰² <http://iase.disa.mil/stigs/iavm-cve.html>⁴¹⁰³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6093>⁴¹⁰⁴ <http://xforce.iss.net/xforce/xfdb/46040>⁴¹⁰⁵ <http://technet.microsoft.com/en-us/security/bulletin/ms08-067>⁴¹⁰⁶ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958644>⁴¹⁰⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4250>⁴¹⁰⁸ <http://secunia.com/advisories/32326/>⁴¹⁰⁹ blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx⁴¹¹⁰ <http://blogs.msdn.com/b/sdl/archive/2008/10/22/ms08-067.aspx>⁴¹¹¹ <http://blogs.technet.com/b/msrc/archive/2008/10/23/ms08-067-released.aspx>⁴¹¹² <http://technet.microsoft.com/en-us/security/bulletin/MS08-067>⁴¹¹³ http://download.windowsupdate.com/msdownload/update/software/secu/2008/10/windowsxpkb958644-x86-enu_5c135a8dae5721849430afe27af255f83e64f62b.exe⁴¹¹⁴ <http://download.microsoft.com/download/5/8/1/5811b6cc-5884-4486-b05d-de69f0e94f67/WindowsServer2003.WindowsXP-KB958644-x64-ENU.exe>⁴¹¹⁵ <http://www.securityfocus.com/bid/31179>⁴¹¹⁶ <http://www.securityfocus.com/bid/33121>⁴¹¹⁷ <http://www.securityfocus.com/bid/33122>⁴¹¹⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5248>⁴¹¹⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5262>⁴¹²⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5863>⁴¹²¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6044>⁴¹²² <http://xforce.iss.net/xforce/xfdb/45146>

		prijavljene a odnose se na protokol Microsoft Server Message Block-a (SMB). Ranjivosti mogu da omoguće daljinsko izvršenje kôda na ugroženim sistemima. Napadač koji je uspešno iskoristio ove ranjivosti može da instalira programe, pregleda, menja ili briše podatke ili otvara nove naloge sa potpunim korisničkim pravima. Praksa je pokazala da zaštitni zid i njegove standardne konfiguracije po defaultu mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan okvira organizacije. Za sisteme koji su stalno povezani na Internet preporuka je da imaju što manji broj izloženih portova.	MS: MS09-001 ⁴¹²³ MSKB: 958687 ⁴¹²⁴ CVE: CVE-2008-4114 ⁴¹²⁵ CVE: CVE-2008-4835 ⁴¹²⁶ CVE: CVE-2008-4834 ⁴¹²⁷ SECUNIA: 31883 ⁴¹²⁸ URL1 ⁴¹²⁹ URL2 ⁴¹³⁰ URL3 ⁴¹³¹		WindowsServer2003.WindowsXP-KB958687-x64-ENU.exe ⁴¹³³
5.	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-012)	172.23.202.109:139 172.23.202.109:445 172.23.202.106:139 172.23.202.106:445 172.23.202.69:139 172.23.202.69:445 Ovo ažuriranje bezbednosti rešava nekoliko privatno prijavljenih ranjivosti na Microsoft Windows-u. Opasnost od ove ranjivosti leži u tome što bi ona omogućila daljinsko izvršavanje kôda ukoliko bi napadač kreirao posebno opremljen SMB paket i poslao ga ugroženom sistemu. Dosadašnja praksa fajervola i standardne fajervol default konfiguracije mogu da pomognu u zaštiti mrežnih resursa od napada (koji bi pokušali da iskoriste ove ranjivosti), a koji potiču izvan okvira organizacije.	MS: MS10-012 ⁴¹³⁴ MSKB - 971468 ⁴¹³⁵ CVE: CVE-2010-0020 ⁴¹³⁶ CVE: CVE-2010-0021 ⁴¹³⁷ CVE: CVE-2010-0022 ⁴¹³⁸ CVE CVE-2010-0231 ⁴¹³⁹ CERT TA10-040A ⁴¹⁴⁰ OVAL OVAL7751 ⁴¹⁴¹ OVAL OVAL8314 ⁴¹⁴² OVAL OVAL8438 ⁴¹⁴³ OVAL OVAL8524 ⁴¹⁴⁴	Kritičan	Uraditi download a zatim instalirati Microsoft patch za 32-bitnu verziju : WindowsXP-KB971468-x86-ENU.exe (664952 bytes) ⁴¹⁴⁵ ili za 64-bitnu verziju Windowsa : WindowsServer2003.WindowsXP-KB971468-x64-ENU.exe ⁴¹⁴⁶
6.	MS10-054:	172.23.202.109:139 172.23.202.109:445	CVE: CVE-2010-2550 ⁴¹⁴⁷ CVE: CVE-2010-2551 ⁴¹⁴⁸	Kritičan	Uraditi download a zatim

⁴¹³² http://download.windowsupdate.com/msdownload/update/software/secu/2008/12/windowsxp-kb958687-x86-enu_a9b85264e9b75e552ae10cd212937b8686a96833.exe

⁴¹²³ <http://technet.microsoft.com/en-us/security/bulletin/MS09-001>

⁴¹²⁴ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958687>

⁴¹²⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4114>

⁴¹²⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4835>

⁴¹²⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4834>

⁴¹²⁸ <http://secunia.com/advisories/31883/>

⁴¹²⁹ http://www.vallejo.cc/proyectos/vista_SMB_write_DoS.htm

⁴¹³⁰ <http://www.zerodayinitiative.com/advisories/ZDI-09-001/>

⁴¹³¹ <http://www.zerodayinitiative.com/advisories/ZDI-09-002/>

⁴¹³³ <http://download.microsoft.com/download/6/6/B/66B29397-A4AB-4586-BEFF-68379C94E99F/WindowsServer2003.WindowsXP-KB958687-x64-ENU.exe>

⁴¹³⁴ <http://technet.microsoft.com/en-us/security/bulletin/MS10-012>

⁴¹³⁵ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;971468>

⁴¹³⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0020>

⁴¹³⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0021>

⁴¹³⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0022>

⁴¹³⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0231>

⁴¹⁴⁰ <http://www.us-cert.gov/ncas/alerts/ta10-040a>

⁴¹⁴¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7751>

⁴¹⁴² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8314>

⁴¹⁴³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8438>

⁴¹⁴⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8524>

⁴¹⁴⁵ http://download.windowsupdate.com/msdownload/update/software/secu/2010/01/windowsxp-kb971468-x86-enu_68d7899c8b8462219daf40f02c6fb9f362b1ee6b.exe

⁴¹⁴⁶ <http://download.microsoft.com/download/6/0/8/6086ED38-9FC7-476F-BE60-F67E56A335FB/WindowsServer2003.WindowsXP-KB971468-x64-ENU.exe>

⁴¹⁴⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2550>

	Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-054)	172.23.202.106:139 172.23.202.106:445 172.23.202.69:139 172.23.202.69:445 Opis je isti kao kod ranjivosti MS10-012	CVE: CVE-2010-2552 ⁴¹⁴⁹ MS: MS10-054 ⁴¹⁵⁰ CERT TA10-222A ⁴¹⁵¹ MSKB 982214 ⁴¹⁵² OVAL OVAL11106 ⁴¹⁵³ OVAL OVAL12015 ⁴¹⁵⁴ OVAL OVAL12072 ⁴¹⁵⁵		instalirati Microsoft patch za 32-bitnu verziju : windowsxp-kb982214-x86-enu.exe (661368 bytes) ⁴¹⁵⁶ ili za 64-bitnu verziju Windowsa : WindowsServer2003.WindowsXP-KB982214-x64-ENU.exe ⁴¹⁵⁷
7.	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms11-020)	172.23.202.109:139 172.23.202.109:445 172.23.202.106:139 172.23.202.106:445 172.23.202.69:139 172.23.202.69:445 Opis je isti kao kod ranjivosti MS10-012	CVE: CVE-2011-0661 ⁴¹⁵⁸ MS: MS11-020 ⁴¹⁵⁹ MSKB: 2508429 ⁴¹⁶⁰ BID 47198 ⁴¹⁶¹ OSVDB 71781 ⁴¹⁶² OVAL OVAL12076 ⁴¹⁶³ CERT TA11-102A ⁴¹⁶⁴ SECUNIA 44072 ⁴¹⁶⁵ IAVM 2011-A-0050 ⁴¹⁶⁶	Kritičan	Uraditi download a zatim instalirati Microsoft patch za 32-bitnu verziju : windowsxp-kb2508429-x86-enu.exe (664960 bytes) ⁴¹⁶⁷ ili za 64-bitnu verziju Windowsa : WindowsServer2003.WindowsXP-KB2508429-x64-ENU.exe ⁴¹⁶⁸
8.	MS03-026: Buffer Overrun In RPC Interface Could Allow Code Execution (823980) (windows-hotfix-ms03-026)	Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti u Windows Distributed Component Object Model (DCOM) Remote Procedure Call (RPC). Napadač koji uspešno iskoristi ovu ranjivost, bio bi u mogućnosti da pokrene kôd sa privilegijama lokalnog sistema na napadnutom sistemu. Napadač bi bio u mogućnosti da preduzme bilo kakvu akciju na sistemu, uključujući instaliranje programa, pregledanje, menjanje ili	BID 8205 ⁴¹⁶⁹ CERT CA-2003-16 ⁴¹⁷⁰ CERT CA-2003-19 ⁴¹⁷¹ CERT-VN 568148 ⁴¹⁷² CVE CVE-2003-0352 ⁴¹⁷³ MS MS03-026 ⁴¹⁷⁴ MSKB 823980 ⁴¹⁷⁵ OVAL OVAL194 ⁴¹⁷⁶ OVAL OVAL2343 ⁴¹⁷⁷ OVAL OVAL296 ⁴¹⁷⁸ XF win-rpc-dcom-	Kritičan	Uraditi download a zatim instalirati Microsoft patch za 32-bitnu verziju : WindowsXP-KB823980-x86-ENU.exe (1291040 bytes) ⁴¹⁸⁰ ili za 64-bitnu verziju Windowsa : WindowsXP-KB823980-ia64-ENU.exe ⁴¹⁸¹

⁴¹⁴⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2551>⁴¹⁴⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2552>⁴¹⁵⁰ <http://technet.microsoft.com/en-us/security/bulletin/MS10-054>⁴¹⁵¹ <http://www.us-cert.gov/ncas/alerts/ta10-222a>⁴¹⁵² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;982214>⁴¹⁵³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11106>⁴¹⁵⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12015>⁴¹⁵⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12072>⁴¹⁵⁶ http://download.windowsupdate.com/msdownload/update/software/secu/2010/07/windowsxp-kb982214-x86-enu_a24853f682dad3157da4e4a39372951a8ec1e407.exe⁴¹⁵⁷ <http://download.microsoft.com/download/6/9/3/693AA8A1-BC95-4504-9AD8-3E69D4D2D1B3/WindowsServer2003.WindowsXP-KB982214-x64-ENU.exe>⁴¹⁵⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661>⁴¹⁵⁹ <http://technet.microsoft.com/en-us/security/bulletin/ms11-020>⁴¹⁶⁰ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;2508429>⁴¹⁶¹ <http://www.securityfocus.com/bid/47198>⁴¹⁶² <http://www.osvdb.org/71781>⁴¹⁶³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12076>⁴¹⁶⁴ <http://www.us-cert.gov/ncas/alerts/ta11-102a>⁴¹⁶⁵ <http://secunia.com/advisories/44072/>⁴¹⁶⁶ <http://secunia.com/advisories/44072/>⁴¹⁶⁷ http://download.windowsupdate.com/msdownload/update/software/secu/2011/03/windowsxp-kb2508429-x86-enu_e0b40d81f2ecc1bad43439a6bd0a9e2a0ab7dd56.exe⁴¹⁶⁸ <http://download.microsoft.com/download/8/3/3/833C20D2-59EA-4D23-960F-11270C0C0319/WindowsServer2003.WindowsXP-KB2508429-x64-ENU.exe>⁴¹⁶⁹ <http://www.securityfocus.com/bid/8205>⁴¹⁷⁰ <http://www.us-cert.gov/ncas/alerts/ca-2003-16>⁴¹⁷¹ <http://www.us-cert.gov/ncas/alerts/ca-2003-19>⁴¹⁷² <http://www.kb.cert.org/vuls/id/568148>⁴¹⁷³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0352>⁴¹⁷⁴ <http://technet.microsoft.com/en-us/security/bulletin/ms03-026>⁴¹⁷⁵ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;823980>⁴¹⁷⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:194>⁴¹⁷⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2343>⁴¹⁷⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:296>

		brisanje podataka, ili pak kreiranje novih naloga sa svim privilegijama. Da bi iskoristio ovu ranjivost, napadač bi morao da pošalje posebno kreiran zahtev udaljenom kompjuteru na specifične RPC portove.	bo(12629) ⁴¹⁷⁹		
9.	MS04-011: Security Update for Microsoft Windows (835732) (windows-hotfix-ms04-011)	172.23.202.109:139 172.23.202.109:445 172.23.202.106:139 172.23.202.106:445 172.23.202.69:139 172.23.202.69:445 Ovo ažuriranje rešava nekoliko novootkrivenih ranjivosti. Napadač koji uspešno iskoristi ovu ranjivost bi mogao da preuzme potpunu kontrolu nad napadnutim sistemom, uključujući instaliranje programa, pregledanje, menjanje ili brisanje podataka ili čak otvaranje novih naloga sa svim privilegijama.	BID 10108⁴¹⁸² BID 10113⁴¹⁸³ BID 10114⁴¹⁸⁴ BID 10115⁴¹⁸⁵ BID 10117⁴¹⁸⁶ BID 10118⁴¹⁸⁷ BID 10119⁴¹⁸⁸ BID 10120⁴¹⁸⁹ BID 10122⁴¹⁹⁰ BID 10124⁴¹⁹¹ BID 10125⁴¹⁹² BID 10126⁴¹⁹³ CERT TA04-104A⁴¹⁹⁴ CERT-VN 122076⁴¹⁹⁵ CERT-VN 150236⁴¹⁹⁶ CERT-VN 206468⁴¹⁹⁷ CERT-VN 255924⁴¹⁹⁸ CERT-VN 260588⁴¹⁹⁹ CERT-VN 353956⁴²⁰⁰ CERT-VN 471260⁴²⁰¹ CERT-VN 526084⁴²⁰² CERT-VN 547028⁴²⁰³ CERT-VN 586540⁴²⁰⁴ CERT-VN 638548⁴²⁰⁵ CERT-VN 639428⁴²⁰⁶ CVE CVE-2003-0663⁴²⁰⁷ CVE CVE-2003-0719⁴²⁰⁸ CVE CVE-2003-0806⁴²⁰⁹ CVE CVE-2003-0906⁴²¹⁰ CVE CVE-2003-0907⁴²¹¹	Kritičan	Uraditi download a zatim instalirati Microsoft patch za 32-bitnu verziju : WindowsXP-KB835732-x86-ENU.EXE (2710296 bytes) ⁴²⁷⁸ ili za 64-bitnu verziju Windowsa : WindowsXP-KB835732-IA64-ENU.EXE ⁴²⁷⁹

⁴¹⁸⁰ http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb823980-x86-enu_1d296adab6699e66210e5a350236381.exe

⁴¹⁸¹ <http://download.microsoft.com/download/a/7/5/a75b3c8f-5df0-451b-b526-cfc7c5c67df5/WindowsXP-KB823980-ia64-ENU.exe>

⁴¹⁷⁹ <http://xforce.iss.net/xforce/xfdb/12629>

⁴¹⁸² <http://www.securityfocus.com/bid/10108>

⁴¹⁸³ <http://www.securityfocus.com/bid/10113>

⁴¹⁸⁴ <http://www.securityfocus.com/bid/10114>

⁴¹⁸⁵ <http://www.securityfocus.com/bid/10115>

⁴¹⁸⁶ <http://www.securityfocus.com/bid/10117>

⁴¹⁸⁷ <http://www.securityfocus.com/bid/10118>

⁴¹⁸⁸ <http://www.securityfocus.com/bid/10119>

⁴¹⁸⁹ <http://www.securityfocus.com/bid/10120>

⁴¹⁹⁰ <http://www.securityfocus.com/bid/10122>

⁴¹⁹¹ <http://www.securityfocus.com/bid/10124>

⁴¹⁹² <http://www.securityfocus.com/bid/10125>

⁴¹⁹³ <http://www.securityfocus.com/bid/10126>

⁴¹⁹⁴ <http://www.us-cert.gov/ncas/alerts/ta04-104a>

⁴¹⁹⁵ <http://www.kb.cert.org/vuls/id/122076>

⁴¹⁹⁶ <http://www.kb.cert.org/vuls/id/150236>

⁴¹⁹⁷ <http://www.kb.cert.org/vuls/id/206468>

⁴¹⁹⁸ <http://www.kb.cert.org/vuls/id/255924>

⁴¹⁹⁹ <http://www.kb.cert.org/vuls/id/260588>

⁴²⁰⁰ <http://www.kb.cert.org/vuls/id/353956>

⁴²⁰¹ <http://www.kb.cert.org/vuls/id/471260>

⁴²⁰² <http://www.kb.cert.org/vuls/id/526084>

⁴²⁰³ <http://www.kb.cert.org/vuls/id/547028>

⁴²⁰⁴ <http://www.kb.cert.org/vuls/id/586540>

⁴²⁰⁵ <http://www.kb.cert.org/vuls/id/638548>

⁴²⁰⁶ <http://www.kb.cert.org/vuls/id/639428>

⁴²⁰⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0663>

⁴²⁰⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0719>

⁴²⁰⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0806>

⁴²¹⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0906>

⁴²¹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0907>

			CVE CVE-2003-0908⁴²¹² CVE CVE-2003-0909⁴²¹³ CVE CVE-2003-0910⁴²¹⁴ CVE CVE-2004-0117⁴²¹⁵ CVE CVE-2004-0118⁴²¹⁶ CVE CVE-2004-0119⁴²¹⁷ CVE CVE-2004-0120⁴²¹⁸ CVE CVE-2004-0123⁴²¹⁹ OVAL OVAL1004⁴²²⁰ OVAL OVAL1007⁴²²¹ OVAL OVAL1016⁴²²² OVAL OVAL1046⁴²²³ OVAL OVAL1054⁴²²⁴ OVAL OVAL1064⁴²²⁵ OVAL OVAL1076⁴²²⁶ OVAL OVAL1093⁴²²⁷ OVAL OVAL1512⁴²²⁸ OVAL OVAL1718⁴²²⁹ OVAL OVAL1808⁴²³⁰ OVAL OVAL1962⁴²³¹ OVAL OVAL1997⁴²³² OVAL OVAL883⁴²³³ OVAL OVAL885⁴²³⁴ OVAL OVAL886⁴²³⁵ OVAL OVAL889⁴²³⁶ OVAL OVAL890⁴²³⁷ OVAL OVAL892⁴²³⁸ OVAL OVAL895⁴²³⁹ OVAL OVAL896⁴²⁴⁰ OVAL OVAL897⁴²⁴¹ OVAL OVAL898⁴²⁴² OVAL OVAL903⁴²⁴³ OVAL OVAL904⁴²⁴⁴ OVAL OVAL907⁴²⁴⁵		

⁴²⁷⁸ http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb835732-x86-enu_99fc98fc8e8cbf6720f28028a1f05eb.exe
⁴²⁷⁹ <http://download.microsoft.com/download/6/b/4/6b4af6c4-62c6-44b2-8d29-9b305636d0b6/WindowsXP-KB835732-IA64-ENU.EXE>
⁴²¹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0908>
⁴²¹³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0909>
⁴²¹⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0910>
⁴²¹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0117>
⁴²¹⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0118>
⁴²¹⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0119>
⁴²¹⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0120>
⁴²¹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0123>
⁴²²⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1004>
⁴²²¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1007>
⁴²²² oval.mitre.org/oval/definitions/data/OVAL1016.html
⁴²²³ oval.mitre.org/oval/definitions/data/OVAL1046.html
⁴²²⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1054>
⁴²²⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1064>
⁴²²⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1076>
⁴²²⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1093>
⁴²²⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1512>
⁴²²⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1718>
⁴²³⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1808>
⁴²³¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1962>
⁴²³² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1997>
⁴²³³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:883>
⁴²³⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:885>
⁴²³⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:886>
⁴²³⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:889>
⁴²³⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:890>
⁴²³⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:892>
⁴²³⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:895>
⁴²⁴⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:896>
⁴²⁴¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:897>
⁴²⁴² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:898>
⁴²⁴³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:903>
⁴²⁴⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:904>

			OVAL OVAL911⁴²⁴⁶ OVAL OVAL919⁴²⁴⁷ OVAL OVAL924⁴²⁴⁸ OVAL OVAL946⁴²⁴⁹ OVAL OVAL951⁴²⁵⁰ OVAL OVAL959⁴²⁵¹ OVAL OVAL964⁴²⁵² URL1⁴²⁵³ URL2⁴²⁵⁴ URL3⁴²⁵⁵ URL4⁴²⁵⁶ URL5⁴²⁵⁷ URL6⁴²⁵⁸ URL7⁴²⁵⁹ URL8⁴²⁶⁰ XF ssl-message-dos(15712)⁴²⁶¹ XF win-asn1-double-free(15713)⁴²⁶² XF win-h323-bo(15710)⁴²⁶³ XF win-hcpurl-code-execution(15704)⁴²⁶⁴ XF win-ldt-gain-privileges(15707)⁴²⁶⁵ XF win-lsass-bo(15699)⁴²⁶⁶ XF win-spp-bo(15715)⁴²⁶⁷ XF win-vdm-gain-privileges(15714)⁴²⁶⁸ XF win-winlogon-bo(15702)⁴²⁶⁹ XF win2k-lsass-ldap-dos(15700)⁴²⁷⁰ XF win2k-utilitymgr-gain-privileges(15632) MS: MS04-011⁴²⁷¹, CVE: CVE-2003-0533⁴²⁷² MSKB: 835732⁴²⁷³		

⁴²⁴⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:907>

⁴²⁴⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:911>

⁴²⁴⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:919>

⁴²⁴⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:924>

⁴²⁴⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:946>

⁴²⁵⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:951>

⁴²⁵¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:959>

⁴²⁵² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:964>

⁴²⁵³ <http://archives.neohapsis.com/archives/vulnwatch/2004-q1/0081.html>

⁴²⁵⁴ <http://archives.neohapsis.com/archives/vulnwatch/2004-q1/0082.html>

⁴²⁵⁵ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020065.html>

⁴²⁵⁶ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020068.html>

⁴²⁵⁷ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020069.html>

⁴²⁵⁸ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020070.html>

⁴²⁵⁹ <http://www.securiteam.com/windowsntfocus/SLP0C2ACKU.html>

⁴²⁶⁰ <http://www.securityfocus.com/archive/1/361836>

⁴²⁶¹ <http://xforce.iss.net/xforce/xfdb/15712>

⁴²⁶² <http://xforce.iss.net/xforce/xfdb/15713>

⁴²⁶³ <http://xforce.iss.net/xforce/xfdb/15710>

⁴²⁶⁴ <http://xforce.iss.net/xforce/xfdb/15704>

⁴²⁶⁵ <http://xforce.iss.net/xforce/xfdb/15707>

⁴²⁶⁶ <http://xforce.iss.net/xforce/xfdb/15699>

⁴²⁶⁷ <http://xforce.iss.net/xforce/xfdb/15715>

⁴²⁶⁸ <http://xforce.iss.net/xforce/xfdb/15714>

⁴²⁶⁹ <http://xforce.iss.net/xforce/xfdb/15702>

⁴²⁷⁰ <http://xforce.iss.net/xforce/xfdb/15700>

⁴²⁷¹ <http://technet.microsoft.com/en-us/security/bulletin/ms04-011>

⁴²⁷² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0533>

			OVAL: OVAL1000 ⁴²⁷⁴ CERT-VN: 753212 ⁴²⁷⁵ CERT-VN: 783748 ⁴²⁷⁶ XF: winxp-task-gain-privileges(15678) ⁴²⁷⁷		
10.	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (windows-hotfixms06-035)	Ovo ažuriranje rešava nekoliko otkrivenih i privatno prijavljenih ranjivosti. Preporučuje se da korisnici odmah primene update.	BID 18863 ⁴²⁸⁰ BID 18891 ⁴²⁸¹ CERT TA06-192A ⁴²⁸² CERT-VN 189140 ⁴²⁸³ CERT-VN 333636 ⁴²⁸⁴ OSVDB 27154 ⁴²⁸⁵ OSVDB 27155 ⁴²⁸⁶ OVAL OVAL3 ⁴²⁸⁷ OVAL OVAL600 ⁴²⁸⁸ CVE: CVE-2006-1314 ⁴²⁸⁹ CVE: VE-2006-1315 ⁴²⁹⁰ MS: MS06-035 ⁴²⁹¹ MSKB: 917159 ⁴²⁹² SANS-06: W4 ⁴²⁹³ SANS-07: S2 ⁴²⁹⁴ SECUNIA: 21007 ⁴²⁹⁵ XF: win-mailslot-bo(26818) ⁴²⁹⁶ XF win-smb-information-disclosure(26820) ⁴²⁹⁷	Kritičan	Uraditi download a zatim instalirati Microsoft patch za 32-bitnu verziju : WindowsXP-KB917159-x86-ENU.exe (725304 bytes) ⁴²⁹⁸ ili za 64-bitnu verziju Windowsa : WindowsServer2003.WindowsXP-KB917159-x64-ENU.exe ⁴²⁹⁹
11.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.109:139 172.23.202.109:445 172.23.202.106:139 172.23.202.106:445 172.23.202.69:139 172.23.202.69:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje omogućava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje	MSKB: 887429 ⁴³⁰⁰ URL1 ⁴³⁰¹	Ozbiljan	Metoda za konfiguracijue SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429 ⁴³⁰² . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB

⁴²⁷³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;835732>⁴²⁷⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1000>⁴²⁷⁵ <http://www.kb.cert.org/vuls/id/753212>⁴²⁷⁶ <http://www.kb.cert.org/vuls/id/783748>⁴²⁷⁷ <http://xforce.iss.net/xforce/xfdb/15678>⁴²⁸⁰ <http://www.securityfocus.com/bid/18863>⁴²⁸¹ <http://www.securityfocus.com/bid/18891>⁴²⁸² <http://www.us-cert.gov/ncas/alerts/ta06-192a>⁴²⁸³ <http://www.kb.cert.org/vuls/id/189140>⁴²⁸⁴ <http://www.kb.cert.org/vuls/id/333636>⁴²⁸⁵ <http://www.osvdb.org/27154>⁴²⁸⁶ <http://www.osvdb.org/27155>⁴²⁸⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3>⁴²⁸⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:600>⁴²⁸⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1314>⁴²⁹⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1315>⁴²⁹¹ <http://technet.microsoft.com/en-us/security/bulletin/ms06-035>⁴²⁹² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;917159>⁴²⁹³ <http://www.sans.org/critical-security-controls/#w4>⁴²⁹⁴ <http://www.sans.org/critical-security-controls/#s2>⁴²⁹⁵ <http://secunia.com/advisories/21007/>⁴²⁹⁶ <http://xforce.iss.net/xforce/xfdb/26818>⁴²⁹⁷ <http://xforce.iss.net/xforce/xfdb/26820>⁴²⁹⁸ http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb917159-x86-enu_5ed838e18ceae61a8d94f8c4be2462a8e19212d7.exe⁴²⁹⁹ <http://download.microsoft.com/download/7/e/3/7e3fa65f-f3bc-49be-8b92-9e19f793933/WindowsServer2003.WindowsXP-KB917159-x64-ENU.exe>⁴³⁰⁰ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429>⁴³⁰¹ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>⁴³⁰² <http://support.microsoft.com/kb/887429>

		može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).			potpisivanje: <i>server signing</i> = <i>auto</i> ili da se zahteva SMB potpisivanje: <i>server signing</i> = <i>mandatory</i> .
12.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.109:139 172.23.202.109:445 172.23.202.106:139 172.23.202.106:445 172.23.202.69:139 172.23.202.69:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti
13.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	172.23.202.109:135 172.23.202.106:135 172.23.202.69:135 Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hедера i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183 ⁴³⁰³ CERT TA04-111A ⁴³⁰⁴ CVE CVE-2004-0230 ⁴³⁰⁵ OSVDB 4030 ⁴³⁰⁶ CERT-VN: 415294 ⁴³⁰⁷ MS: MS05-019 ⁴³⁰⁸ MS: MS06-064 ⁴³⁰⁹ NETBSD: NetBSD-SA2004-006 ⁴³¹⁰ OVAL: OVAL2689 ⁴³¹¹ OVAL: OVAL270 ⁴³¹² OVAL OVAL3508 ⁴³¹³ OVAL OVAL4791 ⁴³¹⁴ OVAL OVAL5711 ⁴³¹⁵ SECUNIA: 11440 ⁴³¹⁶ SECUNIA: 22341 ⁴³¹⁷ SECUNIA 11458 ⁴³¹⁸ SGI 20040403-01-A ⁴³¹⁹ XF tcp-rst-dos(15886) ⁴³²⁰ URL1 ⁴³²¹ URL2 ⁴³²²	Ozbiljan	Uraditi download a zatim instalirati Microsoft patch za 32-bitnu verziju : WindowsXP-KB893066-v2-x86-ENU.exe (791280 bytes) ⁴³²³ ili za 64-bitnu verziju Windowsa : WindowsXP-KB893066-v2-ia64-ENU.exe ⁴³²⁴
14	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server. Ovi anonimni korisnici bi mogli biti u mogućnosti	BID: 494 ⁴³²⁵ CVE: CVE-1999-0519 ⁴³²⁶ MSKB: 143474 ⁴³²⁷ URL1 ⁴³²⁸	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost

⁴³⁰³ <http://www.securityfocus.com/bid/10183>⁴³⁰⁴ <http://www.us-cert.gov/ncas/alerts/ta04-111a>⁴³⁰⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁴³⁰⁶ <http://www.osvdb.org/4030>⁴³⁰⁷ <http://www.kb.cert.org/vuls/id/415294>⁴³⁰⁸ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁴³⁰⁹ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁴³¹⁰ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁴³¹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>⁴³¹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>⁴³¹³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>⁴³¹⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>⁴³¹⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>⁴³¹⁶ <http://secunia.com/advisories/11440/>⁴³¹⁷ <http://secunia.com/advisories/22341/>⁴³¹⁸ <http://secunia.com/advisories/11458/>⁴³¹⁹ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>⁴³²⁰ <http://xforce.iss.net/xforce/xfdb/15886>⁴³²¹ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁴³²² <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>⁴³²³ http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb893066-v2-x86-enu_3d2029a4300c0b7943b20c1287c8143087045d52.exe⁴³²⁴ <http://download.microsoft.com/download/0/6/c/06cda61b-b868-4b3d-a07e-3d60501ac2cb/WindowsXP-KB893066-v2-ia64-ENU.exe>⁴³²⁵ <http://www.securityfocus.com/bid/494>⁴³²⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>⁴³²⁷ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>⁴³²⁸ http://www.hsc.fr/ressources/presentations/null_sessions/

		da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko poziva udaljenih procedura (RPC). Ovi servisi su i u prošlosti bili skloni ranjivostima.. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinjenije napade.			
15.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatišu slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	CVE: CVE-1999-0524 ⁴³²⁹ XF: icmp-netmask(306) ⁴³³⁰ XF: icmp-timestamp(322) ⁴³³¹ OSVDB 95 ⁴³³²	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.

Tabela 109. Windows OS sa IP adresom 172.23.202.107 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.107		OS: Microsoft Windows XP Pro Sp2 x86 IME: WINXPproSP2x86			11
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Microsoft Server Service / CanonicalizePathName() Remote Code Execution Vulnerability (dcerpc-msnetapi-netpathcanonicalize-dos)	Određene verzije Microsoft Windows-a su ranjive na daljinsko preopterećenje bafera (privremene memorije) koje bi moglo da kompromituje određeni računar. Posebno izrađen paket se može koristiti sa pozivom ka NetPathCanonicalize RPC ruti na servisu servera, pri čemu bi napadač mogao da izvrši kôd pod sistemskim nivoom pristupa.	CVE: CVE-2006-3439 ⁴³³³ , MS: MS06-040 ⁴³³⁴ , MSKB: 921883 ⁴³³⁵ , SANS-06: W4 ⁴³³⁶ , SANS-07: S2 ⁴³³⁷	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowXP-KB921883-x86-ENU.EXE ⁴³³⁸
2.	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution	172.23.202.107:139 172.23.202.107:445 Ovo ažuriranje bezbednosti rešava ranjivost koja je prijavljena od strane privatnog lica. Ranjivost bi mogla da	MS: MS08-067 ⁴³³⁹ MSKB: 958644 ⁴³⁴⁰ CVE: CVE-2008-4250 ⁴³⁴¹ SECUNIA: 32326 ⁴³⁴²	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB958644-x86-ENU.exe (648560)

⁴³²⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁴³³⁰ <http://xforce.iss.net/xforce/xfdb/306>⁴³³¹ <http://xforce.iss.net/xforce/xfdb/322>⁴³³² <http://www.osvdb.org/95>⁴³³³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-3439>⁴³³⁴ <http://technet.microsoft.com/en-us/security/bulletin/ms06-040>⁴³³⁵ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;921883>⁴³³⁶ <http://www.sans.org/critical-security-controls/#w4>⁴³³⁷ <http://www.sans.org/critical-security-controls/#s2>⁴³³⁸ download.microsoft.com/download/c/2/b/c2b41862-1113-4e40-a81a-d6971733e361/WindowsXP-KB921883-x86-ENU.exe⁴³³⁹ <http://technet.microsoft.com/en-us/security/bulletin/ms08-067>⁴³⁴⁰ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958644>⁴³⁴¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4250>

	(windows-hotfix-ms08-067)	omogući daljinsko izvršavanje koda ukoliko je napadnuti sistem primio posebno izrađen RPC zahtev. Na sistemima Microsoft Windows 2000, Windows XP, i Windows Server 2003, napadač bi mogao da iskoristi ovu ranjivost bez proveravanja autentičnosti i da pokrene proizvoljan kôd. Moguće je da ova ranjivost može biti upotrebljena za intenziviranje skrivenog korišćenja exploit-a. Praksa je pokazala da upotreba zaštitnog zida može da pomogne u zaštiti mrežnih resursa od napada koji potiču izvan okvira organizacije.	URL1 ⁴³⁴³ URL2 ⁴³⁴⁴ URL3 ⁴³⁴⁵		bytes) ⁴³⁴⁶
3.	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (windows-hotfix-ms09-001)	172.23.202.107:139 172.23.202.107:445 Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti koje su privatno prijavljene a odnose se na protokol Microsoft Server Message Block-a (SMB). Ranjivosti mogu da omoguće daljinsko izvršenje kôda na ugroženim sistemima. Napadač koji je uspešno iskoristion ove ranjivosti može da instalira programe, pregleda, menja ili briše podatke ili otvara nove naloge sa potpunim korisničkim pravima. Praksa je pokazala da zaštitni zid i njegove standardne konfiguracije po difoltu mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan okvira organizacije. Za sisteme koji su stalno povezani na Internet preporuka je da imaju što manji broj izloženih portova.	MS: MS09-001 ⁴³⁴⁷ MSKB: 958687 ⁴³⁴⁸ CVE: CVE-2008-4114 ⁴³⁴⁹ CVE: CVE-2008-4835 ⁴³⁵⁰ CVE: CVE-2008-4834 ⁴³⁵¹ SECUNIA: 31883 ⁴³⁵² URL1 ⁴³⁵³ URL2 ⁴³⁵⁴ URL3 ⁴³⁵⁵	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB958687-x86-ENU.exe (658288 bytes) ⁴³⁵⁶
4.	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-012)	172.23.202.107:139 172.23.202.107:445 Ovo ažuriranje bezbednosti rešava nekoliko privatno prijavljenih ranjivosti na Microsoft Windows-u. Opasnost od ove ranjivosti leži u tome što bi ona omogućila daljinsko izvršavanje kôda ukoliko bi napadač kreirao posebno opremljen SMB	MS: MS10-012 ⁴³⁵⁷ MSKB - 971468 ⁴³⁵⁸ CVE: CVE-2010-0020 ⁴³⁵⁹ CVE: CVE-2010-0021 ⁴³⁶⁰ CVE: CVE-2010-0022 ⁴³⁶¹ CVE CVE-2010-0231 ⁴³⁶²	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB971468-x86-ENU.exe (664952 bytes) ⁴³⁶⁴

⁴³⁴² <http://secunia.com/advisories/32326/>⁴³⁴³ blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx⁴³⁴⁴ <http://blogs.msdn.com/b/sdl/archive/2008/10/22/ms08-067.aspx>⁴³⁴⁵ <http://blogs.technet.com/b/msrc/archive/2008/10/23/ms08-067-released.aspx>⁴³⁴⁶ http://download.windowsupdate.com/msdownload/update/software/secu/2008/10/windowsxpkb958644-x86-enu_5c135a8dae5721849430afe27af255f83e64f62b.exe⁴³⁴⁷ <http://technet.microsoft.com/en-us/security/bulletin/MS09-001>⁴³⁴⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958687>⁴³⁴⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4114>⁴³⁵⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4835>⁴³⁵¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4834>⁴³⁵² <http://secunia.com/advisories/31883/>⁴³⁵³ http://www.vallejo.cc/proyectos/vista_SMB_write_DoS.htm⁴³⁵⁴ <http://www.zerodayinitiative.com/advisories/ZDI-09-001/>⁴³⁵⁵ <http://www.zerodayinitiative.com/advisories/ZDI-09-002/>⁴³⁵⁶ http://download.windowsupdate.com/msdownload/update/software/secu/2008/12/windowsxp-kb958687-x86-enu_a9b85264e9b75e552ae10cd212937b8686a96833.exe⁴³⁵⁷ <http://technet.microsoft.com/en-us/security/bulletin/MS10-012>⁴³⁵⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;971468>⁴³⁵⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0020>⁴³⁶⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0021>⁴³⁶¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0022>⁴³⁶² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0231>

		paket i poslao ga ugroženom sistemu. Dosadašnja praksa fajervola i standardne fajervol difolt konfiguracije mogu da pomognu u zaštiti mrežnih resursa od napada (koji bi pokušali da iskoriste ove ranjivosti), a koji potiču izvan okvira organizacije.	SECUNIA 38510 ⁴³⁶³		
5.	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-054)	172.23.202.107:139 172.23.202.107:445 Opis je isti kao kod ranjivosti MS10-012	CVE: CVE-2010-2550 ⁴³⁶⁵ CVE: CVE-2010-2551 ⁴³⁶⁶ CVE: CVE-2010-2552 ⁴³⁶⁷ MS: MS10-054 ⁴³⁶⁸ MSKB 982214 ⁴³⁶⁹	Kritičan	Uraditi download a zatim instalirati Microsoft patch windowsxp-kb982214-x86-enu.exe (661368 bytes) ⁴³⁷⁰
6.	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms11-020)	172.23.202.107:139 172.23.202.107:445 Opis je isti kao kod ranjivosti MS10-012	CVE: CVE-2011-0661 ⁴³⁷¹ MS: MS11-020 ⁴³⁷² MSKB: 2508429 ⁴³⁷³	Kritičan	Uraditi download a zatim instalirati Microsoft patch windowsxp-kb2508429-x86-enu.exe (664960 bytes) ⁴³⁷⁴
7.	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (windows-hotfixms06-035)	Ovo ažuriranje rešava nekoliko otkrivenih i privatno prijavljenih ranjivosti. Preporučuje se da korisnici odmah primene update.	CVE: CVE-2006-1314 ⁴³⁷⁵ CVE: CVE-2006-1315 ⁴³⁷⁶ MS: MS06-035 ⁴³⁷⁷ MSKB: 917159 ⁴³⁷⁸ SANS-06: W4 ⁴³⁷⁹ SANS-07: S2 ⁴³⁸⁰ SECUNIA: 21007 ⁴³⁸¹ XF: win-mailslot-bo(26818) ⁴³⁸² XF win-smb-information-disclosure(26820) ⁴³⁸³	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB917159-x86-ENU.exe (725304 bytes) ⁴³⁸⁴
8.	SMB signing disabled (cifs-smb-signing-	172.23.202.107:139 172.23.202.107:445	MSKB: 887429 ⁴³⁸⁵ URL1 ⁴³⁸⁶	Ozbiljan	Metoda za konfiguracije SMB potpisivanja je

⁴³⁶⁴ http://download.windowsupdate.com/msdownload/update/software/secu/2010/01/windowsxp-kb971468-x86-enu_68d7899c8b8462219daf40f02c6fb9f362b1ee6b.exe

⁴³⁶³ <http://secunia.com/advisories/38510/>

⁴³⁶⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2550>

⁴³⁶⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2551>

⁴³⁶⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2552>

⁴³⁶⁸ <http://technet.microsoft.com/en-us/security/bulletin/MS10-054>

⁴³⁶⁹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;982214>

⁴³⁷⁰ http://download.windowsupdate.com/msdownload/update/software/secu/2010/07/windowsxp-kb982214-x86-enu_a24853f682dad3157da4e4a39372951a8ec1e407.exe

⁴³⁷¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661>

⁴³⁷² <http://technet.microsoft.com/en-us/security/bulletin/ms11-020>

⁴³⁷³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;2508429>

⁴³⁷⁴ http://download.windowsupdate.com/msdownload/update/software/secu/2011/03/windowsxp-kb2508429-x86-enu_e0b40d81f2ecc1bad43439a6bd0a9e2a0ab7dd56.exe

⁴³⁷⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1314>

⁴³⁷⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1315>

⁴³⁷⁷ <http://technet.microsoft.com/en-us/security/bulletin/ms06-035>

⁴³⁷⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;917159>

⁴³⁷⁹ <http://www.sans.org/critical-security-controls/#w4>

⁴³⁸⁰ <http://www.sans.org/critical-security-controls/#s2>

⁴³⁸¹ <http://secunia.com/advisories/21007/>

⁴³⁸² <http://xforce.iss.net/xforce/xfdb/26818>

⁴³⁸³ <http://xforce.iss.net/xforce/xfdb/26820>

⁴³⁸⁴ http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb917159-x86-enu_5ed838e18ceae61a8d94f8c4be2462a8e19212d7.exe

⁴³⁸⁵ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429>

⁴³⁸⁶ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>

	disabled)	Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje omogućava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).			specifična za svaki sistem i opisana je u KB 887429 ⁴³⁸⁷ . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing</i> = <i>auto</i> ili da se zahteva SMB potpisivanje: <i>server signing</i> = <i>mandatory</i> .
9.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.107:139 172.23.202.107:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti
10.	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server. Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko poziva udaljenih procedura (RPC). Ovi servisi su i u prošlosti bili skloni ranjivostima.. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinjenije napade.	BID: 494 ⁴³⁸⁸ CVE: CVE-1999-0519 ⁴³⁸⁹ MSKB: 143474 ⁴³⁹⁰ URL1 ⁴³⁹¹	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost
11.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	CVE: CVE-1999-0524 ⁴³⁹² XF: netmask(306) ⁴³⁹³ icmp- XF: icmp-timestamp(322) ⁴³⁹⁴	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.

Tabela 110. Windows OS sa IP adresama 172.23.202.110, 172.23.202.76 (2013. godina)

Datum: 20.08.2013	Operativni sistem i ime računara	Broj ranjivosti

⁴³⁸⁷ <http://support.microsoft.com/kb/887429>⁴³⁸⁸ <http://www.securityfocus.com/bid/494>⁴³⁸⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>⁴³⁹⁰ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>⁴³⁹¹ http://www.hsc.fr/ressources/presentations/null_sessions/⁴³⁹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁴³⁹³ <http://xforce.iss.net/xforce/xfdb/306>⁴³⁹⁴ <http://xforce.iss.net/xforce/xfdb/322>

IP adresa: 172.23.202.110		OS: Microsoft Windows 2000 Advanced server Sp4, WIN2000ADVsp4			19
IP adresa: 172.23.202.76		OS: Windows 2000 server Sp4, Win2000srvsp4			19
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Microsoft Server Service / CanonicalizePathName() Remote Code Execution Vulnerability (dcerpc-msnetapi-netpathcanonicalize-dos)	Određene verzije Microsoft Windows-a su ranjive na daljinsko preopterećenje bafera (privremene memorije) koje bi moglo da kompromituje određeni računar. Posebno izrađen paket se može koristiti sa pozivom ka NetPathCanonicalize RPC ruti na servisu servera, pri čemu bi napadač mogao da izvrši kôd pod sistemskim nivoom pristupa.	BID 19409 ⁴³⁹⁵ CERT TA06-220A ⁴³⁹⁶ CERT-VN 650769 ⁴³⁹⁷ CVE CVE-2006-3439 ⁴³⁹⁸ MS MS06-040 ⁴³⁹⁹ OVAL OVAL492 ⁴⁴⁰⁰ SECUNIA 21388 ⁴⁴⁰¹ XF ms-server-service-bo(28002) ⁴⁴⁰²	Kritičan	Uraditi download a zatim instalirati Microsoft patch WinDOWS2000-KB921883-x86-ENU.EXE ⁴⁴⁰³
2.	MS03-039: Buffer Overrun In RPCSS Service Could Allow Code Execution (824146) (windows-hotfix-ms03-039)	Napadač koji bi uspešno iskoristio ove ranjivosti mogao bi da pokrene kôd sa privilegijama lokalnog sistema na napadnutom sistemu, ili bi mogao da prouzrokuje isključenje RPCSS servisa. Napadač bi tada bio u mogućnosti da preduzme bilo kakvu akciju na sistemu, uključujući instaliranje programa, pregledanje, menjanje ili brisanje podataka ili otvaranje novih naloga sa svih privilegijama. Da bi iskoristio ove ranjivosti, napadač bi mogao da kreira program koji bi poslao malicioznu RPC poruku ranjivom sistemu, ciljajući na RPCSS servis.	BID: 8458 ⁴⁴⁰⁴ , CVE: CVE-2003-0528 ⁴⁴⁰⁵ , CVE: CVE-2003-0605 ⁴⁴⁰⁶ , CVE: CVE-2003-0715 ⁴⁴⁰⁷ , MSKB: 824146 ⁴⁴⁰⁸ , MS:MS03-039 ⁴⁴⁰⁹ , CERT CA-2003-19 ⁴⁴¹⁰ CERT CA-2003-23 ⁴⁴¹¹ CERT-VN 254236 ⁴⁴¹² CERT-VN 326746 ⁴⁴¹³ CERT-VN 483492 ⁴⁴¹⁴ CVE CVE-2003-0995 ⁴⁴¹⁵ OVAL OVAL1118 ⁴⁴¹⁶ OVAL OVAL1202 ⁴⁴¹⁷ OVAL OVAL127 ⁴⁴¹⁸ OVAL OVAL1813 ⁴⁴¹⁹ OVAL OVAL20 ⁴⁴²⁰ OVAL OVAL264 ⁴⁴²¹ OVAL OVAL2884 ⁴⁴²²	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows2000-KB824146-x86-ENU.exe (938856 bytes) ⁴⁴²⁸ Uraditi download a zatim instalirati Microsoft patch DirectX9-KB819696-x86-ENU.exe (970312 bytes) ⁴⁴²⁹

⁴³⁹⁵ <http://www.securityfocus.com/bid/19409>⁴³⁹⁶ <http://www.us-cert.gov/ncas/alerts/ta06-220a>⁴³⁹⁷ <http://www.kb.cert.org/vuls/id/650769>⁴³⁹⁸ <http://nvd.nist.gov/?vulnId=CVE-2006-3439>⁴³⁹⁹ <http://technet.microsoft.com/en-us/security/bulletin/ms06-040>⁴⁴⁰⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:492>⁴⁴⁰¹ <http://secunia.com/advisories/21388/>⁴⁴⁰² <http://xforce.iss.net/xforce/xfdb/28002>⁴⁴⁰³ download.microsoft.com/download/9/0/b/90b8dbba-09c1-4b27-b0c4-0cc13706823a/Windows2000-KB921883-x86-ENU.EXE⁴⁴⁰⁴ <http://www.securityfocus.com/bid/8458>⁴⁴⁰⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0528>⁴⁴⁰⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0605>⁴⁴⁰⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0715>⁴⁴⁰⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;824146>⁴⁴⁰⁹ <http://technet.microsoft.com/en-us/security/bulletin/ms03-039>⁴⁴¹⁰ <http://www.us-cert.gov/ncas/alerts/ca-2003-19>⁴⁴¹¹ <http://www.us-cert.gov/ncas/alerts/ca-2003-23>⁴⁴¹² <http://www.kb.cert.org/vuls/id/254236>⁴⁴¹³ <http://www.kb.cert.org/vuls/id/326746>⁴⁴¹⁴ <http://www.kb.cert.org/vuls/id/483492>⁴⁴¹⁵ <http://nvd.nist.gov/?vulnId=CVE-2003-0995>⁴⁴¹⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1118>⁴⁴¹⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1202>⁴⁴¹⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:127>⁴⁴¹⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1813>⁴⁴²⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:20>⁴⁴²¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:264>⁴⁴²² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2884>

			OVAL OVAL2968⁴⁴²³ OVAL OVAL3966⁴⁴²⁴ OVAL OVAL4224⁴⁴²⁵ OVAL OVAL494⁴⁴²⁶ XF win2k-message-queue-bo(13131)⁴⁴²⁷		
3.	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (windows-hotfix-ms08-067)	172.23.202.110:139 172.23.202.110:445 Ova bezbednosna ispravka rešava ranjivost koja je prijavljena od strane privatnog lica. Ranjivost bi mogla da omogući daljinsko izvršavanje koda ukoliko je napadnuti sistem primio posebno opremljeni RPC zahtev. Na sistemima Microsoft Windows 2000, Windows XP, i Windows Server 2003, napadač bi mogao da iskoristi ovu ranjivost bez overavanja autentičnosti i da pokrene proizvoljan kôd. Moguće je da ova ranjivost može biti upotrebljena za intenziviranje skrivenog korišćenja. Najbolje prakse zaštitnog zida i standardne konfiguracije zaštitnog zida po difoltu mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan okvira preduzeća.	BID 31874⁴⁴³⁰ CERT TA08-297A⁴⁴³¹ CERT TA09-088A⁴⁴³² CERT-VN 827267⁴⁴³³ IAVM 2008-A-0081⁴⁴³⁴ OVAL OVAL6093⁴⁴³⁵ XF 46040⁴⁴³⁶ MS: MS08-067⁴⁴³⁷ MSKB: 958644⁴⁴³⁸ CVE: CVE-2008-4250⁴⁴³⁹ SECUNIA: 32326⁴⁴⁴⁰ URL1⁴⁴⁴¹ URL2⁴⁴⁴² URL3⁴⁴⁴³ URL4⁴⁴⁴⁴	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows2000-KB958644-x86-ENU.EXE (618024 bytes) ⁴⁴⁴⁵
4.	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (windows-hotfix-ms09-001)	172.23.202.110:139 172.23.202.110:445 Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti koje su privatno prijavljene, a odnose se na Microsoft Server Message Block (SMB). Ranjivosti mogu da omoguće daljinsko izvršenje koda na ugroženim sistemima. Napadač	BID 31179⁴⁴⁴⁶ BID 33121⁴⁴⁴⁷ BID 33122⁴⁴⁴⁸ CERT TA09-013A⁴⁴⁴⁹ OVAL OVAL5248⁴⁴⁵⁰ OVAL OVAL5262⁴⁴⁵¹ OVAL OVAL5863⁴⁴⁵² OVAL OVAL6044⁴⁴⁵³	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows2000-KB958687-x86-ENU.EXE (617512 bytes) ⁴⁴⁶⁴

⁴⁴²⁸ http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windows2000-kb824146-x86-enu_dcf74565af2d26e87ef7cf974f03c30.exe

⁴⁴²⁹ http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/directx9-kb819696-x86-enu_977f8cc86c1e151a0168d1296210913.exe

⁴⁴²³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2968>

⁴⁴²⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3966>

⁴⁴²⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4224>

⁴⁴²⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:494>

⁴⁴²⁷ <http://xforce.iss.net/xforce/xfdb/13131>

⁴⁴³⁰ <http://www.securityfocus.com/bid/31874>

⁴⁴³¹ <http://www.us-cert.gov/ncas/alerts/ta08-297a>

⁴⁴³² <http://www.us-cert.gov/ncas/alerts/ta09-088a>

⁴⁴³³ <http://www.kb.cert.org/vuls/id/827267>

⁴⁴³⁴ <http://iase.disa.mil/stigs/iavm-cve.html>

⁴⁴³⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6093>

⁴⁴³⁶ <http://xforce.iss.net/xforce/xfdb/46040>

⁴⁴³⁷ <http://technet.microsoft.com/en-us/security/bulletin/ms08-067>

⁴⁴³⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958644>

⁴⁴³⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4250>

⁴⁴⁴⁰ <http://secunia.com/advisories/32326/>

⁴⁴⁴¹ blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx

⁴⁴⁴² <http://blogs.msdn.com/b/sdl/archive/2008/10/22/ms08-067.aspx>

⁴⁴⁴³ <http://blogs.technet.com/b/msrc/archive/2008/10/23/ms08-067-released.aspx>

⁴⁴⁴⁴ <http://technet.microsoft.com/en-us/security/bulletin/MS08-067>

⁴⁴⁴⁵ http://download.windowsupdate.com/msdownload/update/software/secu/2008/10/windows2000-kb958644-x86-enu_32416827ab7de148e5e7998e6e1f4c3b16fa4719.exe

⁴⁴⁴⁶ <http://www.securityfocus.com/bid/31179>

⁴⁴⁴⁷ <http://www.securityfocus.com/bid/33121>

⁴⁴⁴⁸ <http://www.securityfocus.com/bid/33122>

⁴⁴⁴⁹ <http://www.us-cert.gov/ncas/alerts/ta09-013a>

⁴⁴⁵⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5248>

⁴⁴⁵¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5262>

⁴⁴⁵² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5863>

⁴⁴⁵³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6044>

		koji je uspešno iskoristion ove ranjivosti može da instalira programe, pregleda, menja ili briše podatke ili otvara nove naloge sa potpunim korisničkim pravima. Najbolje prakse zaštitnog zida i standardne konfiguracije zaštitnog zida po difoltu mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan okvira preduzeća. Za sisteme koji su stalno povezani na Internet preporuka je da imaju što manji broj izloženih portova.	XF 45146 ⁴⁴⁵⁴ MS: MS09-001 ⁴⁴⁵⁵ MSKB: 958687 ⁴⁴⁵⁶ CVE: CVE-2008-4114 ⁴⁴⁵⁷ CVE: CVE-2008-4835 ⁴⁴⁵⁸ CVE: CVE-2008-4834 ⁴⁴⁵⁹ SECUNIA: 31883 ⁴⁴⁶⁰ URL1 ⁴⁴⁶¹ URL2 ⁴⁴⁶² URL3 ⁴⁴⁶³		
5.	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-012)	172.23.202.110:139 172.23.202.110:445 Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti koje su privatno prijavljene u Microsoft Windows-u. Opasnost od ove ranjivosti leži u tome što bi ona omogućila daljinsko izvršavanje kôda ukoliko bi napadač kreirao posebno opremljeni SMB paket i poslao ga ugroženom sistemu. Praksa je pokazala da upotreba zaštitnog zida može da pomogne u zaštiti mrežnih resursa od napada (koji bi pokušali da iskoriste ove ranjivosti), a koji potiču izvan okvira organizacije.	CERT TA10-040A ⁴⁴⁶⁵ OVAL OVAL7751 ⁴⁴⁶⁶ OVAL OVAL8314 ⁴⁴⁶⁷ OVAL OVAL8438 ⁴⁴⁶⁸ OVAL OVAL8524 ⁴⁴⁶⁹ MS: MS10-012 ⁴⁴⁷⁰ MSKB - 971468 ⁴⁴⁷¹ CVE: CVE-2010-0020 ⁴⁴⁷² CVE: CVE-2010-0021 ⁴⁴⁷³ CVE: CVE-2010-0022 ⁴⁴⁷⁴ CVE CVE-2010-0231 ⁴⁴⁷⁵	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows2000-KB971468-x86-ENU.EXE (621304 bytes) ⁴⁴⁷⁶
6.	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-054)	172.23.202.110:139 172.23.202.110:445 Opis je isti kao kod ranjivosti MS10-012.	CERT TA10-222A ⁴⁴⁷⁷ OVAL OVAL11106 ⁴⁴⁷⁸ OVAL OVAL12015 ⁴⁴⁷⁹ OVAL OVAL12072 ⁴⁴⁸⁰ CVE: CVE-2010-2550 ⁴⁴⁸¹	Kritičan	Blokirati portove 139 i 445 na spoljnom fajervolu. Treba imati u vidu da će ova ranjivost takođe uticati na sisteme Windows 2000, a usled zastarevanja Windows 2000; ne postoji odgovarajuća zakrpa koja bi

⁴⁴⁶⁴ http://download.windowsupdate.com/msdownload/update/software/secu/2008/12/windows2000-kb958687-x86-enu_f0ce8f2df0b10e58fb8c5ee278153eae03ad4ac6.exe

⁴⁴⁵⁴ <http://xforce.iss.net/xforce/xfdb/45146>

⁴⁴⁵⁵ <http://technet.microsoft.com/en-us/security/bulletin/MS09-001>

⁴⁴⁵⁶ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958687>

⁴⁴⁵⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4114>

⁴⁴⁵⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4835>

⁴⁴⁵⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4834>

⁴⁴⁶⁰ <http://secunia.com/advisories/31883/>

⁴⁴⁶¹ http://www.vallejo.cc/proyectos/vista_SMB_write_DoS.htm

⁴⁴⁶² <http://www.zerodayinitiative.com/advisories/ZDI-09-001/>

⁴⁴⁶³ <http://www.zerodayinitiative.com/advisories/ZDI-09-002/>

⁴⁴⁶⁵ <http://www.us-cert.gov/ncas/alerts/ta10-040a>

⁴⁴⁶⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7751>

⁴⁴⁶⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8314>

⁴⁴⁶⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8438>

⁴⁴⁶⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8524>

⁴⁴⁷⁰ <http://technet.microsoft.com/en-us/security/bulletin/MS10-012>

⁴⁴⁷¹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;971468>

⁴⁴⁷² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0020>

⁴⁴⁷³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0021>

⁴⁴⁷⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0022>

⁴⁴⁷⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0231>

⁴⁴⁷⁶ http://download.windowsupdate.com/msdownload/update/software/secu/2010/01/windows2000-kb971468-x86-enu_d951943f14a5e6e52fbbbed11ae55882c685795c.exe

⁴⁴⁷⁷ <http://www.us-cert.gov/ncas/alerts/ta10-222a>

⁴⁴⁷⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11106>

⁴⁴⁷⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12015>

⁴⁴⁸⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12072>

⁴⁴⁸¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2550>

			CVE: CVE-2010-2551 ⁴⁴⁸² CVE: CVE-2010-2552 ⁴⁴⁸³ MS: MS10-054 ⁴⁴⁸⁴ MSKB 982214 ⁴⁴⁸⁵		omogućila ublažavanje ove ranjivosti.
7.	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms11-020)	172.23.202.110:139 172.23.202.110:445 Opis je isti kao kod ranjivosti MS10-012	BID 47198 ⁴⁴⁸⁶ CERT TA11-102A ⁴⁴⁸⁷ IAVM 2011-A-0050 ⁴⁴⁸⁸ OSVDB 71781 ⁴⁴⁸⁹ OVAL OVAL12076 ⁴⁴⁹⁰ SECUNIA 44072 ⁴⁴⁹¹ CVE: CVE-2011-0661 ⁴⁴⁹² MS: MS11-020 ⁴⁴⁹³ MSKB: 2508429 ⁴⁴⁹⁴	Kritičan	Blokirati portove 139 i 445 na spoljnom fajervolu. Treba imati u vidu da će ova ranjivost takođe uticati na sisteme Windows 2000, a usled zastarevanja Windows 2000; ne postoji odgovarajuća zakrpa koja bi omogućila ublažavanje ove ranjivosti.
8.	Obsolete Version of Microsoft Windows 2000 (windows-2000-obsolete)	Proširena podrška za sve verzije Windows 2000 se završila 13. jula 2010. Verzije koje se ne podržavaju mogu da sadrže nezakrpljene propuste. Nadograditi na verziju koja je podržana.	URL1 ⁴⁴⁹⁵ URL2 ⁴⁴⁹⁶ URL3 ⁴⁴⁹⁷ URL4 ⁴⁴⁹⁸	Kritičan	Nadograditi na verziju Microsoft Windows-a koja je podržana.
9.	Anonymous users can obtain the Windows password policy (cifs-nt-0002)	Korišćenjem CIFS NULL sesije, anonimni korisnik može da dobije uvid u polisu šifri. Polisa šifri sadrži osetljive informacije o najmanjoj mogućoj dužini lozinke, zaključavanje šifre, vremensko trajanje zaključanosti šifre itd.	SANS-01 W5 ⁴⁴⁹⁹ CVE CVE-2000-1200 ⁴⁵⁰⁰ MSKB 143474 ⁴⁵⁰¹ XF nt-lsa-domain-sid(4015) ⁴⁵⁰² MSKB 823659 ⁴⁵⁰³ MSKB 246261 ⁴⁵⁰⁴ MSKB 129457 ⁴⁵⁰⁵ SANS-02 W5 ⁴⁵⁰⁶ BID 959 ⁴⁵⁰⁷ SANS-04 W3 ⁴⁵⁰⁸ SANS-03 W5 ⁴⁵⁰⁹ BID 87 ⁴⁵¹⁰	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost.

⁴⁴⁸² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2551>⁴⁴⁸³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2552>⁴⁴⁸⁴ <http://technet.microsoft.com/en-us/security/bulletin/MS10-054>⁴⁴⁸⁵ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;982214>⁴⁴⁸⁶ <http://www.securityfocus.com/bid/47198>⁴⁴⁸⁷ <http://www.us-cert.gov/ncas/alerts/ta11-102a>⁴⁴⁸⁸ <http://iase.disa.mil/stigs/iavm-cve.html>⁴⁴⁸⁹ <http://www.osvdb.org/71781>⁴⁴⁹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12076>⁴⁴⁹¹ <http://secunia.com/advisories/44072/>⁴⁴⁹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661>⁴⁴⁹³ <http://technet.microsoft.com/en-us/security/bulletin/ms11-020>⁴⁴⁹⁴ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;2508429>⁴⁴⁹⁵ <http://support.microsoft.com/common/international.aspx?RDPATH=%2flifecycle%2fdefault.aspx%3fp1%3d3071>⁴⁴⁹⁶ <http://support.microsoft.com/common/international.aspx?RDPATH=%2flifecycle%2fdefault.aspx%3fp1%3d7017>⁴⁴⁹⁷ <http://support.microsoft.com/common/international.aspx?RDPATH=%2flifecycle%2fdefault.aspx%3fp1%3d7274>⁴⁴⁹⁸ <http://support.microsoft.com/common/international.aspx?RDPATH=%2flifecycle%2fdefault.aspx%3fp1%3d7936>⁴⁴⁹⁹ <http://www.sans.org/critical-security-controls/#w5>⁴⁵⁰⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2000-1200>⁴⁵⁰¹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>⁴⁵⁰² <http://xforce.iss.net/xforce/xfdb/4015>⁴⁵⁰³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;823659>⁴⁵⁰⁴ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;246261>⁴⁵⁰⁵ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;129457>⁴⁵⁰⁶ <http://www.sans.org/critical-security-controls/#w5>⁴⁵⁰⁷ <http://www.securityfocus.com/bid/959>⁴⁵⁰⁸ <http://www.sans.org/critical-security-controls/#w3>⁴⁵⁰⁹ <http://www.sans.org/critical-security-controls/#w5>⁴⁵¹⁰ <http://www.securityfocus.com/bid/87>

10.	MS03-026: Buffer Overrun In RPC Interface Could Allow Code Execution (823980) (windows-hotfix-ms03-026)	Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti u Windows Distributed Component Object Model (DCOM) Remote Procedure Call (RPC). Napadač koji uspešno iskoristi ovu ranjivost, bio bi u mogućnosti da pokrene kôd sa privilegijama lokalnog sistema na napadnutom sistemu. Napadač bi bio u mogućnosti da preduzme bilo kakvu akciju na sistemu, uključujući instaliranje programa, pregledanje, menjanje ili brisanje podataka, ili pak kreiranje novih naloga sa svim privilegijama. Da bi iskoristio ovu ranjivost, napadač bi morao da pošalje posebno kreiran zahtev udaljenom kompjuteru na specifične RPC portove.	CERT CA-2003-16 ⁴⁵¹¹ CERT CA-2003-19 ⁴⁵¹² CERT-VN 568148 ⁴⁵¹³ OVAL OVAL194 ⁴⁵¹⁴ OVAL OVAL2343 ⁴⁵¹⁵ OVAL OVAL296 ⁴⁵¹⁶ XF win-rpc-dcom-bo(12629) ⁴⁵¹⁷ CVE: CVE-2003-0352 ⁴⁵¹⁸ MS: MS03-026 ⁴⁵¹⁹ BID: 8205 ⁴⁵²⁰ MSKB: 823980 ⁴⁵²¹	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows2000-KB823980-x86-ENU.exe ⁴⁵²²
11.	MS04-011: Security Update for Microsoft Windows (835732) (windows-hotfix-ms04-011)	172.23.202.110:139 172.23.202.110:445 Ovo ažuriranje rešava nekoliko novootkrivenih ranjivosti. Napadač koji uspešno iskoristi ovu ranjivost bi mogao da preuzme potpunu kontrolu nad napadnutim sistemom, uključujući instaliranje programa, pregledanje, menjanje ili brisanje podataka ili čak otvaranje novih naloga sa svim privilegijama.	BID 10108 ⁴⁵²³ BID 10113 ⁴⁵²⁴ BID 10114 ⁴⁵²⁵ BID 10115 ⁴⁵²⁶ BID 10117 ⁴⁵²⁷ BID 10118 ⁴⁵²⁸ BID 10119 ⁴⁵²⁹ BID 10120 ⁴⁵³⁰ BID 10122 ⁴⁵³¹ BID 10124 ⁴⁵³² BID 10125 ⁴⁵³³ BID 10126 ⁴⁵³⁴ CERT-VN 122076 ⁴⁵³⁵ CERT-VN 150236 ⁴⁵³⁶ CERT-VN 206468 ⁴⁵³⁷ CERT-VN 255924 ⁴⁵³⁸ CERT-VN 260588 ⁴⁵³⁹ CERT-VN 353956 ⁴⁵⁴⁰ CERT-VN 471260 ⁴⁵⁴¹ CERT-VN 526084 ⁴⁵⁴² CERT-VN 547028 ⁴⁵⁴³	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows2000-KB835732-x86-ENU ⁴⁶¹⁸

⁴⁵¹¹ <http://www.us-cert.gov/ncas/alerts/ca-2003-16>⁴⁵¹² <http://www.us-cert.gov/ncas/alerts/ca-2003-19>⁴⁵¹³ <http://www.kb.cert.org/vuls/id/568148>⁴⁵¹⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:194>⁴⁵¹⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2343>⁴⁵¹⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:296>⁴⁵¹⁷ <http://xforce.iss.net/xforce/xfdb/12629>⁴⁵¹⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0352>⁴⁵¹⁹ <http://technet.microsoft.com/en-us/security/bulletin/ms03-026>⁴⁵²⁰ <http://www.securityfocus.com/bid/8205>⁴⁵²¹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;823980>⁴⁵²² download.microsoft.com/download/0/1/f/01fdd40f-efc5-433d-8ad2-b4b9d42049d5/windows2000-kb823980-x86-enu.exe⁴⁵²³ <http://www.securityfocus.com/bid/10108>⁴⁵²⁴ <http://www.securityfocus.com/bid/10113>⁴⁵²⁵ <http://www.securityfocus.com/bid/10114>⁴⁵²⁶ <http://www.securityfocus.com/bid/10115>⁴⁵²⁷ <http://www.securityfocus.com/bid/10117>⁴⁵²⁸ <http://www.securityfocus.com/bid/10118>⁴⁵²⁹ <http://www.securityfocus.com/bid/10119>⁴⁵³⁰ <http://www.securityfocus.com/bid/10120>⁴⁵³¹ <http://www.securityfocus.com/bid/10122>⁴⁵³² <http://www.securityfocus.com/bid/10124>⁴⁵³³ <http://www.securityfocus.com/bid/10125>⁴⁵³⁴ <http://www.securityfocus.com/bid/10126>⁴⁵³⁵ <http://www.kb.cert.org/vuls/id/122076>⁴⁵³⁶ <http://www.kb.cert.org/vuls/id/150236>⁴⁵³⁷ <http://www.kb.cert.org/vuls/id/206468>⁴⁵³⁸ <http://www.kb.cert.org/vuls/id/255924>⁴⁵³⁹ <http://www.kb.cert.org/vuls/id/260588>⁴⁵⁴⁰ <http://www.kb.cert.org/vuls/id/353956>⁴⁵⁴¹ <http://www.kb.cert.org/vuls/id/471260>⁴⁵⁴² <http://www.kb.cert.org/vuls/id/526084>

			CERT-VN 586540 ⁴⁵⁴⁴ CERT-VN 638548 ⁴⁵⁴⁵ CERT-VN 639428 ⁴⁵⁴⁶ CVE CVE-2003-0663 ⁴⁵⁴⁷ CVE CVE-2003-0719 ⁴⁵⁴⁸ CVE CVE-2003-0806 ⁴⁵⁴⁹ CVE CVE-2003-0906 ⁴⁵⁵⁰ CVE CVE-2003-0907 ⁴⁵⁵¹ CVE CVE-2003-0908 ⁴⁵⁵² CVE CVE-2003-0909 ⁴⁵⁵³ CVE CVE-2003-0910 ⁴⁵⁵⁴ CVE CVE-2004-0117 ⁴⁵⁵⁵ CVE CVE-2004-0118 ⁴⁵⁵⁶ CVE CVE-2004-0119 ⁴⁵⁵⁷ CVE CVE-2004-0120 ⁴⁵⁵⁸ CVE CVE-2004-0123 ⁴⁵⁵⁹ OVAL OVAL1004 ⁴⁵⁶⁰ OVAL OVAL1007 ⁴⁵⁶¹ OVAL OVAL1016 ⁴⁵⁶² OVAL OVAL1046 ⁴⁵⁶³ OVAL OVAL1054 ⁴⁵⁶⁴ OVAL OVAL1064 ⁴⁵⁶⁵ OVAL OVAL1076 ⁴⁵⁶⁶ OVAL OVAL1093 ⁴⁵⁶⁷ OVAL OVAL1512 ⁴⁵⁶⁸ OVAL OVAL1718 ⁴⁵⁶⁹ OVAL OVAL1808 ⁴⁵⁷⁰		

⁴⁵⁴³ <http://www.kb.cert.org/vuls/id/547028>⁴⁶¹⁸ download.microsoft.com/download/F/A/A/FAA796AA-399D-437A-9284-C3536E9F2E6E/Windows2000-KB835732-x86-ENU.EXE⁴⁵⁴⁴ <http://www.kb.cert.org/vuls/id/586540>⁴⁵⁴⁵ <http://www.kb.cert.org/vuls/id/638548>⁴⁵⁴⁶ <http://www.kb.cert.org/vuls/id/639428>⁴⁵⁴⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0663>⁴⁵⁴⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0719>⁴⁵⁴⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0806>⁴⁵⁵⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0906>⁴⁵⁵¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0907>⁴⁵⁵² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0908>⁴⁵⁵³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0909>⁴⁵⁵⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0910>⁴⁵⁵⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0117>⁴⁵⁵⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0118>⁴⁵⁵⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0119>⁴⁵⁵⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0120>⁴⁵⁵⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0123>⁴⁵⁶⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1004>⁴⁵⁶¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1007>⁴⁵⁶² oval.mitre.org/oval/definitions/data/OVAL1016.html⁴⁵⁶³ oval.mitre.org/oval/definitions/data/OVAL1046.html⁴⁵⁶⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1054>⁴⁵⁶⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1064>⁴⁵⁶⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1076>⁴⁵⁶⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1093>⁴⁵⁶⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1512>⁴⁵⁶⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1718>⁴⁵⁷⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1808>

			OVAL OVAL1962 ⁴⁵⁷¹ OVAL OVAL1997 ⁴⁵⁷² OVAL OVAL883 ⁴⁵⁷³ OVAL OVAL885 ⁴⁵⁷⁴ OVAL OVAL886 ⁴⁵⁷⁵ OVAL OVAL889 ⁴⁵⁷⁶ OVAL OVAL890 ⁴⁵⁷⁷ OVAL OVAL892 ⁴⁵⁷⁸ OVAL OVAL895 ⁴⁵⁷⁹ OVAL OVAL896 ⁴⁵⁸⁰ OVAL OVAL897 ⁴⁵⁸¹ OVAL OVAL898 ⁴⁵⁸² OVAL OVAL903 ⁴⁵⁸³ OVAL OVAL904 ⁴⁵⁸⁴ OVAL OVAL907 ⁴⁵⁸⁵ OVAL OVAL911 ⁴⁵⁸⁶ OVAL OVAL919 ⁴⁵⁸⁷ OVAL OVAL924 ⁴⁵⁸⁸ OVAL OVAL946 ⁴⁵⁸⁹ OVAL OVAL951 ⁴⁵⁹⁰ OVAL OVAL959 ⁴⁵⁹¹ OVAL OVAL964 ⁴⁵⁹² URL1 ⁴⁵⁹³ URL2 ⁴⁵⁹⁴ URL3 ⁴⁵⁹⁵ URL4 ⁴⁵⁹⁶ URL5 ⁴⁵⁹⁷ URL6 ⁴⁵⁹⁸ URL7 ⁴⁵⁹⁹ URL8 ⁴⁶⁰⁰ XF ssl-message- dos(15712) ⁴⁶⁰¹ XF win-asn1-double- free(15713) ⁴⁶⁰² XF win-h323- bo(15710) ⁴⁶⁰³		

⁴⁵⁷¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1962>

⁴⁵⁷² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1997>

⁴⁵⁷³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:883>

⁴⁵⁷⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:885>

⁴⁵⁷⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:886>

⁴⁵⁷⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:889>

⁴⁵⁷⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:890>

⁴⁵⁷⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:892>

⁴⁵⁷⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:895>

⁴⁵⁸⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:896>

⁴⁵⁸¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:897>

⁴⁵⁸² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:898>

⁴⁵⁸³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:903>

⁴⁵⁸⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:904>

⁴⁵⁸⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:907>

⁴⁵⁸⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:911>

⁴⁵⁸⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:919>

⁴⁵⁸⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:924>

⁴⁵⁸⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:946>

⁴⁵⁹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:951>

⁴⁵⁹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:959>

⁴⁵⁹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:964>

⁴⁵⁹³ <http://archives.neohapsis.com/archives/vulnwatch/2004-q1/0081.html>

⁴⁵⁹⁴ <http://archives.neohapsis.com/archives/vulnwatch/2004-q1/0082.html>

⁴⁵⁹⁵ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020065.html>

⁴⁵⁹⁶ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020068.html>

⁴⁵⁹⁷ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020069.html>

⁴⁵⁹⁸ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020070.html>

⁴⁵⁹⁹ <http://www.securiteam.com/windowsntfocus/5LP0C2ACKU.html>

⁴⁶⁰⁰ <http://www.securityfocus.com/archive/1/361836>

⁴⁶⁰¹ <http://xforce.iss.net/xforce/xfdb/15712>

⁴⁶⁰² <http://xforce.iss.net/xforce/xfdb/15713>

⁴⁶⁰³ <http://xforce.iss.net/xforce/xfdb/15710>

			XF win-hcpurl-code-execution(15704)⁴⁶⁰⁴ XF win-ldt-gain-privileges(15707)⁴⁶⁰⁵ XF win-lsass-bo(15699)⁴⁶⁰⁶ XF win-spp-bo(15715)⁴⁶⁰⁷ XF win-vdm-gain-privileges(15714)⁴⁶⁰⁸ XF win-winlogon-bo(15702)⁴⁶⁰⁹ XF win2k-lsass-ldap-dos(15700)⁴⁶¹⁰ XF win2k-utilitymgr-gain-privileges(15632) MS: MS04-011⁴⁶¹¹, CVE: CVE-2003-0533⁴⁶¹² MSKB: 835732⁴⁶¹³ OVAL: OVAL1000⁴⁶¹⁴ CERT-VN: 753212⁴⁶¹⁵ CERT-VN: 783748⁴⁶¹⁶ XF: winxp-task-gain-privileges(15678)⁴⁶¹⁷		
12.	MS05-051: Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution (902400) (windowshotfix-ms05-051)	Ovo ažuriranje rešava nekoliko novootkrivenih ranjivosti. Napadač koji uspešno iskoristi ovu ranjivost bi mogao da preuzme potpunu kontrolu nad napadnutim sistemom, uključujući instaliranje programa, pregledanje, menjanje ili brisanje podataka ili čak otvaranje novih naloga sa svim privilegijama.	BID 15056⁴⁶¹⁹ BID 15057⁴⁶²⁰ BID 15058⁴⁶²¹ BID 15059⁴⁶²² CERT TA05-284A⁴⁶²³ CERT-VN 180868⁴⁶²⁴ CERT-VN 950516⁴⁶²⁵ CVE CVE-2005-1978⁴⁶²⁶ CVE CVE-2005-1979⁴⁶²⁷ CVE CVE-2005-1980⁴⁶²⁸ CVE CVE-2005-2119⁴⁶²⁹ MS MS05-051⁴⁶³⁰	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows2000-KB902400-x86-ENU.EXE (5417976 bytes) ⁴⁶⁶¹

⁴⁶⁰⁴ <http://xforce.iss.net/xforce/xfdb/15704>⁴⁶⁰⁵ <http://xforce.iss.net/xforce/xfdb/15707>⁴⁶⁰⁶ <http://xforce.iss.net/xforce/xfdb/15699>⁴⁶⁰⁷ <http://xforce.iss.net/xforce/xfdb/15715>⁴⁶⁰⁸ <http://xforce.iss.net/xforce/xfdb/15714>⁴⁶⁰⁹ <http://xforce.iss.net/xforce/xfdb/15702>⁴⁶¹⁰ <http://xforce.iss.net/xforce/xfdb/15700>⁴⁶¹¹ <http://technet.microsoft.com/en-us/security/bulletin/ms04-011>⁴⁶¹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0533>⁴⁶¹³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;835732>⁴⁶¹⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1000>⁴⁶¹⁵ <http://www.kb.cert.org/vuls/id/753212>⁴⁶¹⁶ <http://www.kb.cert.org/vuls/id/783748>⁴⁶¹⁷ <http://xforce.iss.net/xforce/xfdb/15678>⁴⁶¹⁹ <http://www.securityfocus.com/bid/15056>⁴⁶²⁰ <http://www.securityfocus.com/bid/15057>⁴⁶²¹ <http://www.securityfocus.com/bid/15058>⁴⁶²² <http://www.securityfocus.com/bid/15059>⁴⁶²³ <http://www.us-cert.gov/ncas/alerts/ta05-284a>⁴⁶²⁴ <http://www.kb.cert.org/vuls/id/180868>⁴⁶²⁵ <http://www.kb.cert.org/vuls/id/950516>⁴⁶²⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-1978>⁴⁶²⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-1979>⁴⁶²⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-1980>⁴⁶²⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2119>⁴⁶³⁰ <http://technet.microsoft.com/en-us/security/bulletin/ms05-051>

			MSKB 902400 ⁴⁶³¹ OSVDB 18828 ⁴⁶³² OVAL OVAL1071 ⁴⁶³³ OVAL OVAL1134 ⁴⁶³⁴ OVAL OVAL1136 ⁴⁶³⁵ OVAL OVAL1182 ⁴⁶³⁶ OVAL OVAL1203 ⁴⁶³⁷ OVAL OVAL1253 ⁴⁶³⁸ OVAL OVAL1261 ⁴⁶³⁹ OVAL OVAL1269 ⁴⁶⁴⁰ OVAL OVAL1283 ⁴⁶⁴¹ OVAL OVAL1325 ⁴⁶⁴² OVAL OVAL1338 ⁴⁶⁴³ OVAL OVAL1413 ⁴⁶⁴⁴ OVAL OVAL1452 ⁴⁶⁴⁵ OVAL OVAL1466 ⁴⁶⁴⁶ OVAL OVAL1499 ⁴⁶⁴⁷ OVAL OVAL1513 ⁴⁶⁴⁸ OVAL OVAL1550 ⁴⁶⁴⁹ OVAL OVAL551 ⁴⁶⁵⁰ OVAL OVAL576 ⁴⁶⁵¹ OVAL OVAL686 ⁴⁶⁵² OVAL OVAL816 ⁴⁶⁵³ SECTRAK 1015037 ⁴⁶⁵⁴ SECUNIA 17161 ⁴⁶⁵⁵ SECUNIA 17172 ⁴⁶⁵⁶ SECUNIA 17223 ⁴⁶⁵⁷ SECUNIA 17509 ⁴⁶⁵⁸ URL1 ⁴⁶⁵⁹ URL2 ⁴⁶⁶⁰		
13.	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution	Ovo ažuriranje rešava nekoliko otkrivenih i privatno prijavljenih ranjivosti. Preporučuje se da korisnici odmah primene update.	BID 18863 ⁴⁶⁶² BID 18891 ⁴⁶⁶³ CERT TA06-192A ⁴⁶⁶⁴ CERT-VN 189140 ⁴⁶⁶⁵	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows2000-KB917159-

⁴⁶⁶¹ www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windows2000-kb902400-x86-enu_f6eabdb255f52661f789b6fb94bbc8dea6822213.exe

⁴⁶³¹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;902400>

⁴⁶³² <http://www.osvdb.org/18828>

⁴⁶³³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1071>

⁴⁶³⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1134>

⁴⁶³⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1136>

⁴⁶³⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1182>

⁴⁶³⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1203>

⁴⁶³⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1253>

⁴⁶³⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1261>

⁴⁶⁴⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1269>

⁴⁶⁴¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1283>

⁴⁶⁴² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1325>

⁴⁶⁴³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1338>

⁴⁶⁴⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1413>

⁴⁶⁴⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1452>

⁴⁶⁴⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1466>

⁴⁶⁴⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1499>

⁴⁶⁴⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1513>

⁴⁶⁴⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1550>

⁴⁶⁵⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:551>

⁴⁶⁵¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:576>

⁴⁶⁵² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:686>

⁴⁶⁵³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:816>

⁴⁶⁵⁴ <http://securitytracker.com/id?1015037>

⁴⁶⁵⁵ <http://secunia.com/advisories/17161/>

⁴⁶⁵⁶ <http://secunia.com/advisories/17172/>

⁴⁶⁵⁷ <http://secunia.com/advisories/17223/>

⁴⁶⁵⁸ <http://secunia.com/advisories/17509/>

⁴⁶⁵⁹ <https://downloads.avaya.com/elmodocs2/security/ASA-2005-214.pdf>

⁴⁶⁶⁰ <http://technet.microsoft.com/en-us/security/bulletin/MS05-051>

⁴⁶⁶² <http://www.securityfocus.com/bid/18863>

⁴⁶⁶³ <http://www.securityfocus.com/bid/18891>

⁴⁶⁶⁴ <http://www.us-cert.gov/ncas/alerts/ta06-192a>

	(917159) (windows-hotfixms06-035)		CERT-VN 333636 ⁴⁶⁶⁶ OSVDB 27154 ⁴⁶⁶⁷ OSVDB 27155 ⁴⁶⁶⁸ OVAL OVAL3 ⁴⁶⁶⁹ OVAL OVAL600 ⁴⁶⁷⁰ CVE: CVE-2006-1314 ⁴⁶⁷¹ CVE:VE-2006-1315 ⁴⁶⁷² MS: MS06-035 ⁴⁶⁷³ MSKB: 917159 ⁴⁶⁷⁴ SANS-06: W4 ⁴⁶⁷⁵ SANS-07: S2 ⁴⁶⁷⁶ SECUNIA: 21007 ⁴⁶⁷⁷ XF: win-mailslot-bo(26818) ⁴⁶⁷⁸ XF win-smb-information-disclosure(26820) ⁴⁶⁷⁹ URL1 ⁴⁶⁸⁰		x86-ENU.EXE (614888 bytes) ⁴⁶⁸¹
14.	CIFS Account Password Never Expires (cifs-acct-password-never-expires)	CIFS nalog ne zahteva vremensko ograničenje šifre. Ovo je rizik za bezbednost. Ako šifra nije vremenski ograničena, to omogućava zlonamernom napadaču da izvrši napad sa ciljem otkrivanja korisničke šifre. Ukoliko rok trajanja šifre nikada ne ističe, napad se može sprovoditi tokom dužeg perioda, što povećava mogućnost da šifra bude otkrivena.		Ozbiljan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 pod primerom Opšte ranjivosti
15.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.110:139 172.23.202.110:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB: 887429 ⁴⁶⁸² URL1 ⁴⁶⁸³	Ozbiljan	Metoda za konfiguraciju SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429 ⁴⁶⁸⁴ . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing</i> = <i>auto</i> ili da se zahteva SMB potpisivanje: <i>server signing</i> = <i>mandatory</i> .
16.	SMB signing not	172.23.202.110:139	Isto kao kod „SMB	Ozbiljan	Isto kao kod „SMB signing

⁴⁶⁶⁵ <http://www.kb.cert.org/vuls/id/189140>⁴⁶⁶⁶ <http://www.kb.cert.org/vuls/id/333636>⁴⁶⁶⁷ <http://www.osvdb.org/27154>⁴⁶⁶⁸ <http://www.osvdb.org/27155>⁴⁶⁶⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3>⁴⁶⁷⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:600>⁴⁶⁷¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1314>⁴⁶⁷² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1315>⁴⁶⁷³ <http://technet.microsoft.com/en-us/security/bulletin/ms06-035>⁴⁶⁷⁴ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;917159>⁴⁶⁷⁵ <http://www.sans.org/critical-security-controls/#w4>⁴⁶⁷⁶ <http://www.sans.org/critical-security-controls/#s2>⁴⁶⁷⁷ <http://secunia.com/advisories/21007/>⁴⁶⁷⁸ <http://xforce.iss.net/xforce/xfdb/26818>⁴⁶⁷⁹ <http://xforce.iss.net/xforce/xfdb/26820>⁴⁶⁸⁰ <http://technet.microsoft.com/en-us/security/bulletin/MS06-035>⁴⁶⁸¹ www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windows2000-kb917159-x86-enu_e685b01f66b72125ed2c97afd2813ce309b9a7f5.exe⁴⁶⁸² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429>⁴⁶⁸³ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>⁴⁶⁸⁴ <http://support.microsoft.com/kb/887429>

	required (cifs-smb-signing-not-required)	172.23.202.110:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	signing disabled (cifs-smb-signing-disabled)“ ranjivosti		disabled (cifs-smb-signing-disabled)“ ranjivosti.
17.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	172.23.202.110:135: Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183 ⁴⁶⁸⁵ CERT TA04-111A ⁴⁶⁸⁶ CERT-VN: 415294 ⁴⁶⁸⁷ CVE CVE-2004-0230 ⁴⁶⁸⁸ MS: MS05-019 ⁴⁶⁸⁹ MS: MS06-064 ⁴⁶⁹⁰ NETBSD: NetBSD-SA2004-006 ⁴⁶⁹¹ OSVDB 4030 ⁴⁶⁹² OVAL: OVAL2689 ⁴⁶⁹³ OVAL: OVAL270 ⁴⁶⁹⁴ OVAL OVAL3508 ⁴⁶⁹⁵ OVAL OVAL4791 ⁴⁶⁹⁶ OVAL OVAL5711 ⁴⁶⁹⁷ SECUNIA: 11440 ⁴⁶⁹⁸ SECUNIA: 22341 ⁴⁶⁹⁹ SECUNIA 11458 ⁴⁷⁰⁰ SGI 20040403-01-A ⁴⁷⁰¹ XF tcp-rst-dos(15886) ⁴⁷⁰² URL1 ⁴⁷⁰³	Ozbiljan	Uraditi download a zatim instalirati Microsoft patch Windows2000-KB893066-v2-x86-ENU.EXE (756728 bytes) ⁴⁷⁰⁴
18.	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server. Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko poziva udaljenih procedura (RPC). Ovi servisi su i u prošlosti bili skloni ranjivostima.. Mnoštvo informacija koje napadačima	BID: 494 ⁴⁷⁰⁵ CVE: CVE-1999-0519 ⁴⁷⁰⁶ MSKB: 143474 ⁴⁷⁰⁷ URL1 ⁴⁷⁰⁸	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost

⁴⁶⁸⁵ <http://www.securityfocus.com/bid/10183>⁴⁶⁸⁶ <http://www.us-cert.gov/ncas/alerts/ta04-111a>⁴⁶⁸⁷ <http://www.kb.cert.org/vuls/id/415294>⁴⁶⁸⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁴⁶⁸⁹ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁴⁶⁹⁰ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁴⁶⁹¹ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁴⁶⁹² <http://www.osvdb.org/4030>⁴⁶⁹³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>⁴⁶⁹⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>⁴⁶⁹⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>⁴⁶⁹⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>⁴⁶⁹⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>⁴⁶⁹⁸ <http://secunia.com/advisories/11440/>⁴⁶⁹⁹ <http://secunia.com/advisories/22341/>⁴⁷⁰⁰ <http://secunia.com/advisories/11458/>⁴⁷⁰¹ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>⁴⁷⁰² <http://xforce.iss.net/xforce/xfdb/15886>⁴⁷⁰³ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁴⁷⁰⁴ www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windows2000-kb893066-v2-x86-enu_a5b95ec14e70e531e784ea83e633d24a0ea83795.exe⁴⁷⁰⁵ <http://www.securityfocus.com/bid/494>⁴⁷⁰⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>⁴⁷⁰⁷ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>⁴⁷⁰⁸ http://www.hsc.fr/ressources/presentations/null_sessions/

		postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinjenije napade.			
19.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	OSVDB 95 ⁴⁷⁰⁹ CVE: CVE-1999-0524 ⁴⁷¹⁰ XF: icmp-netmask(306) ⁴⁷¹¹ XF: icmp-timestamp(322) ⁴⁷¹²	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost

Tabela 111. Windows OS sa IP adresama 172.23.202.111, 172.23.202.75, 172.23.202.74, 172.23.202.73 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.111		OS: Microsoft Windows 2003 Enterprise server x64 SP1, WIN2003ENX64sp1			14
IP adresa: 172.23.202.75		OS: Windows server 2003 Enterprise x86 SP1, WIN2003ENX86sp1			14
IP adresa: 172.23.202.74		OS: Windows server 2003 Standard x86 SP1, WIN2003StX86sp1			14
IP adresa: 172.23.202.73		OS: Windows server 2003 Standard x64 SP1, WIN2003StX64sp1			14
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Microsoft Server Service / CanonicalizePathName() Remote Code Execution Vulnerability (dcerpc-msnetapi-netpathcanonicalize-dos)	Odredene verzije Microsoft Windows-a su ranjive na daljinsko preopterećenje bafera (privremene memorije) koje bi moglo da kompromituje određeni računar. Posebno izrađen paket se može koristiti sa pozivom ka NetPathCanonicalize RPC ruti na servisu servera, pri čemu bi napadač mogao da izvrši kôd pod sistemskim nivoom pristupa.	BID 19409 CERT TA06-220A CERT-VN 650769 CVE CVE-2006-3439 MS MS06-040 OVAL OVAL492 SECUNIA 21388 XF ms-server-service-bo(28002)	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003.WindowsXP-KB921883-v2-x64.ENU.EXE ⁴⁷¹³ , a za 32-bitnu verziju : WindowsServer2003-KB921883-v2-x86-ENU.exe ⁴⁷¹⁴

⁴⁷⁰⁹ <http://www.osvdb.org/95>

⁴⁷¹⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>

⁴⁷¹¹ <http://xforce.iss.net/xforce/xfdb/306>

⁴⁷¹² <http://xforce.iss.net/xforce/xfdb/322>

⁴⁷¹³ <http://download.microsoft.com/download/3/9/e/39ee55a0-f350-4a1c-ab0f-a3525c072593/WindowsServer2003.WindowsXP-KB921883-v2-x64-ENU.exe>

⁴⁷¹⁴ <http://download.microsoft.com/download/6/e/e/6ee2a18d-b3a7-457a-af39-fb687fd6aa91/WindowsServer2003-KB921883-v2-x86-ENU.exe>

2.	MS03-039: Buffer Overrun In RPCSS Service Could Allow Code Execution (824146) (windows-hotfix-ms03-039)	Napadač koji je uspešno iskoristio ovu ranjivost bi mogao biti u mogućnosti da pokrene kôd sa privilegijama lokalnog sistema na pogođenom sistemu ili bi mogao da prouzrokuje kvar RPCSS servisa. Napadač bi tada mogao biti u mogućnosti da preduzme bilo kakvu radnju na sistemu, uključujući instaliranje programa, pregledanje, izmene i brisanje podataka ili kreiranje novih naloga sa svim privilegijama. Da bi iskoristio ove ranjivosti, napadač bi mogao da napravi program sa kojim bi poslao malicioznu RPC poruku ranjivom sistemu, ciljajući RPCSS servis.	BID: 8458 ⁴⁷¹⁵ , CVE: CVE-2003-0528 ⁴⁷¹⁶ , CVE: CVE-2003-0605 ⁴⁷¹⁷ , CVE: CVE-2003-0715 ⁴⁷¹⁸ , MSKB: 824146 ⁴⁷¹⁹ , MS:MS03-039 ⁴⁷²⁰	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003-KB824146-ia64-ENU.exe ⁴⁷²¹ , a za 32-bitnu verziju WindowsXP-KB824146-x86-ENU.exe ⁴⁷²² Uraditi download a zatim instalirati Microsoft patch WindowsServer2003-KB819696-ia64-ENU.exe ⁴⁷²³ , a za 32-bitnu verziju WindowsServer2003-KB819696-x86-ENU.exe ⁴⁷²⁴
3.	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (windows-hotfix-ms08-067)	172.23.202.111:139 172.23.202.111:445 172.23.202.75:139 172.23.202.75:445 172.23.202.74:139 172.23.202.74:445 172.23.202.73:139 172.23.202.73:445 Ovo ažuriranje bezbednosti rešava ranjivost koja je prijavljena od strane privatnog lica. Ranjivost bi mogla da omogući daljinsko izvršavanje koda ukoliko je napadnuti sistem primio posebno izrađen RPC zahtev. Na sistemima Microsoft Windows 2000, Windows XP, i Windows Server 2003, napadač bi mogao da iskoristi ovu ranjivost bez proveravanja	BID 31874 ⁴⁷²⁵ CERT TA08-297A ⁴⁷²⁶ CERT TA09-088A ⁴⁷²⁷ CERT-VN 827267 ⁴⁷²⁸ IAVM 2008-A-0081 ⁴⁷²⁹ OVAL OVAL6093 ⁴⁷³⁰ XF 46040 ⁴⁷³¹ MS: MS08-067 ⁴⁷³² MSKB: 958644 ⁴⁷³³ CVE: CVE-2008-4250 ⁴⁷³⁴ SECUNIA: 32326 ⁴⁷³⁵ URL1 ⁴⁷³⁶ URL2 ⁴⁷³⁷ URL3 ⁴⁷³⁸ URL4 ⁴⁷³⁹	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003-WindowsXP-KB958644-x64-ENU.exe (1288568 bytes) ⁴⁷⁴⁰ , a za 32-bitnu verziju WindowsServer2003-KB958644-x86-ENU.exe ⁴⁷⁴¹

⁴⁷¹⁵ <http://www.securityfocus.com/bid/8458>⁴⁷¹⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0528>⁴⁷¹⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0605>⁴⁷¹⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0715>⁴⁷¹⁹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;824146>⁴⁷²⁰ <http://technet.microsoft.com/en-us/security/bulletin/ms03-039>⁴⁷²¹ <http://www.microsoft.com/en-us/download/confirmation.aspx?id=13195>⁴⁷²² <http://download.microsoft.com/download/c/d/d/cdd7ac92-e4cc-4b1e-bc2f-7a61b46b23bf/WindowsXP-KB824146-x86-ENU.exe>⁴⁷²³ <http://www.microsoft.com/en-us/download/confirmation.aspx?id=627>⁴⁷²⁴ <http://download.microsoft.com/download/5/e/6/5e6f9e28-b684-4788-8b1a-013eb62a41ba/WindowsServer2003-KB819696-x86-ENU.exe>⁴⁷²⁵ <http://www.securityfocus.com/bid/31874>⁴⁷²⁶ <http://www.us-cert.gov/ncas/alerts/ta08-297a>⁴⁷²⁷ <http://www.us-cert.gov/ncas/alerts/ta09-088a>⁴⁷²⁸ <http://www.kb.cert.org/vuls/id/827267>⁴⁷²⁹ <http://iase.disa.mil/stigs/iavm-cve.html>⁴⁷³⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6093>⁴⁷³¹ <http://xforce.iss.net/xforce/xfdb/46040>⁴⁷³² <http://technet.microsoft.com/en-us/security/bulletin/ms08-067>⁴⁷³³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958644>⁴⁷³⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4250>⁴⁷³⁵ <http://secunia.com/advisories/32326/>⁴⁷³⁶ blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx⁴⁷³⁷ <http://blogs.msdn.com/b/sdl/archive/2008/10/22/ms08-067.aspx>⁴⁷³⁸ <http://blogs.technet.com/b/msrc/archive/2008/10/23/ms08-067-released.aspx>⁴⁷³⁹ <http://technet.microsoft.com/en-us/security/bulletin/MS08-067>⁴⁷⁴⁰ download.windowsupdate.com/msdownload/update/software/secu/2008/10/windowsserver2003.windowsexp-kb958644-x64-enu_75717882c206870bdba8c8e606c588853fb8e34c.exe⁴⁷⁴¹ <http://download.microsoft.com/download/e/e/3/ee322649-7f38-4553-a26b-a2ac40a0b205/WindowsServer2003-KB958644-x86-ENU.exe>

		autentičnosti i da pokrene proizvoljan kôd. Moguće je da ova ranjivost može biti upotrebljena za intenziviranje skrivenog korišćenja exploit-a. Praksa je pokazala da upotreba zaštitnog zida može da pomogne u zaštiti mrežnih resursa od napada koji potiču izvan okvira organizacije.			
4.	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (windows-hotfix-ms09-001)	172.23.202.111:139 172.23.202.111:445 172.23.202.75:139 172.23.202.75:445 172.23.202.74:139 172.23.202.74:445 172.23.202.73:139 172.23.202.73:445 Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti koje su privatno prijavljene a odnose se na protokol Microsoft Server Message Block-a (SMB). Ranjivosti mogu da omoguće daljinsko izvršenje kôda na ugroženim sistemima. Napadač koji je uspešno iskoristio ove ranjivosti može da instalira programe, pregleda, menja ili briše podatke ili otvara nove naloge sa potpunim korisničkim pravima. Praksa je pokazala da zaštitni zid i njegove standardne konfiguracije po defaultu mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan okvira organizacije. Za sisteme koji su stalno povezani na Internet preporuka je da imaju što manji broj izloženih portova.	BID 31179 ⁴⁷⁴² BID 33121 ⁴⁷⁴³ BID 33122 ⁴⁷⁴⁴ CERT TA09-013A ⁴⁷⁴⁵ OVAL OVAL5248 ⁴⁷⁴⁶ OVAL OVAL5262 ⁴⁷⁴⁷ OVAL OVAL5863 ⁴⁷⁴⁸ OVAL OVAL6044 ⁴⁷⁴⁹ XF 45146 ⁴⁷⁵⁰ MS: MS09-001 ⁴⁷⁵¹ MSKB: 958687 ⁴⁷⁵² CVE: CVE-2008-4114 ⁴⁷⁵³ CVE: CVE-2008-4835 ⁴⁷⁵⁴ CVE: CVE-2008-4834 ⁴⁷⁵⁵ SECUNIA: 31883 ⁴⁷⁵⁶ URL1 ⁴⁷⁵⁷ URL2 ⁴⁷⁵⁸ URL3 ⁴⁷⁵⁹	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003-KB958687-ia64-ENU.exe (1691512 bytes) ⁴⁷⁶⁰ , a za 32-bitnu verziju WindowsServer2003-KB958687-x86-ENU.exe ⁴⁷⁶¹
5.	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-012)	172.23.202.111:139 172.23.202.111:445 172.23.202.75:139 172.23.202.75:445 172.23.202.74:139 172.23.202.74:445	CERT TA10-040A ⁴⁷⁶² OVAL OVAL7751 ⁴⁷⁶³ OVAL OVAL8314 ⁴⁷⁶⁴ OVAL OVAL8438 ⁴⁷⁶⁵ OVAL OVAL8524 ⁴⁷⁶⁶ MS: MS10-012 ⁴⁷⁶⁷	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003.WindowsXP-KB971468-x64-ENU.exe (1026944)

⁴⁷⁴² <http://www.securityfocus.com/bid/31179>⁴⁷⁴³ <http://www.securityfocus.com/bid/33121>⁴⁷⁴⁴ <http://www.securityfocus.com/bid/33122>⁴⁷⁴⁵ <http://www.us-cert.gov/ncas/alerts/ta09-013a>⁴⁷⁴⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5248>⁴⁷⁴⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5262>⁴⁷⁴⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5863>⁴⁷⁴⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6044>⁴⁷⁵⁰ <http://xforce.iss.net/xforce/xfdb/45146>⁴⁷⁵¹ <http://technet.microsoft.com/en-us/security/bulletin/MS09-001>⁴⁷⁵² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958687>⁴⁷⁵³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4114>⁴⁷⁵⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4835>⁴⁷⁵⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4834>⁴⁷⁵⁶ <http://secunia.com/advisories/31883/>⁴⁷⁵⁷ http://www.vallejo.cc/proyectos/vista_SMB_write_DoS.htm⁴⁷⁵⁸ <http://www.zerodayinitiative.com/advisories/ZDI-09-001/>⁴⁷⁵⁹ <http://www.zerodayinitiative.com/advisories/ZDI-09-002/>⁴⁷⁶⁰ download.windowsupdate.com/msdownload/update/software/secu/2008/12/windowsserver2003-kb958687-ia64-enu_a4d695fccfc7fc0071240d49035fbc9e6fbb16df.exe⁴⁷⁶¹ <http://download.microsoft.com/download/6/9/8/698F11AA-15C7-4BAF-818D-2BCC1704F202/WindowsServer2003-KB958687-x86-ENU.exe>⁴⁷⁶² <http://www.us-cert.gov/ncas/alerts/ta10-040a>⁴⁷⁶³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7751>⁴⁷⁶⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8314>⁴⁷⁶⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8438>⁴⁷⁶⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8524>⁴⁷⁶⁷ <http://technet.microsoft.com/en-us/security/bulletin/MS10-012>

	012)	172.23.202.73:139 172.23.202.73:445 Ovo ažuriranje bezbednosti rešava privatno prijavljenu ranjivost. Ova ranjivost bi mogla da omogući izvršenje udaljenog kôda ukoliko bi napadnuti sistem primio posebno kreiran RPC zahtev. Na sistemima Microsoft Windows 2000, Windows XP i Windows Server 2003, napadač bi mogao da iskoristi ovu ranjivost bez autentičnosti da pokrene proizvoljan kôd. Moguće je iskoristiti ovu ranjivost da se kreira eksploatacija. Dosadašnja praksa fajervola i standardne fajervol difolt konfiguracije mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan organizacije.	MSKB - 971468 ⁴⁷⁶⁸ CVE: CVE-2010-0020 ⁴⁷⁶⁹ CVE: CVE-2010-0021 ⁴⁷⁷⁰ CVE: CVE-2010-0022 ⁴⁷⁷¹ CVE CVE-2010-0231 ⁴⁷⁷²		bytes) ⁴⁷⁷³ , a za 32-bitnu verziju WindowsServer2003-KB971468-x86-ENU.exe ⁴⁷⁷⁴
6.	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-054)	172.23.202.111:139 172.23.202.111:445 172.23.202.75:139 172.23.202.75:445 172.23.202.74:139 172.23.202.74:445 172.23.202.73:139 172.23.202.73:445 Opis je isti kao kod ranjivosti MS10-012	CERT TA10-222A ⁴⁷⁷⁵ OVAL OVAL11106 ⁴⁷⁷⁶ OVAL OVAL12015 ⁴⁷⁷⁷ OVAL OVAL12072 ⁴⁷⁷⁸ CVE: CVE-2010-2550 ⁴⁷⁷⁹ CVE: CVE-2010-2551 ⁴⁷⁸⁰ CVE: CVE-2010-2552 ⁴⁷⁸¹ MS: MS10-054 ⁴⁷⁸² MSKB 982214 ⁴⁷⁸³	Kritičan	Uraditi download a zatim instalirati Microsoft patch windowsserver2003.window wsxp-kb982214-x64- enu.exe (1027968 bytes) ⁴⁷⁸⁴ , a za 32-bitnu verziju WindowsServer2003-KB982214-x86- ENU.exe ⁴⁷⁸⁵
7.	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms11-020)	172.23.202.111:139 172.23.202.111:445 172.23.202.75:139 172.23.202.75:445 172.23.202.74:139 172.23.202.74:445 172.23.202.73:139 172.23.202.73:445	BID 47198 ⁴⁷⁸⁶ CERT TA11-102A ⁴⁷⁸⁷ IAVM 2011-A-0050 ⁴⁷⁸⁸ OSVDB 71781 ⁴⁷⁸⁹ OVAL OVAL12076 ⁴⁷⁹⁰ SECUNIA 44072 ⁴⁷⁹¹ CVE: CVE-2011-0661 ⁴⁷⁹² MS: MS11-020 ⁴⁷⁹³	Kritičan	Uraditi download a zatim instalirati Microsoft patch windowsserver2003.window wsxp-kb2508429-x64- enu.exe (1044864 bytes) ⁴⁷⁹⁵ , a za 32-bitnu verziju

⁴⁷⁶⁸<http://support.microsoft.com/default.aspx?scid=kb;EN-US;971468>⁴⁷⁶⁹<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0020>⁴⁷⁷⁰<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0021>⁴⁷⁷¹<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0022>⁴⁷⁷²<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0231>⁴⁷⁷³download.windowsupdate.com/msdownload/update/software/secu/2010/01/windowsserver2003.windowwsxp-kb971468-x64-enu_8ea00e574a923da8a3aa9205a07780ed0a8741fa.exe⁴⁷⁷⁴<http://download.microsoft.com/download/F/5/B/F5BCEB3A-58B9-4FFE-8698-D0F74F02CAE2/WindowsServer2003-KB971468-x86-ENU.exe>⁴⁷⁷⁵<http://www.us-cert.gov/ncas/alerts/ta10-222a>⁴⁷⁷⁶<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11106>⁴⁷⁷⁷<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12015>⁴⁷⁷⁸<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12072>⁴⁷⁷⁹<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2550>⁴⁷⁸⁰<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2551>⁴⁷⁸¹<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2552>⁴⁷⁸²<http://technet.microsoft.com/en-us/security/bulletin/MS10-054>⁴⁷⁸³<http://support.microsoft.com/default.aspx?scid=kb;EN-US;982214>⁴⁷⁸⁴download.windowsupdate.com/msdownload/update/software/secu/2010/07/windowsserver2003.windowwsxp-kb982214-x64-enu_3780ab4068c4715ca93c4d5e4d9d4dbf9bbb6bc3.exe⁴⁷⁸⁵<http://download.microsoft.com/download/E/F/9/EF903A71-690C-4D73-A871-63E5932FD5E3/WindowsServer2003-KB982214-x86-ENU.exe>⁴⁷⁸⁶<http://www.securityfocus.com/bid/47198>⁴⁷⁸⁷<http://www.us-cert.gov/ncas/alerts/ta11-102a>⁴⁷⁸⁸<http://iase.disa.mil/stigs/iavm-cve.html>⁴⁷⁸⁹<http://www.osvdb.org/71781>⁴⁷⁹⁰<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12076>⁴⁷⁹¹<http://secunia.com/advisories/44072/>⁴⁷⁹²<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661>⁴⁷⁹³<http://technet.microsoft.com/en-us/security/bulletin/ms11-020>

		Opis je isti kao kod ranjivosti MS10-012	MSKB: 2508429 ⁴⁷⁹⁴		WindowsServer2003-KB2508429-x86-ENU.exe ⁴⁷⁹⁶
8.	MS03-026: Buffer Overrun In RPC Interface Could Allow Code Execution (823980) (windows-hotfix-ms03-026)	Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti u Windows Distributed Component Object Model (DCOM) Remote Procedure Call (RPC). Napadač koji uspešno iskoristi ovu ranjivost, bio bi u mogućnosti da pokrene kôd sa privilegijama lokalnog sistema na napadnutom sistemu. Napadač bi bio u mogućnosti da preduzme bilo kakvu akciju na sistemu, uključujući instaliranje programa, pregledanje, menjanje ili brisanje podataka, ili pak kreiranje novih naloga sa svim privilegijama. Da bi iskoristio ovu ranjivost, napadač bi morao da pošalje posebno kreiran zahtev udaljenom kompjuteru na specifične RPC portove.	CERT CA-2003-16 ⁴⁷⁹⁷ CERT CA-2003-19 ⁴⁷⁹⁸ CERT-VN 568148 ⁴⁷⁹⁹ OVAL OVAL194 ⁴⁸⁰⁰ OVAL OVAL2343 ⁴⁸⁰¹ OVAL OVAL296 ⁴⁸⁰² XF win-rpc-dcom-bo(12629) ⁴⁸⁰³ CVE: CVE-2003-0352 ⁴⁸⁰⁴ MS: MS03-026 ⁴⁸⁰⁵ BID: 8205 ⁴⁸⁰⁶ MSKB: 823980 ⁴⁸⁰⁷	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003-KB823980-ia64-ENU.exe ⁴⁸⁰⁸ , a za 32-bitnu verziju WindowsServer2003-KB823980-x86-ENU.exe ⁴⁸⁰⁹
9.	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (windows-hotfixms06-035)	Ovo ažuriranje rešava nekoliko otkrivenih i privatno prijavljenih ranjivosti. Preporučuje se da korisnici odmah primene update.	BID 18863 ⁴⁸¹⁰ BID 18891 ⁴⁸¹¹ CERT TA06-192A ⁴⁸¹² CERT-VN 189140 ⁴⁸¹³ CERT-VN 333636 ⁴⁸¹⁴ OSVDB 27154 ⁴⁸¹⁵ OSVDB 27155 ⁴⁸¹⁶ OVAL OVAL3 ⁴⁸¹⁷ OVAL OVAL600 ⁴⁸¹⁸ CVE: CVE-2006-1314 ⁴⁸¹⁹ CVE:VE-2006-1315 ⁴⁸²⁰ MS: MS06-035 ⁴⁸²¹ MSKB: 917159 ⁴⁸²² SANS-06: W4 ⁴⁸²³ SANS-07: S2 ⁴⁸²⁴	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003.WindowsXP-KB917159-x64-ENU.exe (1033528 bytes) ⁴⁸²⁹ , a za 32-bitnu verziju WindowsServer2003-KB917159-x86-ENU.exe ⁴⁸³⁰

⁴⁷⁹⁵ download.windowsupdate.com/msdownload/update/software/secu/2011/03/windowsserver2003.windowsexp-kb2508429-x64-enu_a1ab44f33a891a3fdff7273ad240f35d5af7ce99.exe

⁴⁷⁹⁴ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;2508429>

⁴⁷⁹⁶ <http://download.microsoft.com/download/E/D/7/ED71C471-3229-4120-B9E3-F6B03D7D3714/WindowsServer2003-KB2508429-x86-ENU.exe>

⁴⁷⁹⁷ <http://www.us-cert.gov/ncas/alerts/ca-2003-16>

⁴⁷⁹⁸ <http://www.us-cert.gov/ncas/alerts/ca-2003-19>

⁴⁷⁹⁹ <http://www.kb.cert.org/vuls/id/568148>

⁴⁸⁰⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:194>

⁴⁸⁰¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2343>

⁴⁸⁰² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:296>

⁴⁸⁰³ <http://xforce.iss.net/xforce/xfdb/12629>

⁴⁸⁰⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0352>

⁴⁸⁰⁵ <http://technet.microsoft.com/en-us/security/bulletin/ms03-026>

⁴⁸⁰⁶ <http://www.securityfocus.com/bid/8205>

⁴⁸⁰⁷ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;823980>

⁴⁸⁰⁸ <http://www.microsoft.com/en-us/download/confirmation.aspx?id=186>

⁴⁸⁰⁹ <http://download.microsoft.com/download/8/f/2/8f21131d-9df3-4530-802a-2780629390b9/WindowsServer2003-KB823980-x86-ENU.exe>

⁴⁸¹⁰ <http://www.securityfocus.com/bid/18863>

⁴⁸¹¹ <http://www.securityfocus.com/bid/18891>

⁴⁸¹² <http://www.us-cert.gov/ncas/alerts/ta06-192a>

⁴⁸¹³ <http://www.kb.cert.org/vuls/id/189140>

⁴⁸¹⁴ <http://www.kb.cert.org/vuls/id/333636>

⁴⁸¹⁵ <http://www.osvdb.org/27154>

⁴⁸¹⁶ <http://www.osvdb.org/27155>

⁴⁸¹⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3>

⁴⁸¹⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:600>

⁴⁸¹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1314>

⁴⁸²⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1315>

⁴⁸²¹ <http://technet.microsoft.com/en-us/security/bulletin/ms06-035>

⁴⁸²² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;917159>

⁴⁸²³ <http://www.sans.org/critical-security-controls/#w4>

			SECUNIA: 21007 ⁴⁸²⁵ XF: win-mailslot-bo(26818) ⁴⁸²⁶ XF win-smb-information-disclosure(26820) ⁴⁸²⁷ URL1 ⁴⁸²⁸		
10.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.111:139 172.23.202.111:445 172.23.202.75:139 172.23.202.75:445 172.23.202.74:139 172.23.202.74:445 172.23.202.73:139 172.23.202.73:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB: 887429 ⁴⁸³¹ URL1 ⁴⁸³²	Ozbiljan	Metoda za konfigurisanje SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429 ⁴⁸³³ . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracionom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing = auto</i> ili da se zahteva SMB potpisivanje: <i>server signing = mandatory</i>
11.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.111:139 172.23.202.111:445 172.23.202.75:139 172.23.202.75:445 172.23.202.74:139 172.23.202.74:445 172.23.202.73:139 172.23.202.73:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti.
12.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	172.23.202.111:135 172.23.202.75:135 172.23.202.74:135 172.23.202.73:135 Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hедера i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr.	BID: 10183 ⁴⁸³⁴ CERT TA04-111A ⁴⁸³⁵ CERT-VN: 415294 ⁴⁸³⁶ CVE CVE-2004-0230 ⁴⁸³⁷ MS: MS05-019 ⁴⁸³⁸ MS: MS06-064 ⁴⁸³⁹ NETBSD: NetBSD-SA2004-006 ⁴⁸⁴⁰ OSVDB 4030 ⁴⁸⁴¹ OVAL: OVAL2689 ⁴⁸⁴² OVAL: OVAL270 ⁴⁸⁴³ OVAL OVAL3508 ⁴⁸⁴⁴	Ozbiljan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003.WindowsXP-KB922819-x64-ENU.exe (898360 bytes) ⁴⁸⁵³ , a za 32-bitnu verziju WindowsServer2003-KB922819-x86-ENU.exe ⁴⁸⁵⁴

⁴⁸²⁴ <http://www.sans.org/critical-security-controls/#s2>⁴⁸²⁹ www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsserver2003.windowsxp-kb917159-x64-enu_93a5cfec377221668b923e88a741ce1cadcb76c1.exe⁴⁸³⁰ <http://download.microsoft.com/download/e/f/e/efef9f44-94fd-4659-8b95-db20ca3378d9/WindowsServer2003-KB917159-x86-ENU.exe>⁴⁸²⁵ <http://secunia.com/advisories/21007/>⁴⁸²⁶ <http://xforce.iss.net/xforce/xfdb/26818>⁴⁸²⁷ <http://xforce.iss.net/xforce/xfdb/26820>⁴⁸²⁸ <http://technet.microsoft.com/en-us/security/bulletin/MS06-035>⁴⁸³¹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429>⁴⁸³² <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>⁴⁸³³ <http://support.microsoft.com/kb/887429>⁴⁸³⁴ <http://www.securityfocus.com/bid/10183>⁴⁸³⁵ <http://www.us-cert.gov/ncas/alerts/ta04-111a>⁴⁸³⁶ <http://www.kb.cert.org/vuls/id/415294>⁴⁸³⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁴⁸³⁸ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁴⁸³⁹ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁴⁸⁴⁰ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁴⁸⁴¹ <http://www.osvdb.org/4030>⁴⁸⁴² <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:2689>⁴⁸⁴³ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:270>⁴⁸⁴⁴ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:3508>

		BGP.	OVAL OVAL4791⁴⁸⁴⁵ OVAL OVAL5711⁴⁸⁴⁶ SECUNIA: 11440⁴⁸⁴⁷ SECUNIA: 22341⁴⁸⁴⁸ SECUNIA 11458⁴⁸⁴⁹ SGI 20040403-01-A⁴⁸⁵⁰ XF tcp-rst-dos(15886)⁴⁸⁵¹ URL1⁴⁸⁵²		
13.	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server. Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko poziva udaljenih procedura (RPC). Ovi servisi su i u prošlosti bili skloni ranjivostima.. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinjenije napade.	BID: 494⁴⁸⁵⁵ CVE: CVE-1999-0519⁴⁸⁵⁶ MSKB: 143474⁴⁸⁵⁷ URL1⁴⁸⁵⁸	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost.
14.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatišu slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeci ICMP-ov zahtev za vremenski pečat.	OSVDB 95⁴⁸⁵⁹ CVE: CVE-1999-0524⁴⁸⁶⁰ XF: icmp-netmask(306)⁴⁸⁶¹ XF: icmp-timestamp(322)⁴⁸⁶²	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.

Tabela 112. Windows OS sa IP adresom 172.23.202.101 (2013. godina)

Datum: 16.11.2013	Operativni sistem i ime računara	Broj ranjivosti

⁴⁸⁵³ www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsserver2003.windowsexp-kb922819-x64-enu_4c34629b0664f2d2cd78c0276e4bd6b5e72ede61.exe

⁴⁸⁵⁴ <http://download.microsoft.com/download/a/d/2/ad2acd40-3ae7-49d3-88fe-064a71ccc61a/WindowsServer2003-KB922819-x86-ENU.exe>

⁴⁸⁴⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>

⁴⁸⁴⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>

⁴⁸⁴⁷ <http://secunia.com/advisories/11440/>

⁴⁸⁴⁸ <http://secunia.com/advisories/22341/>

⁴⁸⁴⁹ <http://secunia.com/advisories/11458/>

⁴⁸⁵⁰ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>

⁴⁸⁵¹ <http://xforce.iss.net/xforce/xfdb/15886>

⁴⁸⁵² <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>

⁴⁸⁵⁵ <http://www.securityfocus.com/bid/494>

⁴⁸⁵⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>

⁴⁸⁵⁷ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>

⁴⁸⁵⁸ http://www.hsc.fr/ressources/presentations/null_sessions/

⁴⁸⁵⁹ <http://www.osvdb.org/95>

⁴⁸⁶⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>

⁴⁸⁶¹ <http://xforce.iss.net/xforce/xfdb/306>

⁴⁸⁶² <http://xforce.iss.net/xforce/xfdb/322>

IP adresa: 172.23.202.101		OS: Microsoft Windows NT 4 Enterprise Sp6, NT4entsp6			22
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	MS03-039: Buffer Overrun In RPCSS Service Could Allow Code Execution (824146) (windows-hotfix-ms03-039)	Napadač koji je uspešno iskoristio ovu ranjivost bi mogao biti u mogućnosti da pokrene kôd sa privilegijama lokalnog sistema na pogođenom sistemu ili bi mogao da prouzrokuje kvar RPCSS servisa. Napadač bi tada mogao biti u mogućnosti da preduzme bilo kakvu radnju na sistemu, uključujući instaliranje programa, pregledanje, izmene i brisanje podataka ili kreiranje novih naloga sa svim privilegijama. Da bi iskoristio ove ranjivosti, napadač bi mogao da napravi program sa kojim bi poslao malicioznu RPC poruku ranjivom sistemu, ciljajući RPCSS servis.	BID: 8458 ⁴⁸⁶³ , CVE: CVE-2003-0528 ⁴⁸⁶⁴ , CVE: CVE-2003-0605 ⁴⁸⁶⁵ , CVE: CVE-2003-0715 ⁴⁸⁶⁶ , MSKB: 824146 ⁴⁸⁶⁷ , MS:MS03-039 ⁴⁸⁶⁸	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsNT4Workstation-KB824146-x86-ENU.EXE ⁴⁸⁶⁹
2.	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (windows-hotfix-ms09-001)	172.23.202.101:139 172.23.202.101:445 Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti koje su privatno prijavljene a odnose se na protokol Microsoft Server Message Block-a (SMB). Ranjivosti mogu da omoguće daljinsko izvršenje kôda na ugroženim sistemima. Napadač koji je uspešno iskoristio ove ranjivosti može da instalira programe, pregleda, menja ili briše podatke ili otvara nove naloge sa potpunim korisničkim pravima. Praksa je pokazala da zaštitni zid i njegove standardne konfiguracije po defaultu mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan okvira organizacije. Za sisteme koji su stalno povezani na Internet preporuka je da imaju što manji broj izloženih portova.	BID 31179 ⁴⁸⁷⁰ BID 33121 ⁴⁸⁷¹ BID 33122 ⁴⁸⁷² CERT TA09-013A ⁴⁸⁷³ OVAL OVAL5248 ⁴⁸⁷⁴ OVAL OVAL5262 ⁴⁸⁷⁵ OVAL OVAL5863 ⁴⁸⁷⁶ OVAL OVAL6044 ⁴⁸⁷⁷ XF 45146 ⁴⁸⁷⁸ MS: MS09-001 ⁴⁸⁷⁹ MSKB: 958687 ⁴⁸⁸⁰ CVE: CVE-2008-4114 ⁴⁸⁸¹ CVE: CVE-2008-4835 ⁴⁸⁸² CVE: CVE-2008-4834 ⁴⁸⁸³ SECUNIA: 31883 ⁴⁸⁸⁴ URL1 ⁴⁸⁸⁵ URL2 ⁴⁸⁸⁶ URL3 ⁴⁸⁸⁷	Kritičan	Nema adekvatne zakrpe zbog prestanka porške. Rešenje ažuriranje Operativnog sistema.

⁴⁸⁶³ <http://www.securityfocus.com/bid/8458>⁴⁸⁶⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0528>⁴⁸⁶⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0605>⁴⁸⁶⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0715>⁴⁸⁶⁷ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;824146>⁴⁸⁶⁸ <http://technet.microsoft.com/en-us/security/bulletin/ms03-039>⁴⁸⁶⁹ download.microsoft.com/download/3/0/c/30cff3cd-414d-4754-b9db-276de8161eef/windowsnt4workstation-kb824146-x86-enu.exe⁴⁸⁷⁰ <http://www.securityfocus.com/bid/31179>⁴⁸⁷¹ <http://www.securityfocus.com/bid/33121>⁴⁸⁷² <http://www.securityfocus.com/bid/33122>⁴⁸⁷³ <http://www.us-cert.gov/ncas/alerts/ta09-013a>⁴⁸⁷⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5248>⁴⁸⁷⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5262>⁴⁸⁷⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5863>⁴⁸⁷⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6044>⁴⁸⁷⁸ <http://xforce.iss.net/xforce/xfdb/45146>⁴⁸⁷⁹ <http://technet.microsoft.com/en-us/security/bulletin/MS09-001>⁴⁸⁸⁰ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958687>⁴⁸⁸¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4114>⁴⁸⁸² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4835>⁴⁸⁸³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4834>⁴⁸⁸⁴ <http://secunia.com/advisories/31883/>⁴⁸⁸⁵ http://www.vallejo.cc/proyectos/vista_SMB_write_DoS.htm⁴⁸⁸⁶ <http://www.zerodayinitiative.com/advisories/ZDI-09-001/>⁴⁸⁸⁷ <http://www.zerodayinitiative.com/advisories/ZDI-09-002/>

3.	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-012)	172.23.202.101:139 172.23.202.101:445 Ovo ažuriranje bezbednosti rešava nekoliko privatno prijavljenih ranjivosti na Microsoft Windows-u. Opasnost od ove ranjivosti leži u tome što bi ona omogućila daljinsko izvršavanje kôda ukoliko bi napadač kreirao posebno opremljen SMB paket i poslao ga ugroženom sistemu. Dosadašnja praksa fajervola i standardne fajervol difolt konfiguracije mogu da pomognu u zaštiti mrežnih resursa od napada (koji bi pokušali da iskoriste ove ranjivosti), a koji potiču izvan okvira organizacije.	CERT TA10-040A ⁴⁸⁸⁸ OVAL OVAL7751 ⁴⁸⁸⁹ OVAL OVAL8314 ⁴⁸⁹⁰ OVAL OVAL8438 ⁴⁸⁹¹ OVAL OVAL8524 ⁴⁸⁹² MS: MS10-012 ⁴⁸⁹³ MSKB - 971468 ⁴⁸⁹⁴ CVE: CVE-2010-0020 ⁴⁸⁹⁵ CVE: CVE-2010-0021 ⁴⁸⁹⁶ CVE: CVE-2010-0022 ⁴⁸⁹⁷ CVE CVE-2010-0231 ⁴⁸⁹⁸ SECUNIA 38510 ⁴⁸⁹⁹	Kritičan	Blokirati portove 139 i 445 na spoljnom fajervolu. Treba imati u vidu da će ova ranjivost takođe uticati na sisteme Windows 2000, a usled zastarevanja Windows 2000; ne postoji odgovarajuća zakrpa koja bi omogućila ublažavanje ove ranjivosti.
4.	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-054)	172.23.202.101:139 172.23.202.101:445 Opis je isti kao kod ranjivosti MS10-012	CERT TA10-222A ⁴⁹⁰⁰ OVAL OVAL11106 ⁴⁹⁰¹ OVAL OVAL12015 ⁴⁹⁰² OVAL OVAL12072 ⁴⁹⁰³ CVE: CVE-2010-2550 ⁴⁹⁰⁴ CVE: CVE-2010-2551 ⁴⁹⁰⁵ CVE: CVE-2010-2552 ⁴⁹⁰⁶ MS: MS10-054 ⁴⁹⁰⁷ MSKB 982214 ⁴⁹⁰⁸	Kritičan	Blokirati portove 139 i 445 na spoljnom fajervolu. Treba imati u vidu da će ova ranjivost takođe uticati na sisteme Windows 2000, a usled zastarevanja Windows 2000; ne postoji odgovarajuća zakrpa koja bi omogućila ublažavanje ove ranjivosti.
5.	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms11-020)	172.23.202.101:139 172.23.202.101:445 Opis je isti kao kod ranjivosti MS10-012	BID 47198 ⁴⁹⁰⁹ CERT TA11-102A ⁴⁹¹⁰ IAVM 2011-A-0050 ⁴⁹¹¹ OSVDB 71781 ⁴⁹¹² OVAL OVAL12076 ⁴⁹¹³ SECUNIA 44072 ⁴⁹¹⁴ CVE CVE-2011-0661 ⁴⁹¹⁵ MS: MS11-020 ⁴⁹¹⁶ MSKB: 2508429 ⁴⁹¹⁷	Kritičan	Blokirati portove 139 i 445 na spoljnom fajervolu. Treba imati u vidu da će ova ranjivost takođe uticati na sisteme Windows 2000, a usled zastarevanja Windows 2000; ne postoji odgovarajuća zakrpa koja bi omogućila ublažavanje ove

⁴⁸⁸⁸ <http://www.us-cert.gov/ncas/alerts/ta10-040a>⁴⁸⁸⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7751>⁴⁸⁹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8314>⁴⁸⁹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8438>⁴⁸⁹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8524>⁴⁸⁹³ <http://technet.microsoft.com/en-us/security/bulletin/MS10-012>⁴⁸⁹⁴ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;971468>⁴⁸⁹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0020>⁴⁸⁹⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0021>⁴⁸⁹⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0022>⁴⁸⁹⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0231>⁴⁸⁹⁹ <http://secunia.com/advisories/38510/>⁴⁹⁰⁰ <http://www.us-cert.gov/ncas/alerts/ta10-222a>⁴⁹⁰¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11106>⁴⁹⁰² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12015>⁴⁹⁰³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12072>⁴⁹⁰⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2550>⁴⁹⁰⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2551>⁴⁹⁰⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2552>⁴⁹⁰⁷ <http://technet.microsoft.com/en-us/security/bulletin/MS10-054>⁴⁹⁰⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;982214>⁴⁹⁰⁹ <http://www.securityfocus.com/bid/47198>⁴⁹¹⁰ <http://www.us-cert.gov/ncas/alerts/ta11-102a>⁴⁹¹¹ <http://iase.disa.mil/stigs/iavm-cve.html>⁴⁹¹² <http://www.osvdb.org/71781>⁴⁹¹³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12076>⁴⁹¹⁴ <http://secunia.com/advisories/44072/>⁴⁹¹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661>⁴⁹¹⁶ <http://technet.microsoft.com/en-us/security/bulletin/ms11-020>⁴⁹¹⁷ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;2508429>

					ranjivosti.
6.	Anonymous users can obtain the Windows password policy (cifs-nt-0002)	Korišćenjem CIFS NULL sesije, anonimni korisnik može da dobije uvid u polisu šifri. Polisa šifri sadrži osetljive informacije o najmanjoj mogućoj dužini lozinke, zaključavanje šifre, vremensko trajanje zaključanosti šifre itd.	SANS-01 W5 ⁴⁹¹⁸ CVE CVE-2000-1200 ⁴⁹¹⁹ MSKB 143474 ⁴⁹²⁰ XF nt-lsa-domain-sid(4015) ⁴⁹²¹ MSKB 823659 ⁴⁹²² MSKB 246261 ⁴⁹²³ MSKB 129457 ⁴⁹²⁴ SANS-02 W5 ⁴⁹²⁵ BID 959 ⁴⁹²⁶ SANS-04 W3 ⁴⁹²⁷ SANS-03 W5 ⁴⁹²⁸ BID 87 ⁴⁹²⁹		Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost.
7.	MS03-026: Buffer Overrun In RPC Interface Could Allow Code Execution (823980) (windows-hotfix-ms03-026)	Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti u Windows Distributed Component Object Model (DCOM) Remote Procedure Call (RPC). Napadač koji uspešno iskoristi ovu ranjivost, bio bi u mogućnosti da pokrene kôd sa privilegijama lokalnog sistema na napadnutom sistemu. Napadač bi bio u mogućnosti da preduzme bilo kakvu akciju na sistemu, uključujući instaliranje programa, pregledanje, menjanje ili brisanje podataka, ili pak kreiranje novih naloga sa svim privilegijama. Da bi iskoristio ovu ranjivost, napadač bi morao da pošalje posebno kreiran zahtev udaljenom kompjuteru na specifične RPC portove.	CVE: CVE-2003-0352 ⁴⁹³⁰ MS: MS03-026 ⁴⁹³¹ BID: 8205 ⁴⁹³² MSKB: 823980 ⁴⁹³³	Kritičan	Uraditi download a zatim instalirati Microsoft patch Q823980i.EXE ⁴⁹³⁴ Napomena: Posle instaliranja ove zakrpe obavezno je restart sistema.
8.	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (windows-hotfixms06-035)	Ovo ažuriranje rešava nekoliko otkrivenih i privatno prijavljenih ranjivosti. Preporučuje se da korisnici odmah primene update.	BID 18863 ⁴⁹³⁵ BID 18891 ⁴⁹³⁶ CERT TA06-192A ⁴⁹³⁷ CERT-VN 189140 ⁴⁹³⁸ CERT-VN 333636 ⁴⁹³⁹ OSVDB 27154 ⁴⁹⁴⁰ OSVDB 27155 ⁴⁹⁴¹ OVAL OVAL3 ⁴⁹⁴² OVAL OVAL600 ⁴⁹⁴³ URL1 ⁴⁹⁴⁴	Kritičan	Nema adekvatne zakrpe zbog prestanka podrške za ovaj OS. Rešenje: ažurirati sistem novijom verzijom operativnog sistema.

⁴⁹¹⁸ <http://www.sans.org/critical-security-controls/#w5>⁴⁹¹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2000-1200>⁴⁹²⁰ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>⁴⁹²¹ <http://xforce.iss.net/xforce/xfdb/4015>⁴⁹²² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;823659>⁴⁹²³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;246261>⁴⁹²⁴ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;129457>⁴⁹²⁵ <http://www.sans.org/critical-security-controls/#w5>⁴⁹²⁶ <http://www.securityfocus.com/bid/959>⁴⁹²⁷ <http://www.sans.org/critical-security-controls/#w3>⁴⁹²⁸ <http://www.sans.org/critical-security-controls/#w5>⁴⁹²⁹ <http://www.securityfocus.com/bid/87>⁴⁹³⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0352>⁴⁹³¹ <http://technet.microsoft.com/en-us/security/bulletin/ms03-026>⁴⁹³² <http://www.securityfocus.com/bid/8205>⁴⁹³³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;823980>⁴⁹³⁴ download.microsoft.com/download/6/5/1/651c3333-4892-431f-ae93-bf8718d29e1a/q823980i.exe⁴⁹³⁵ <http://www.securityfocus.com/bid/18863>⁴⁹³⁶ <http://www.securityfocus.com/bid/18891>⁴⁹³⁷ <http://www.us-cert.gov/ncas/alerts/ta06-192a>⁴⁹³⁸ <http://www.kb.cert.org/vuls/id/189140>⁴⁹³⁹ <http://www.kb.cert.org/vuls/id/333636>⁴⁹⁴⁰ <http://www.osvdb.org/27154>⁴⁹⁴¹ <http://www.osvdb.org/27155>⁴⁹⁴² <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:3>⁴⁹⁴³ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:600>

			CVE: CVE-2006-1314 ⁴⁹⁴⁵ CVE: VE-2006-1315 ⁴⁹⁴⁶ MS: MS06-035 ⁴⁹⁴⁷ MSKB: 917159 ⁴⁹⁴⁸ SANS-06: W4 ⁴⁹⁴⁹ SANS-07: S2 ⁴⁹⁵⁰ SECUNIA: 21007 ⁴⁹⁵¹ XF: win-mailslot-bo(26818) ⁴⁹⁵² XF win-smb-information-disclosure(26820) ⁴⁹⁵³		
9.	CIFS Account Password Never Expires (cifs-acct-password-never-expires)	CIFS nalog ne zahteva vremensko ograničenje šifre. Ovo je rizik za bezbednost. Ako šifra nije vremenski ograničena, to omogućava zlonamernom napadaču da izvrši napad sa ciljem otkrivanja korisničke šifre. Ukoliko rok trajanja šifre nikada ne ističe, napad se može sprovoditi tokom dužeg perioda, što povećava mogućnost da šifra bude otkrivena.		Ozbiljan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 pod primerom Opšte ranjivosti
10.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.101:139 172.23.202.101:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB: 887429 ⁴⁹⁵⁴ URL1 ⁴⁹⁵⁵	Ozbiljan	Metoda za konfiguracije SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429 ⁴⁹⁵⁶ . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing = auto</i> ili da se zahteva SMB potpisivanje: <i>server signing = mandatory</i> .
11.	Microsoft IIS 3.0 newdsn.exe File Creation Vulnerability (http-iis-0017)	172.23.202.101:80 Microsoft IIS 3.0 se instalira po defaultu zajedno sa programom newdsn.exe u direktorijumu wwwroot/scripts/tools/. Pokretanje ovog programa sa odgovarajućim prosledenim URL-om može omogućiti daljisko kreiranje fajlova. Tako kreiran fajl je Microsoft Access Database formata, ali može imati bilo kakvu ekstenziju, uključujući i .html.	OSVDB 275 ⁴⁹⁵⁷ BID 1818 ⁴⁹⁵⁸ CVE CVE-1999-0191 ⁴⁹⁵⁹ SANS-03 W1 ⁴⁹⁶⁰ XF http-cgi-newdsn(1530) ⁴⁹⁶¹	Ozbiljan	Ukloniti sve semplovane programe sa servera. Takođe iz direktorijuma wwwroot/scripts/tools ukloniti fajl newdsn.exe
12.	SMB signing not	172.23.202.101:139 172.23.202.101:445	Isto kao kod „SMB	Ozbiljan	Isto kao kod „SMB signing

⁴⁹⁴⁴ <http://technet.microsoft.com/en-us/security/bulletin/MS06-035>⁴⁹⁴⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1314>⁴⁹⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1315>⁴⁹⁴⁷ <http://technet.microsoft.com/en-us/security/bulletin/ms06-035>⁴⁹⁴⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;917159>⁴⁹⁴⁹ <http://www.sans.org/critical-security-controls/#w4>⁴⁹⁵⁰ <http://www.sans.org/critical-security-controls/#s2>⁴⁹⁵¹ <http://secunia.com/advisories/21007/>⁴⁹⁵² <http://xforce.iss.net/xforce/xfdb/26818>⁴⁹⁵³ <http://xforce.iss.net/xforce/xfdb/26820>⁴⁹⁵⁴ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429>⁴⁹⁵⁵ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>⁴⁹⁵⁶ <http://support.microsoft.com/kb/887429>⁴⁹⁵⁷ <http://www.osvdb.org/275>⁴⁹⁵⁸ <http://www.securityfocus.com/bid/1818>⁴⁹⁵⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0191>⁴⁹⁶⁰ <http://www.sans.org/critical-security-controls/#w1>⁴⁹⁶¹ <http://xforce.iss.net/xforce/xfdb/1530>

	required (cifs-smb-signing-not-required)	Sistem omogućava, ali ne zahteva SMB potpisivanje.	signing disabled (cifs-smb-signing-disabled)“ ranjivosti.		disabled (cifs-smb-signing-disabled)“ ranjivosti.
13.	Weak LAN Manager hashing permitted (cifs-generic-0005)	Ovaj sistem omogućava udaljenim korisnicima da se autentifikuju kroz LAN Manager (LM) heš mehanizam za otkrivanje lozinke. LM heš vrednost se lako može kreirati presretanjem korisničke komunikacije na mreži. Microsoft je obezbedio metod autentifikacije pod imenom NTLMv2 koji uvek treba koristiti umesto LM. NTLMv2 je dostupan na Windows NT 4.0 SP4 i na kasnijim verzijama (uključujući Windows 2000, Windows XP i Windows 2003).	SANS-02 W6 ⁴⁹⁶² URL1 ⁴⁹⁶³ SANS-03 W3 ⁴⁹⁶⁴ SANS-04 W5 ⁴⁹⁶⁵ SANS-01 W6 ⁴⁹⁶⁶	Ozbiljan	Ažurirati metod autorizacije korišćenjem registra. Treba imati u vidu da će ažuriranje metode autorizacije na NTMLv2 ukinuti kompatibilnost sa sistemima Windows 95/98/ME i starijim sistemima, pre -NT4 SP4. Pokrenuti editovanje registra (regedit.exe ili regedt32.exe) i potražiti do sledeće stavke: „HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa“ a zatim postaviti sledeću vrednost: -Naziv vrednosti: LMCompatibilityLevel -tip podataka: REG_DWORD -Podaci: treba koristiti najmanje nivo 3, ali se preporučuje nivo 5. Dodatno uraditi registarska podešavanja prema Microsoft uputstvu Q147706 ⁴⁹⁶⁷
14.	FTP access with ftp account (ftp-generic-0001)	172.23.202.101:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisničkim ID-jem „ftp“ i šifrom „ftp“. Dosadašnja praksa je pokazala da treba ukloniti difoltnu naloge, ako je to moguće. Za naloge koje zahteva sistem, treba promeniti difoltnu šifru.	CVE CVE-1999-0497 ⁴⁹⁶⁸	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko to nije kritično za dalje funkcionisanje sistema. U suprotnom, treba promeniti lozinku u nedifoltnu vrednost.
15.	FTP access with anonymous account (ftp-generic-0002)	172.23.202.101:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisničkim ID-jem „anonymous“ i šifrom „ftp@“. Dosadašnja praksa je pokazala da treba ukloniti difoltnu naloge, ako je to moguće. Za naloge koje zahteva sistem, treba promeniti difoltnu šifru.	CVE CVE-1999-0497 ⁴⁹⁶⁹	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko to nije kritično za dalje funkcionisanje sistema. U suprotnom, treba promeniti lozinku u nedifoltnu vrednost.
16.	FTP server does not support AUTH command (ftp-generic-0007)	Klijenti na FTP server po difoltu šalju poverljive podatke (korisnički ID i šifru) u vidu čitkog teksta. Ova okolnost dozvoljava zlonamernim korisnicima omogućava da presreću poverljive podatke ukoliko prisluškuju vezu. Noviji FTP serveri podržavaju komandu AUTH, koja daje veće opcije autentifikacije, kao TLS, Kerberos, GSSAPI, itd. Njih treba		Ozbiljan	Nadograditi/Ažurirati na a FTP server koji podržava komandu AUTH.

⁴⁹⁶² <http://www.sans.org/critical-security-controls/#w6>⁴⁹⁶³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;147706>⁴⁹⁶⁴ <http://www.sans.org/critical-security-controls/#w3>⁴⁹⁶⁵ <http://www.sans.org/critical-security-controls/#w5>⁴⁹⁶⁶ <http://www.sans.org/critical-security-controls/#w6>⁴⁹⁶⁷ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;147706>⁴⁹⁶⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>⁴⁹⁶⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>

		koristiti da bi se sprečilo prisluškivanje na FTP vezama.			
17.	NT IIS4 Remote Web-Based Administration Vulnerability (http-iis-0018)	172.23.202.101:80 Administriranje za IIS 4.0 je po defaultu ograničen na lokalnu mrežnu loopback adresu, 127.0.0.1. U slučajevima kada je IIS 4.0 instaliran kao nadogradnja IIS 2.0 ili 3.0, a prethodna verzija ISAPI DLL (ISM.DLL) je ostala u direktorijumu /scripts/iisadmin. Napadač može da pozove DLL preko sledeće sintakse: http://www.server.com/scripts/iisadmin/ism.dll?http/dir Ovaj URL traži od korisnika korisničko ime/lozinku da bi pristupio administrativnoj konzoli. Iako omogućen pristup ne dozvoljava korisnicima da vrši izmene na IIS serveru, može im dozvoliti da prikupe osetljive informacije o mrežnom serveru i njegovoj konfiguraciji.	BID 189 ⁴⁹⁷⁰ CVE CVE-1999-1538 ⁴⁹⁷¹ URL1 ⁴⁹⁷²	Ozbiljan	Izbrisati ISM.DLL iz direktorijuma /scripts/iisadmin.
18.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	172.23.202.101:135: Connection reset by peer Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hедера i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183 ⁴⁹⁷³ CERT TA04-111A ⁴⁹⁷⁴ CERT-VN: 415294 ⁴⁹⁷⁵ CVE CVE-2004-0230 ⁴⁹⁷⁶ MS: MS05-019 ⁴⁹⁷⁷ MS: MS06-064 ⁴⁹⁷⁸ NETBSD: NetBSD-SA2004-006 ⁴⁹⁷⁹ OSVDB 4030 ⁴⁹⁸⁰ OVAL: OVAL2689 ⁴⁹⁸¹ OVAL: OVAL270 ⁴⁹⁸² OVAL OVAL3508 ⁴⁹⁸³ OVAL OVAL4791 ⁴⁹⁸⁴ OVAL OVAL5711 ⁴⁹⁸⁵ SECUNIA: 11440 ⁴⁹⁸⁶ SECUNIA: 22341 ⁴⁹⁸⁷ SECUNIA 11458 ⁴⁹⁸⁸ SGI 20040403-01-A ⁴⁹⁸⁹ URL1 ⁴⁹⁹⁰ URL2 ⁴⁹⁹¹	Ozbiljan	Nema adekvatne zakrpe zbog prestanka podrške za ovaj OS. Rešenje : ažurirati sistem novijom verzijom operativnog sistema.
19.	FTP server uses predictable port	FTP server koristi sekvencijalne brojeve za portove za PASV FTP veze. FTP server je koristio portove	XF pasv-pizza-thief-dos(3389) ⁴⁹⁹²	Ozbiljan	Ažurirati verziju FTP servera i Operativnog sistema koji dodeljuje

⁴⁹⁷⁰ <http://www.securityfocus.com/bid/189>⁴⁹⁷¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-1538>⁴⁹⁷² <http://www.securityfocus.com/bid/189>⁴⁹⁷³ <http://www.securityfocus.com/bid/10183>⁴⁹⁷⁴ <http://www.us-cert.gov/ncas/alerts/ta04-111a>⁴⁹⁷⁵ <http://www.kb.cert.org/vuls/id/415294>⁴⁹⁷⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁴⁹⁷⁷ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁴⁹⁷⁸ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁴⁹⁷⁹ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁴⁹⁸⁰ <http://www.osvdb.org/4030>⁴⁹⁸¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>⁴⁹⁸² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>⁴⁹⁸³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>⁴⁹⁸⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>⁴⁹⁸⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>⁴⁹⁸⁶ <http://secunia.com/advisories/11440/>⁴⁹⁸⁷ <http://secunia.com/advisories/22341/>⁴⁹⁸⁸ <http://secunia.com/advisories/11458/>⁴⁹⁸⁹ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>⁴⁹⁹⁰ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁴⁹⁹¹ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>⁴⁹⁹² <http://xforce.iss.net/xforce/xfdb/3389>

	numbers for PASV connections (ftp-pasv-predictable-ports)	1030, 1031, 1032, 1033, 1034, što je predvidiv redosled. Ovo bi moglo olakšati napadaču da presretne ili prisvoji autorizovane FTP veze sa serverom i pristupi ili ukrade fajlove na FTP serveru. Ovo je uglavnom poznato kao napad "Pizza Thief"-a. FTP serveri bi trebalo da koriste pseudoslučajne brojeve za portove za PASV veze da bi otežali napadaču da prisvaja sesije. Važno je imati u vidu da na mnogim platformama brojeve portova bira operativni sistem, a ne FTP server. To ovu ranjivost čini još opasnijom, jer bi napadač mogao da iskoristi FTP serverov PASV mehanizam da predvidi brojeve portova za ostale (ne-FTP) servise.	CVE CVE-1999-0351 ⁴⁹⁹³ URL1 ⁴⁹⁹⁴ BID 5461 ⁴⁹⁹⁵ CERT-VN 2558 ⁴⁹⁹⁶ XF openunix-unixware-pasv-hijacking(9253) ⁴⁹⁹⁷ BID 4895 ⁴⁹⁹⁸ MSKB 260934 ⁴⁹⁹⁹		otvorene brojeve portova po naizmeničnom redosledu, a ne po redu. Uzeti u obzir da ažuriranje FTP servera bez ažuriranja operativnog sistema možda ne da željeni rezultat. Za IIS FTP servere na Windows 2000, ažuriranje na Windows 2000 Service Pack 1 će dati rezultat. Za više informacija pogledati Microsoft Knowledge Base Article Q260934 ⁵⁰⁰⁰ . Za wu-ftp servere ažurirati na verziju wu-ftp version 2.5.0 ili novije.
20.	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server. Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko poziva udaljenih procedura (RPC). Ovi servisi su i u prošlosti bili skloni ranjivostima.. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinjenije napade.	BID: 494 ⁵⁰⁰¹ CVE: CVE-1999-0519 ⁵⁰⁰² MSKB: 143474 ⁵⁰⁰³ URL1 ⁵⁰⁰⁴	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost.
21.	Database Open Access (database-open-access)	172.23.202.101:70 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posjedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7.	URL1 ⁵⁰⁰⁵	Umeren	Konfigurisati server baze podataka tako da se dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.
22.	Obsolete Version of	Proširena podrška za sve verzije	URL1 ⁵⁰⁰⁶	Kritičan	Nadograditi na verziju

⁴⁹⁹³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0351>⁴⁹⁹⁴ http://www.cert.org/tech_tips/ftp_port_attacks.html⁴⁹⁹⁵ <http://www.securityfocus.com/bid/5461>⁴⁹⁹⁶ <http://www.kb.cert.org/vuls/id/2558>⁴⁹⁹⁷ <http://xforce.iss.net/xforce/xfdb/9253>⁴⁹⁹⁸ <http://www.securityfocus.com/bid/4895>⁴⁹⁹⁹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;260934>⁵⁰⁰⁰ <http://smallbusiness.support.microsoft.com/en-au/kb/260934>⁵⁰⁰¹ <http://www.securityfocus.com/bid/494>⁵⁰⁰² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>⁵⁰⁰³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>⁵⁰⁰⁴ http://www.hsc.fr/ressources/presentations/null_sessions/⁵⁰⁰⁵ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf

Microsoft Windows NT (windows-nt-obsolete)	Windows NT se završila 31. decembra 2004. Verzije koje se ne podržavaju mogu da sadrže nezakrpljene propuste. Nadograditi na verziju koja je podržana.			Microsoft Windows-a koja je podržana.

Tabela 113. Windows OS sa IP adresama 172.23.202.112, 172.23.202.72, 172.23.202.71, 172.23.202.70 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.112		OS: Microsoft Windows 2003 Enterprise server x86 SP2, WIN2003ENSP2x86			9
IP adresa: 172.23.202.72		OS: Windows Server 2003 Enterprise x64 SP2, WIN2003ENSP2x64			9
IP adresa: 172.23.202.71		OS: Windows server 2003 Standard x86 SP2, WIN2003StX86sp2			9
IP adresa: 172.23.202.70		OS: Windows server 2003 Standard x64 SP2, WIN2003StX64sp2			9
Rbr	Ime ranjivosti	Opis ranjivosti	Izvori	Značaj	Rešenje ranjivosti
1.	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (windows-hotfix-ms08-067)	172.23.202.112:139 172.23.202.112:445 172.23.202.72:139 172.23.202.72:445 172.23.202.71:139 172.23.202.71:445 172.23.202.70:139 172.23.202.70:445 Ovo ažuriranje bezbednosti rešava privatno prijavljenu ranjivost. Ova ranjivost bi mogla da omogući izvršenje udaljenog kôda ukoliko bi napadnuti sistem primio posebno kreiran RPC zahtev. Na sistemima Microsoft Windows 2000, Windows XP i Windows Server 2003, napadač bi mogao da iskoristi ovu ranjivost bez autentičnosti da pokrene proizvoljan kôd. Moguće je iskoristiti ovu ranjivost da se kreira eksploatacija. Dosadašnja praksa fajervola i standardne fajervol difolt konfiguracije mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan organizacije.	BID 31874 ⁵⁰⁰⁷ CERT TA08-297A ⁵⁰⁰⁸ CERT TA09-088A ⁵⁰⁰⁹ CERT-VN 827267 ⁵⁰¹⁰ IAVM 2008-A-0081 ⁵⁰¹¹ OVAL OVAL6093 ⁵⁰¹² XF 46040 ⁵⁰¹³ MS: MS08-067 ⁵⁰¹⁴ MSKB: 958644 ⁵⁰¹⁵ CVE: CVE-2008-4250 ⁵⁰¹⁶ SECUNIA: 32326 ⁵⁰¹⁷ URL1 ⁵⁰¹⁸ URL2 ⁵⁰¹⁹ URL3 ⁵⁰²⁰ URL4 ⁵⁰²¹	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003-KB958644-x86-ENU.exe (702840 bytes) ⁵⁰²²

⁵⁰⁰⁶ <http://support.microsoft.com/lifecycle/?p1=3182>

⁵⁰⁰⁷ <http://www.securityfocus.com/bid/31874>

⁵⁰⁰⁸ <http://www.us-cert.gov/ncas/alerts/ta08-297a>

⁵⁰⁰⁹ <http://www.us-cert.gov/ncas/alerts/ta09-088a>

⁵⁰¹⁰ <http://www.kb.cert.org/vuls/id/827267>

⁵⁰¹¹ <http://iase.disa.mil/stigs/iavm-cve.html>

⁵⁰¹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6093>

⁵⁰¹³ <http://xforce.iss.net/xforce/xfdb/46040>

⁵⁰¹⁴ <http://technet.microsoft.com/en-us/security/bulletin/ms08-067>

⁵⁰¹⁵ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958644>

⁵⁰¹⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4250>

⁵⁰¹⁷ <http://secunia.com/advisories/32326/>

⁵⁰¹⁸ blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx

⁵⁰¹⁹ <http://blogs.msdn.com/b/sdl/archive/2008/10/22/ms08-067.aspx>

⁵⁰²⁰ <http://blogs.technet.com/b/msrc/archive/2008/10/23/ms08-067-released.aspx>

⁵⁰²¹ <http://technet.microsoft.com/en-us/security/bulletin/MS08-067>

⁵⁰²² download.windowsupdate.com/msdownload/update/software/secu/2008/10/windowsserver2003-kb958644-x86-enu_af4987620549ae4174e45ec5aa872f4a352f34c1.exe

2.	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (windows-hotfix-ms09-001)	172.23.202.112:139 172.23.202.112:445 172.23.202.72:139 172.23.202.72:445 172.23.202.71:139 172.23.202.71:445 172.23.202.70:139 172.23.202.70:445 Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti koje su privatno prijavljene, a odnose se na Microsoft Server Message Block (SMB). Ranjivosti mogu da omoguće daljinsko izvršenje koda na ugroženim sistemima. Napadač koji je uspešno iskoristio ove ranjivosti može da instalira programe, pregleda, menja ili briše podatke ili otvara nove naloge sa potpunim korisničkim pravima. Najbolje prakse zaštitnog zida i standardne konfiguracije zaštitnog zida po defaultu mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan okvira preduzeća. Za sisteme koji su stalno povezani na Internet preporuka je da imaju što manji broj izloženih portova.	BID 31179 ⁵⁰²³ BID 33121 ⁵⁰²⁴ BID 33122 ⁵⁰²⁵ CERT TA09-013A ⁵⁰²⁶ OVAL OVAL5248 ⁵⁰²⁷ OVAL OVAL5262 ⁵⁰²⁸ OVAL OVAL5863 ⁵⁰²⁹ OVAL OVAL6044 ⁵⁰³⁰ XF 45146 ⁵⁰³¹ MS: MS09-001 ⁵⁰³² MSKB: 958687 ⁵⁰³³ CVE: CVE-2008-4114 ⁵⁰³⁴ CVE: CVE-2008-4835 ⁵⁰³⁵ CVE: CVE-2008-4834 ⁵⁰³⁶ SECUNIA: 31883 ⁵⁰³⁷ URL1 ⁵⁰³⁸ URL2 ⁵⁰³⁹ URL3 ⁵⁰⁴⁰	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003-KB958687-x86-ENU.exe (736632 bytes) ⁵⁰⁴¹
3.	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-012)	172.23.202.112:139 172.23.202.112:445 172.23.202.72:139 172.23.202.72:445 172.23.202.71:139 172.23.202.71:445 172.23.202.70:139 172.23.202.70:445 Ovo ažuriranje bezbednosti rešava nekoliko privatno prijavljenih ranjivosti na Microsoft Windows-u.	CERT TA10-040A ⁵⁰⁴² OVAL OVAL7751 ⁵⁰⁴³ OVAL OVAL8314 ⁵⁰⁴⁴ OVAL OVAL8438 ⁵⁰⁴⁵ OVAL OVAL8524 ⁵⁰⁴⁶ MS: MS10-012 ⁵⁰⁴⁷ MSKB - 971468 ⁵⁰⁴⁸ CVE: CVE-2010-0020 ⁵⁰⁴⁹ CVE: CVE-2010-0021 ⁵⁰⁵⁰ CVE: CVE-2010-0022 ⁵⁰⁵¹ CVE CVE-2010-0231 ⁵⁰⁵²	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsServer2003-KB971468-x86-ENU.exe (681856 bytes) ⁵⁰⁵⁴

⁵⁰²³ <http://www.securityfocus.com/bid/31179>⁵⁰²⁴ <http://www.securityfocus.com/bid/33121>⁵⁰²⁵ <http://www.securityfocus.com/bid/33122>⁵⁰²⁶ <http://www.us-cert.gov/ncas/alerts/ta09-013a>⁵⁰²⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5248>⁵⁰²⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5262>⁵⁰²⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5863>⁵⁰³⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6044>⁵⁰³¹ <http://xforce.iss.net/xforce/xfdb/45146>⁵⁰³² <http://technet.microsoft.com/en-us/security/bulletin/MS09-001>⁵⁰³³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958687>⁵⁰³⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4114>⁵⁰³⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4835>⁵⁰³⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4834>⁵⁰³⁷ <http://secunia.com/advisories/31883/>⁵⁰³⁸ http://www.vallejo.cc/proyectos/vista_SMB_write_DoS.htm⁵⁰³⁹ <http://www.zerodayinitiative.com/advisories/ZDI-09-001/>⁵⁰⁴⁰ <http://www.zerodayinitiative.com/advisories/ZDI-09-002/>⁵⁰⁴¹ download.windowsupdate.com/msdownload/update/software/secu/2008/12/windowsserver2003-kb958687-x86-enu_7769ec8bf8869acd01fb8f9f63d79c23afbad5c6.exe⁵⁰⁴² <http://www.us-cert.gov/ncas/alerts/ta10-040a>⁵⁰⁴³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7751>⁵⁰⁴⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8314>⁵⁰⁴⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8438>⁵⁰⁴⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8524>⁵⁰⁴⁷ <http://technet.microsoft.com/en-us/security/bulletin/MS10-012>⁵⁰⁴⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;971468>⁵⁰⁴⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0020>⁵⁰⁵⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0021>⁵⁰⁵¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0022>⁵⁰⁵² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0231>

		Opasnost od ove ranjivosti leži u tome što bi ona omogućila daljinsko izvršavanje kôda ukoliko bi napadač kreirao posebno opremljen SMB paket i poslao ga ugroženom sistemu. Dosadašnja praksa fajervola i standardne fajervol difolt konfiguracije mogu da pomognu u zaštiti mrežnih resursa od napada (koji bi pokušali da iskoriste ove ranjivosti), a koji potiču izvan okvira organizacije.	SECUNIA 38510 ⁵⁰⁵³		
4.	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-054)	172.23.202.112:139 172.23.202.112:445 172.23.202.72:139 172.23.202.72:445 172.23.202.71:139 172.23.202.71:445 172.23.202.70:139 172.23.202.70:445 Opis je isti kao kod ranjivosti MS10-012	CERT TA10-222A ⁵⁰⁵⁵ OVAL OVAL11106 ⁵⁰⁵⁶ OVAL OVAL12015 ⁵⁰⁵⁷ OVAL OVAL12072 ⁵⁰⁵⁸ CVE: CVE-2010-2550 ⁵⁰⁵⁹ CVE: CVE-2010-2551 ⁵⁰⁶⁰ CVE: CVE-2010-2552 ⁵⁰⁶¹ MS: MS10-054 ⁵⁰⁶² MSKB 982214 ⁵⁰⁶³	Kritičan	Uraditi download a zatim instalirati Microsoft patch windowsserver2003-kb982214-x86-enu.exe (682880 bytes) ⁵⁰⁶⁴
5.	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms11-020)	172.23.202.112:139 172.23.202.112:445 172.23.202.72:139 172.23.202.72:445 172.23.202.71:139 172.23.202.71:445 172.23.202.70:139 172.23.202.70:445 Opis je isti kao kod ranjivosti MS10-012	BID 47198 ⁵⁰⁶⁵ CERT TA11-102A ⁵⁰⁶⁶ IAVM 2011-A-0050 ⁵⁰⁶⁷ OSVDB 71781 ⁵⁰⁶⁸ OVAL OVAL12076 ⁵⁰⁶⁹ SECUNIA 44072 ⁵⁰⁷⁰ CVE CVE-2011-0661 ⁵⁰⁷¹ MS: MS11-020 ⁵⁰⁷² MSKB: 2508429 ⁵⁰⁷³	Kritičan	Uraditi download a zatim instalirati Microsoft patch windowsserver2003-kb2508429-x86-enu.exe (693120 bytes) ⁵⁰⁷⁴
6.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.112:139 172.23.202.112:445 172.23.202.72:139 172.23.202.72:445 172.23.202.71:139 172.23.202.71:445 172.23.202.70:139 172.23.202.70:445 Ovaj sistem ne dozvoljava SMB	MSKB: 887429 ⁵⁰⁷⁵ URL1 ⁵⁰⁷⁶	Ozbiljan	Metoda za konfiguracije SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429 ⁵⁰⁷⁷ . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na

⁵⁰⁵⁴ download.windowsupdate.com/msdownload/update/software/secu/2010/01/windowsserver2003-kb971468-x86-enu_b6dcb60d113c4affd98b5bae0dfd1f5a785ae64d.exe

⁵⁰⁵³ <http://secunia.com/advisories/38510/>

⁵⁰⁵⁵ <http://www.us-cert.gov/ncas/alerts/ta10-222a>

⁵⁰⁵⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11106>

⁵⁰⁵⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12015>

⁵⁰⁵⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12072>

⁵⁰⁵⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2550>

⁵⁰⁶⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2551>

⁵⁰⁶¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2552>

⁵⁰⁶² <http://technet.microsoft.com/en-us/security/bulletin/MS10-054>

⁵⁰⁶³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;982214>

⁵⁰⁶⁴ download.windowsupdate.com/msdownload/update/software/secu/2010/07/windowsserver2003-kb982214-x86-enu_40e37ace02116c2baf27c14c7e3d1883887707e6.exe

⁵⁰⁶⁵ <http://www.securityfocus.com/bid/47198>

⁵⁰⁶⁶ <http://www.us-cert.gov/ncas/alerts/ta11-102a>

⁵⁰⁶⁷ <http://iase.disa.mil/stigs/iavm-cve.html>

⁵⁰⁶⁸ <http://www.osvdb.org/71781>

⁵⁰⁶⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12076>

⁵⁰⁷⁰ <http://secunia.com/advisories/44072/>

⁵⁰⁷¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661>

⁵⁰⁷² <http://technet.microsoft.com/en-us/security/bulletin/ms11-020>

⁵⁰⁷³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;2508429>

⁵⁰⁷⁴ download.windowsupdate.com/msdownload/update/software/secu/2011/03/windowsserver2003-kb2508429-x86-enu_1d4ff4ef7163f06d580e7fbc94cc222bafd0733f.exe

⁵⁰⁷⁵ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429>

⁵⁰⁷⁶ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>

⁵⁰⁷⁷ <http://support.microsoft.com/kb/887429>

		potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).			konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing</i> = <i>auto</i> ili da se zahteva SMB potpisivanje: <i>server signing</i> = <i>mandatory</i> .
7.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.112:139 172.23.202.112:445 172.23.202.72:139 172.23.202.72:445 172.23.202.71:139 172.23.202.71:445 172.23.202.70:139 172.23.202.70:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti.
8.	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server. Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko poziva udaljenih procedura (RPC). Ovi servisi su i u prošlosti bili skloni ranjivostima.. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinjenije napade.	BID: 494 ⁵⁰⁷⁸ CVE: CVE-1999-0519 ⁵⁰⁷⁹ MSKB: 143474 ⁵⁰⁸⁰ URL1 ⁵⁰⁸¹	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost.
9.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	OSVDB 95 ⁵⁰⁸² CVE: CVE-1999-0524 ⁵⁰⁸³ XF: icmp-netmask(306) ⁵⁰⁸⁴ XF: icmp-timestamp(322) ⁵⁰⁸⁵	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.

⁵⁰⁷⁸ <http://www.securityfocus.com/bid/494>⁵⁰⁷⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>⁵⁰⁸⁰ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>⁵⁰⁸¹ http://www.hsc.fr/ressources/presentations/null_sessions/⁵⁰⁸² <http://www.osvdb.org/95>⁵⁰⁸³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁵⁰⁸⁴ <http://xforce.iss.net/xforce/xfdb/306>⁵⁰⁸⁵ <http://xforce.iss.net/xforce/xfdb/322>

Tabela 114. Windows OS sa IP adresama 172.23.202.113, 172.23.202.89, 172.23.202.88, 172.23.202.87, 172.23.202.86, 172.23.202.85, 172.23.202.84, 172.23.202.83 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.113		OS: : Windows Vista ultimate x86, VISTAx86ULT			8
IP adresa: 172.23.202.89		OS: Windows Vista Home Basic x86, VISTAx86HoBa			8
IP adresa: 172.23.202.88		OS: Windows Vista Home Basic x64, VISTAx64HoBa			8
IP adresa: 172.23.202.87		OS: Windows Vista Home Premium x86, VISTAx86HoPre			8
IP adresa: 172.23.202.86		OS: Windows Vista Home Premium x64, VISTAx64HoPre			8
IP adresa: 172.23.202.85		OS: Windows Vista Business x86, VISTAx86Bsn			8
IP adresa: 172.23.202.84		OS: Windows Vista Business x64, VISTAx64Bsn			8
IP adresa: 172.23.202.83		OS: Windows Vista Ultimate x64, VISTAx64ULT			8
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (windows-hotfix-ms09-001)	172.23.202.113:139 172.23.202.113:445 172.23.202.89:139 172.23.202.89:445 172.23.202.88:139 172.23.202.88:445 172.23.202.87:139 172.23.202.87:445 172.23.202.86:139 172.23.202.86:445 172.23.202.85:139 172.23.202.85:445 172.23.202.84:139 172.23.202.84:445 172.23.202.83:139 172.23.202.83:445 Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti koje su privatno prijavljene, a odnose se na Microsoft Server Message Block (SMB). Ranjivosti mogu da omoguće daljinsko izvršenje koda na ugroženim sistemima. Napadač koji	BID 31179 ⁵⁰⁸⁶ BID 33121 ⁵⁰⁸⁷ BID 33122 ⁵⁰⁸⁸ CERT TA09-013A ⁵⁰⁸⁹ OVAL OVAL5248 ⁵⁰⁹⁰ OVAL OVAL5262 ⁵⁰⁹¹ OVAL OVAL5863 ⁵⁰⁹² OVAL OVAL6044 ⁵⁰⁹³ XF 45146 ⁵⁰⁹⁴ MS: MS09-001 ⁵⁰⁹⁵ MSKB: 958687 ⁵⁰⁹⁶ CVE: CVE-2008-4114 ⁵⁰⁹⁷ CVE: CVE-2008-4835 ⁵⁰⁹⁸ CVE: CVE-2008-4834 ⁵⁰⁹⁹ SECUNIA: 31883 ⁵¹⁰⁰ URL1 ⁵¹⁰¹ URL2 ⁵¹⁰² URL3 ⁵¹⁰³	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows6.0-KB958687-x86.cab (216319 bytes) ⁵¹⁰⁴ , ili za 64-bitnu verziju Windows6.0-KB958687-x64.msu ⁵¹⁰⁵

⁵⁰⁸⁶ <http://www.securityfocus.com/bid/31179>⁵⁰⁸⁷ <http://www.securityfocus.com/bid/33121>⁵⁰⁸⁸ <http://www.securityfocus.com/bid/33122>⁵⁰⁸⁹ <http://www.us-cert.gov/ncas/alerts/ta09-013a>⁵⁰⁹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5248>⁵⁰⁹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5262>⁵⁰⁹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5863>⁵⁰⁹³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6044>⁵⁰⁹⁴ <http://xforce.iss.net/xforce/xfdb/45146>⁵⁰⁹⁵ <http://technet.microsoft.com/en-us/security/bulletin/MS09-001>⁵⁰⁹⁶ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958687>⁵⁰⁹⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4114>⁵⁰⁹⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4835>⁵⁰⁹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4834>⁵¹⁰⁰ <http://secunia.com/advisories/31883/>⁵¹⁰¹ http://www.vallejo.cc/proyectos/vista_SMB_write_DoS.htm⁵¹⁰² <http://www.zerodayinitiative.com/advisories/ZDI-09-001/>⁵¹⁰³ <http://www.zerodayinitiative.com/advisories/ZDI-09-002/>⁵¹⁰⁴ download.windowsupdate.com/msdownload/update/software/secu/2008/12/windows6.0-kb958687-x86_48df8df9513e517d7db0a4a75ed2b260c5b7acbf.cab⁵¹⁰⁵ <http://download.microsoft.com/download/7/5/9/759DF890-E7DB-471C-B52A-E03712BBD616/Windows6.0-KB958687-x64.msu>

		je uspešno iskoristion ove ranjivosti može da instalira programe, pregleda, menja ili briše podatke ili otvara nove naloge sa potpunim korisničkim pravima. Najbolje prakse zaštitnog zida i standardne konfiguracije zaštitnog zida po difoltu mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan okvira preduzeća. Za sisteme koji su stalno povezani na Internet preporuka je da imaju što manji broj izloženih portova.			
2.	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-012)	172.23.202.113:139 172.23.202.113:445 172.23.202.89:139 172.23.202.89:445 172.23.202.88:139 172.23.202.88:445 172.23.202.87:139 172.23.202.87:445 172.23.202.86:139 172.23.202.86:445 172.23.202.85:139 172.23.202.85:445 172.23.202.84:139 172.23.202.84:445 172.23.202.83:139 172.23.202.83:445 Ovo ažuriranje bezbednosti rešava nekoliko privatno prijavljenih ranjivosti na Microsoft Windows-u. Opasnost od ove ranjivosti leži u tome što bi ona omogućila daljinsko izvršavanje kôda ukoliko bi napadač kreirao posebno opremljen SMB paket i poslao ga ugroženom sistemu. Dosadašnja praksa fajervola i standardne fajervol difolt konfiguracije mogu da pomognu u zaštiti mrežnih resursa od napada (koji bi pokušali da iskoriste ove ranjivosti), a koji potiču izvan okvira organizacije.	TA10-040A ⁵¹⁰⁶ OVAL OVAL7751 ⁵¹⁰⁷ OVAL OVAL8314 ⁵¹⁰⁸ OVAL OVAL8438 ⁵¹⁰⁹ OVAL OVAL8524 ⁵¹¹⁰ MS: MS10-012 ⁵¹¹¹ MSKB - 971468 ⁵¹¹² CVE: CVE-2010-0020 ⁵¹¹³ CVE: CVE-2010-0021 ⁵¹¹⁴ CVE: CVE-2010-0022 ⁵¹¹⁵ CVE CVE-2010-0231 ⁵¹¹⁶ SECUNIA 38510 ⁵¹¹⁷	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows6.0-KB971468-x86.cab (319207 bytes) ⁵¹¹⁸ , ili za 64-bitnu verziju Windows6.0-KB971468-x64.msu ⁵¹¹⁹
3.	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution	172.23.202.113:139 172.23.202.113:445 172.23.202.89:139 172.23.202.89:445 172.23.202.88:139	CERT TA10-222A ⁵¹²⁰ OVAL OVAL11106 ⁵¹²¹ OVAL OVAL12015 ⁵¹²² OVAL OVAL12072 ⁵¹²³ CVE: CVE-2010-2550 ⁵¹²⁴	Kritičan	Uraditi download a zatim instalirati Microsoft patch windows6.0-kb982214-x86.cab (325694 bytes) ⁵¹²⁹ ,

⁵¹⁰⁶ <http://www.us-cert.gov/ncas/alerts/ta10-040a>⁵¹⁰⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7751>⁵¹⁰⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8314>⁵¹⁰⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8438>⁵¹¹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8524>⁵¹¹¹ <http://technet.microsoft.com/en-us/security/bulletin/MS10-012>⁵¹¹² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;971468>⁵¹¹³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0020>⁵¹¹⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0021>⁵¹¹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0022>⁵¹¹⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0231>⁵¹¹⁷ <http://secunia.com/advisories/38510/>⁵¹¹⁸ download.windowsupdate.com/msdownload/update/software/secu/2010/01/windows6.0-kb971468-x86_673ca9ff1fae6a26038f2e8764d07033c451de06.cab⁵¹¹⁹ <http://download.microsoft.com/download/8/D/7/8D7713E1-543D-434E-B80B-48495CC2244B/Windows6.0-KB971468-x64.msu>⁵¹²⁰ <http://www.us-cert.gov/ncas/alerts/ta10-222a>⁵¹²¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11106>⁵¹²² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12015>⁵¹²³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12072>⁵¹²⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2550>

	(windows-hotfix-ms10-054)	172.23.202.88:445 172.23.202.87:139 172.23.202.87:445 172.23.202.86:139 172.23.202.86:445 172.23.202.85:139 172.23.202.85:445 172.23.202.84:139 172.23.202.84:445 172.23.202.83:139 172.23.202.83:445 Opis je isti kao kod ranjivosti MS10-012	CVE: CVE-2010-2551 ⁵¹²⁵ CVE: CVE-2010-2552 ⁵¹²⁶ MS: MS10-054 ⁵¹²⁷ MSKB: 982214 ⁵¹²⁸		ili za 64-bitnu verziju Windows6.0-KB982214-x64.msu ⁵¹³⁰
4.	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms11-020)	172.23.202.113:139 172.23.202.113:445 172.23.202.89:139 172.23.202.89:445 172.23.202.88:139 172.23.202.88:445 172.23.202.87:139 172.23.202.87:445 172.23.202.86:139 172.23.202.86:445 172.23.202.85:139 172.23.202.85:445 172.23.202.84:139 172.23.202.84:445 172.23.202.83:139 172.23.202.83:445 Opis je isti kao kod ranjivosti MS10-012	BID 47198 ⁵¹³¹ CERT TA11-102A ⁵¹³² IAVM 2011-A-0050 ⁵¹³³ OSVDB 71781 ⁵¹³⁴ OVAL OVAL12076 ⁵¹³⁵ SECUNIA 44072 ⁵¹³⁶ CVE CVE-2011-0661 ⁵¹³⁷ MS: MS11-020 ⁵¹³⁸ MSKB: 2508429 ⁵¹³⁹	Kritičan	Uraditi download a zatim instalirati Microsoft patch windows6.0-kb2508429-x86.cab (332927 bytes) ⁵¹⁴⁰ ili za 64-bitnu verziju Windows6.0-KB2508429-x64.msu ⁵¹⁴¹
5.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.113:139 172.23.202.113:445 172.23.202.89:139 172.23.202.89:445 172.23.202.88:139 172.23.202.88:445 172.23.202.87:139 172.23.202.87:445 172.23.202.86:139 172.23.202.86:445 172.23.202.85:139 172.23.202.85:445 172.23.202.84:139 172.23.202.84:445 172.23.202.83:139 172.23.202.83:445	MSKB: 887429 ⁵¹⁴² URL ⁵¹⁴³	Ozbiljan	Metoda za konfiguracije SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429. ⁵¹⁴⁴ Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: server signing = auto ili da se zahteva SMB potpisivanje: <i>server signing = mandatory</i>

⁵¹²⁹ download.windowsupdate.com/msdownload/update/software/secu/2010/07/windows6.0-kb982214-x86_50d77476159fef060a2470a0f66e7e8ecb9808ea.cab

⁵¹²⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2551>

⁵¹²⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2552>

⁵¹²⁷ <http://technet.microsoft.com/en-us/security/bulletin/MS10-054>

⁵¹²⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;982214>

⁵¹³⁰ <http://download.microsoft.com/download/5/8/D/58D3BE5D-9C2F-45DB-84C0-638AC2BEF57D/Windows6.0-KB982214-x64.msu>

⁵¹³¹ <http://www.securityfocus.com/bid/47198>

⁵¹³² <http://www.us-cert.gov/ncas/alerts/ta11-102a>

⁵¹³³ <http://iase.disa.mil/stigs/iavm-cve.html>

⁵¹³⁴ <http://www.osvdb.org/71781>

⁵¹³⁵ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:12076>

⁵¹³⁶ <http://secunia.com/advisories/44072/>

⁵¹³⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661>

⁵¹³⁸ <http://technet.microsoft.com/en-us/security/bulletin/ms11-020>

⁵¹³⁹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;2508429>

⁵¹⁴⁰ download.windowsupdate.com/msdownload/update/software/secu/2011/03/windows6.0-kb2508429-x86_2e7adf8e8e545432372edbd59952a925fb7a69da.cab

⁵¹⁴¹ <http://download.microsoft.com/download/2/1/8/218341B5-0F6A-4359-8929-27D166C98031/Windows6.0-KB2508429-x64.msu>

⁵¹⁴² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429>

⁵¹⁴³ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>

⁵¹⁴⁴ <http://support.microsoft.com/kb/887429>

		Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).			
6.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.113:139 172.23.202.113:445 172.23.202.89:139 172.23.202.89:445 172.23.202.88:139 172.23.202.88:445 172.23.202.87:139 172.23.202.87:445 172.23.202.86:139 172.23.202.86:445 172.23.202.85:139 172.23.202.85:445 172.23.202.84:139 172.23.202.84:445 172.23.202.83:139 172.23.202.83:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti.	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti.
7.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	OSVDB 95 ⁵¹⁴⁵ CVE: CVE-1999-0524 ⁵¹⁴⁶ XF: icmp-netmask(306) ⁵¹⁴⁷ XF: icmp-timestamp(322) ⁵¹⁴⁸	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
8.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1 ⁵¹⁴⁹ URL2 ⁵¹⁵⁰ URL3 ⁵¹⁵¹	Umeren	Onemogućavanje TCP timestamp odgovora na Windows OS. Podesiti Tcp1323Opts vrednost na sledećem ključu na 1: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters Od Windows Viste onemogućavanja TCP timestamp nije moguće pa se to radi uz pomoć fajerevola.

⁵¹⁴⁵ <http://www.osvdb.org/95>⁵¹⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁵¹⁴⁷ <http://xforce.iss.net/xforce/xfdb/306>⁵¹⁴⁸ <http://xforce.iss.net/xforce/xfdb/322>⁵¹⁴⁹ http://www.forensicswiki.org/wiki/TCP_timestamps⁵¹⁵⁰ <http://www.ietf.org/rfc/rfc1323.txt>⁵¹⁵¹ <http://uptime.netcraft.com/>

Tabela 115. Windows OS sa IP adresama 172.23.202.114, 172.23.202.82, 172.23.202.81, 172.23.202.80, 172.23.202.79, 172.23.202.78, 172.23.202.77 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara		Broj ranjivosti	
IP adresa: 172.23.202.114		OS: : Microsoft Windows Vista ultimate x86 SP2, VISTAx86ULTSP2		7	
IP adresa: 172.23.202.82		OS: Windows Vista Home Basic x86 SP2, VISTAx86HoBaSp2		7	
IP adresa: 172.23.202.81		OS: Windows Vista Home Basic x64 SP2, VISTAx64HoBaSp2		7	
IP adresa: 172.23.202.80		OS: Windows Vista Business x86 SP2, VISTAx86BsnSp2		7	
IP adresa: 172.23.202.79		OS: Windows Vista Business x64 SP2, VISTAx64BsnSp2		7	
IP adresa: 172.23.202.78		OS: Windows Vista Home Premium x86 SP2, VISTAx86HoPrSp2		7	
IP adresa: 172.23.202.77		OS: Windows Vista Home Premium x64 SP2, VISTAx64HoPrSp2		7	
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	MS09-050: Vulnerabilities in SMBv2 Could Allow Remote Code Execution (windows-hotfix-ms09-050)	Ovo ažuriranje bezbednosti rešava nekoliko privatno prijavljenih ranjivosti, a odnose se na protokol Microsoft Server Message Block-a Version 2 (SMBv2). Ove ranjivosti bi mogle da omoguće izvršenje udaljenog kôda na napadnutim sistemima. Dosadašnja praksa fajervola i standardne fajervol difolt konfiguracije mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan organizacije. Za sisteme koji su stalno povezani na Internet preporuka je da imaju što manji broj izloženih portova.	BID 36299 ⁵¹⁵² CERT TA09-286A ⁵¹⁵³ CERT-VN 135940 ⁵¹⁵⁴ OSVDB 57799 ⁵¹⁵⁵ OVAL OVAL5595 ⁵¹⁵⁶ OVAL OVAL6336 ⁵¹⁵⁷ OVAL OVAL6489 ⁵¹⁵⁸ XF 53090 ⁵¹⁵⁹ MS MS09-050 ⁵¹⁶⁰ MSKB 975517 ⁵¹⁶¹ CVE CVE-2009-2526 ⁵¹⁶² CVE CVE-2009-2532 ⁵¹⁶³ CVE CVE-2009-3103 ⁵¹⁶⁴ SECUNIA 36623 ⁵¹⁶⁵ URL1 ⁵¹⁶⁶	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows6.0-KB975517-x86.cab (197912 bytes) ⁵¹⁶⁷ , ili za 64-bitnu verziju Windows6.0-KB975517-x64.msu ⁵¹⁶⁸
2.	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-054)	172.23.202.114:139 172.23.202.114:445 172.23.202.82:139 172.23.202.82:445 172.23.202.81:139 172.23.202.81:445	CERT TA10-222A ⁵¹⁶⁹ OVAL OVAL11106 ⁵¹⁷⁰ OVAL OVAL12015 ⁵¹⁷¹ OVAL OVAL12072 ⁵¹⁷² CVE: CVE-2010-2550 ⁵¹⁷³ CVE: CVE-2010-2551 ⁵¹⁷⁴	Kritičan	Uraditi download a zatim instalirati Microsoft patch windows6.0-kb982214-x86.cab (325694 bytes) ⁵¹⁷⁸ , ili za 64-bitnu verziju

⁵¹⁵² <http://www.securityfocus.com/bid/36299>⁵¹⁵³ <http://www.us-cert.gov/ncas/alerts/ta09-286a>⁵¹⁵⁴ <http://www.kb.cert.org/vuls/id/135940>⁵¹⁵⁵ <http://www.osvdb.org/57799>⁵¹⁵⁶ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:5595>⁵¹⁵⁷ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:6336>⁵¹⁵⁸ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:6489>⁵¹⁵⁹ <http://xforce.iss.net/xforce/xfdb/53090>⁵¹⁶⁰ <http://technet.microsoft.com/en-us/security/bulletin/MS09-050>⁵¹⁶¹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;975517>⁵¹⁶² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2526>⁵¹⁶³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2532>⁵¹⁶⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3103>⁵¹⁶⁵ <http://secunia.com/advisories/36623/>⁵¹⁶⁶ <http://g-laurent.blogspot.com/2009/09/windows-vista7-smb20-negotiate-protocol.html>⁵¹⁶⁷ download.windowsupdate.com/msdownload/update/software/secu/2009/09/windows6.0-kb975517-x86_dc06aeba89a24a1f1aa016bf6f0d10e76eca34d.cab⁵¹⁶⁸ <http://download.microsoft.com/download/9/3/F/93F97002-436E-47FF-8D46-725F6150E53E/Windows6.0-KB975517-x64.msu>⁵¹⁶⁹ <http://www.us-cert.gov/ncas/alerts/ta10-222a>⁵¹⁷⁰ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:11106>⁵¹⁷¹ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:12015>⁵¹⁷² <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:12072>⁵¹⁷³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2550>⁵¹⁷⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2551>

	054)	172.23.202.80:139 172.23.202.80:445 172.23.202.79:139 172.23.202.79:445 172.23.202.78:139 172.23.202.78:445 172.23.202.77:139 172.23.202.77:445 Opis je isti kao kod ranjivosti MS10-012	CVE: CVE-2010-2552 ⁵¹⁷⁵ MS: MS10-054 ⁵¹⁷⁶ MSKB 982214 ⁵¹⁷⁷		Windows6.0-KB982214-x64.msu ⁵¹⁷⁹
3.	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms11-020)	172.23.202.114:139 172.23.202.114:445 172.23.202.82:139 172.23.202.82:445 172.23.202.81:139 172.23.202.81:445 172.23.202.80:139 172.23.202.80:445 172.23.202.79:139 172.23.202.79:445 172.23.202.78:139 172.23.202.78:445 172.23.202.77:139 172.23.202.77:445 Opis je isti kao kod ranjivosti MS10-012	BID 47198 ⁵¹⁸⁰ CERT TA11-102A ⁵¹⁸¹ IAVM 2011-A-0050 ⁵¹⁸² OSVDB 71781 ⁵¹⁸³ OVAL OVAL12076 ⁵¹⁸⁴ SECUNIA 44072 ⁵¹⁸⁵ CVE CVE-2011-0661 ⁵¹⁸⁶ MS: MS11-020 ⁵¹⁸⁷ MSKB: 2508429 ⁵¹⁸⁸	Kritičan	Uraditi download a zatim instalirati Microsoft patch windows6.0-kb2508429-x86.cab (332927 bytes) ⁵¹⁸⁹ , ili za 64-bitnu verziju Windows6.0-KB2508429-x64.msu ⁵¹⁹⁰
4.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.114:139 172.23.202.114:445 172.23.202.82:139 172.23.202.82:445 172.23.202.81:139 172.23.202.81:445 172.23.202.80:139 172.23.202.80:445 172.23.202.79:139 172.23.202.79:445 172.23.202.78:139 172.23.202.78:445 172.23.202.77:139 172.23.202.77:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen	MSKB: 887429 ⁵¹⁹¹ URL1 ⁵¹⁹²	Ozbiljan	Metoda za konfiguracije SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429 ⁵¹⁹³ . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing</i> = <i>auto</i> ili da se zahteva SMB potpisivanje: <i>server signing</i> = <i>mandatory</i> .

⁵¹⁷⁸ [download.windowsupdate.com/msdownload/update/software/secu/2010/07/windows6.0-kb982214-](http://download.windowsupdate.com/msdownload/update/software/secu/2010/07/windows6.0-kb982214-x86_50d77476159fef060a2470a0f66e7e8ecb9808ea.cab)[x86_50d77476159fef060a2470a0f66e7e8ecb9808ea.cab](http://download.windowsupdate.com/msdownload/update/software/secu/2010/07/windows6.0-kb982214-x86_50d77476159fef060a2470a0f66e7e8ecb9808ea.cab)⁵¹⁷⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2552>⁵¹⁷⁶ <http://technet.microsoft.com/en-us/security/bulletin/MS10-054>⁵¹⁷⁷ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;982214>⁵¹⁷⁹ <http://download.microsoft.com/download/5/8/D/58D3BE5D-9C2F-45DB-84C0-638AC2BEF57D/Windows6.0-KB982214-x64.msu>⁵¹⁸⁰ <http://www.osvdb.org/bid/47198>⁵¹⁸¹ <http://www.us-cert.gov/ncas/alerts/ta11-102a>⁵¹⁸² <http://iase.disa.mil/stigs/iavm-cve.html>⁵¹⁸³ <http://www.osvdb.org/71781>⁵¹⁸⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12076>⁵¹⁸⁵ <http://secunia.com/advisories/44072/>⁵¹⁸⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661>⁵¹⁸⁷ <http://technet.microsoft.com/en-us/security/bulletin/ms11-020>⁵¹⁸⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;2508429>⁵¹⁸⁹ [download.windowsupdate.com/msdownload/update/software/secu/2011/03/windows6.0-kb2508429-](http://download.windowsupdate.com/msdownload/update/software/secu/2011/03/windows6.0-kb2508429-x86_2e7adf8e8e545432372edbd59952a925fb7a69da.cab)[x86_2e7adf8e8e545432372edbd59952a925fb7a69da.cab](http://download.windowsupdate.com/msdownload/update/software/secu/2011/03/windows6.0-kb2508429-x86_2e7adf8e8e545432372edbd59952a925fb7a69da.cab)⁵¹⁹⁰ <http://download.microsoft.com/download/2/1/8/218341B5-0F6A-4359-8929-27D166C98031/Windows6.0-KB2508429-x64.msu>⁵¹⁹¹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429>⁵¹⁹² <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>⁵¹⁹³ <http://support.microsoft.com/kb/887429>

		(najmanje bezbedno), omogućen i zahtevan (najsigurnije).			
5.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.114:139 172.23.202.114:445 172.23.202.82:139 172.23.202.82:445 172.23.202.81:139 172.23.202.81:445 172.23.202.80:139 172.23.202.80:445 172.23.202.79:139 172.23.202.79:445 172.23.202.78:139 172.23.202.78:445 172.23.202.77:139 172.23.202.77:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti.
6.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatišu slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	OSVDB 95 ⁵¹⁹⁴ CVE: CVE-1999-0524 ⁵¹⁹⁵ XF: icmp-netmask(306) ⁵¹⁹⁶ XF: icmp-timestamp(322) ⁵¹⁹⁷	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
7.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1 ⁵¹⁹⁸ URL2 ⁵¹⁹⁹ URL3 ⁵²⁰⁰	Umeren	Onemogućavanje TCP timestamp odgovora na Windows OS. Podesiti Tcp1323Opts vrednost na sledećem ključu na 1: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters Od Windows Viste onemogućavanja TCP timestamp nije moguće pa se to radi uz pomoć fajerevola.

Tabela 116. Windows OS sa IP adresama 172.23.202.117, 172.23.202.68 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara		Broj ranjivosti	
IP adresa: 172.23.202.117		OS: : Microsoft Windows 2008 Datacenter x86 SP1, 2008DTCX86SP1		7	
IP adresa: 172.23.202.68		Wwindows 2008 server Enterprise x86 SP1, 2008EntX86SP1		7	
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti

⁵¹⁹⁴ <http://www.osvdb.org/95>⁵¹⁹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁵¹⁹⁶ <http://xforce.iss.net/xforce/xfdb/306>⁵¹⁹⁷ <http://xforce.iss.net/xforce/xfdb/322>⁵¹⁹⁸ http://www.forensicswiki.org/wiki/TCP_timestamps⁵¹⁹⁹ <http://www.ietf.org/rfc/rfc1323.txt>⁵²⁰⁰ <http://uptime.netcraft.com/>

1.	MS09-050: Vulnerabilities in SMBv2 Could Allow Remote Code Execution (windows-hotfix-ms09-050)	Ovo ažuriranje bezbednosti rešava nekoliko privatno prijavljenih ranjivosti, a odnose se na protokol Microsoft Server Message Block-a Version 2 (SMBv2). Ove ranjivosti bi mogle da omoguće izvršenje udaljenog kôda na napadnutim sistemima. Dosadašnja praksa fajervola i standardne fajervol difolt konfiguracije mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan organizacije. Za sisteme koji su stalno povezani na Internet preporuka je da imaju što manji broj izloženih portova.	BID 36299 ⁵²⁰¹ CERT TA09-286A ⁵²⁰² CERT-VN 135940 ⁵²⁰³ OSVDB 57799 ⁵²⁰⁴ OVAL OVAL5595 ⁵²⁰⁵ OVAL OVAL6336 ⁵²⁰⁶ OVAL OVAL6489 ⁵²⁰⁷ XF 53090 ⁵²⁰⁸ MS MS09-050 ⁵²⁰⁹ MSKB 975517 ⁵²¹⁰ CVE CVE-2009-2526 ⁵²¹¹ CVE CVE-2009-2532 ⁵²¹² CVE CVE-2009-3103 ⁵²¹³ SECUNIA 36623 ⁵²¹⁴ URL1 ⁵²¹⁵	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windows6.0-KB975517-x86.cab (197912 bytes) ⁵²¹⁶
2.	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-054)	172.23.202.117:139 172.23.202.117:445 172.23.202.68:139 172.23.202.68:445 Opis je isti kao kod ranjivosti MS10-012	CERT TA10-222A ⁵²¹⁷ OVAL OVAL11106 ⁵²¹⁸ OVAL OVAL12015 ⁵²¹⁹ OVAL OVAL12072 ⁵²²⁰ CVE: CVE-2010-2550 ⁵²²¹ CVE: CVE-2010-2551 ⁵²²² CVE: CVE-2010-2552 ⁵²²³ MS: MS10-054 ⁵²²⁴ MSKB 982214 ⁵²²⁵	Kritičan	Uraditi download a zatim instalirati Microsoft patch windows6.0-kb982214-x86.cab (325694 bytes) ⁵²²⁶
3.	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms11-020)	172.23.202.117:139 172.23.202.117:445 172.23.202.68:139 172.23.202.68:445 Opis je isti kao kod ranjivosti MS10-012	BID 47198 ⁵²²⁷ CERT TA11-102A ⁵²²⁸ IAVM 2011-A-0050 ⁵²²⁹ OSVDB 71781 ⁵²³⁰ OVAL OVAL12076 ⁵²³¹ SECUNIA 44072 ⁵²³² CVE-2011-0661 ⁵²³³ MS: MS11-020 ⁵²³⁴	Kritičan	Uraditi download a zatim instalirati Microsoft patch windows6.0-kb2508429-x86.cab (332927 bytes) ⁵²³⁶

⁵²⁰¹ <http://www.securityfocus.com/bid/36299>⁵²⁰² <http://www.us-cert.gov/ncas/alerts/ta09-286a>⁵²⁰³ <http://www.kb.cert.org/vuls/id/135940>⁵²⁰⁴ <http://www.osvdb.org/57799>⁵²⁰⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5595>⁵²⁰⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6336>⁵²⁰⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6489>⁵²⁰⁸ <http://xforce.iss.net/xforce/xfdb/53090>⁵²⁰⁹ <http://technet.microsoft.com/en-us/security/bulletin/MS09-050>⁵²¹⁰ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;975517>⁵²¹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2526>⁵²¹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2532>⁵²¹³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3103>⁵²¹⁴ <http://secunia.com/advisories/36623/>⁵²¹⁵ <http://g-laurent.blogspot.com/2009/09/windows-vista7-smb20-negotiate-protocol.html>⁵²¹⁶ download.windowsupdate.com/msdownload/update/software/secu/2009/09/windows6.0-kb975517-x86_dc06eae8a89a24a1f1aa016bf6fd10e76eca34d.cab⁵²¹⁷ <http://www.us-cert.gov/ncas/alerts/ta10-222a>⁵²¹⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11106>⁵²¹⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12015>⁵²²⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12072>⁵²²¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2550>⁵²²² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2551>⁵²²³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2552>⁵²²⁴ <http://technet.microsoft.com/en-us/security/bulletin/MS10-054>⁵²²⁵ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;982214>⁵²²⁶ download.windowsupdate.com/msdownload/update/software/secu/2010/07/windows6.0-kb982214-x86_50d77476159fef060a2470a0f66e7e8ecb9808ea.cab⁵²²⁷ <http://www.securityfocus.com/bid/47198>⁵²²⁸ <http://www.us-cert.gov/ncas/alerts/ta11-102a>⁵²²⁹ <http://iase.disa.mil/stigs/iavm-cve.html>⁵²³⁰ <http://www.osvdb.org/71781>⁵²³¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12076>⁵²³² secunia.com/advisories/44072/⁵²³³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661>⁵²³⁴ <http://technet.microsoft.com/en-us/security/bulletin/ms11-020>

			MSKB: 2508429 ⁵²³⁵		
4.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.117:139 172.23.202.117:445 172.23.202.68:139 172.23.202.68:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB: 887429 ⁵²³⁷ URL1 ⁵²³⁸	Ozbiljan	Metoda za konfiguracije SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429 ⁵²³⁹ . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing</i> = <i>auto</i> ili da se zahteva SMB potpisivanje: <i>server signing</i> = <i>mandatory</i> .
5.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.117:139 172.23.202.117:445 172.23.202.68:139 172.23.202.68:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti.	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti.
6.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatišu slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	OSVDB 95 ⁵²⁴⁰ CVE: CVE-1999-0524 ⁵²⁴¹ XF: icmp-netmask(306) ⁵²⁴² XF: icmp-timestamp(322) ⁵²⁴³	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
7.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1 ⁵²⁴⁴ URL2 ⁵²⁴⁵ URL3 ⁵²⁴⁶	Umeren	Onemogućavanje TCP timestamp odgovora na Windows OS. Podesiti Tcp1323Opts vrednost na sledećem ključu na 1: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters Od Windows Viste onemogućavanja TCP timestamp nije moguće pa se to radi uz pomoć fajerevola.

⁵²³⁶ [download.windowsupdate.com/msdownload/update/software/secu/2011/03/windows6.0-kb2508429-](http://download.windowsupdate.com/msdownload/update/software/secu/2011/03/windows6.0-kb2508429-x86_2e7adf8e8e545432372edbd59952a925fb7a69da.cab)⁵²³⁵ support.microsoft.com/default.aspx?scid=kb;EN-US;2508429⁵²³⁷ support.microsoft.com/default.aspx?scid=kb;EN-US;887429⁵²³⁸ blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx⁵²³⁹ support.microsoft.com/kb/887429⁵²⁴⁰ www.osvdb.org/95⁵²⁴¹ web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524⁵²⁴² xforce.iss.net/xforce/xfdb/306⁵²⁴³ xforce.iss.net/xforce/xfdb/322⁵²⁴⁴ www.forensicswiki.org/wiki/TCP_timestamps⁵²⁴⁵ www.ietf.org/rfc/rfc1323.txt⁵²⁴⁶ uptime.netcraft.com/

Tabela 117. Windows OS sa IP adresom 172.23.202.108 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.108		OS: : Microsoft Windows XP Pro Sp3 x86, WINXPproSP3x86			4
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.108:139 172.23.202.108:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB: 887429 ⁵²⁴⁷ URL ⁵²⁴⁸	Ozbiljan	Metoda za konfiguracije SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429 ⁵²⁴⁹ . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing = auto</i> ili da se zahteva SMB potpisivanje: <i>server signing = mandatory</i> .
2.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.108:139 172.23.202.108:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti.	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti.
3.	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server. Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko poziva udaljenih procedura (RPC). Ovi servisi su i u prošlosti bili skloni ranjivostima.. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinjenije napade.	BID: 494 ⁵²⁵⁰ CVE: CVE-1999-0519 ⁵²⁵¹ MSKB: 143474 ⁵²⁵² URL ⁵²⁵³	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost.
4.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatišu slabe time-based generatore slučajnih	OSVDB 95 ⁵²⁵⁴ CVE: CVE-1999-0524 ⁵²⁵⁵ XF: icmp-netmask(306) ⁵²⁵⁶ XF: icmp-timestamp(322) ⁵²⁵⁷	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti

⁵²⁴⁷ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429>⁵²⁴⁸ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>⁵²⁴⁹ <http://support.microsoft.com/kb/887429>⁵²⁵⁰ <http://www.securityfocus.com/bid/494>⁵²⁵¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>⁵²⁵² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>⁵²⁵³ http://www.hsc.fr/ressources/presentations/null_sessions/⁵²⁵⁴ <http://www.osvdb.org/95>⁵²⁵⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁵²⁵⁶ <http://xforce.iss.net/xforce/xfdb/306>⁵²⁵⁷ <http://xforce.iss.net/xforce/xfdb/322>

		brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.			detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.

Tabela 118. Windows OS sa IP adresom 172.23.202.105 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.105		OS: : Microsoft Windows XP Professional x86, WINXPprox86			15
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Microsoft Server Service / CanonicalizePathName() Remote Code Execution Vulnerability (dcerpc-msnetapi-netpathcanonicalize-dos)	Određene verzije Microsoft Windows-a su ranjive na daljinsko preopterećenje bafera (privremene memorije) koje bi moglo da kompromituje određeni računar. Posebno izrađen paket se može koristiti sa pozivom ka NetPathCanonicalize RPC ruti na servisu servera, pri čemu bi napadač mogao da izvrši kôd pod sistemskim nivoom pristupa.	BID 19409 ⁵²⁵⁸ CERT TA06-220A ⁵²⁵⁹ CERT-VN 650769 ⁵²⁶⁰ OVAL OVAL492 ⁵²⁶¹ SECUNIA 21388 ⁵²⁶² XF ms-server-service-bo(28002) ⁵²⁶³ CVE: CVE-2006-3439 ⁵²⁶⁴ , MS: MS06-040 ⁵²⁶⁵ , MSKB: 921883 ⁵²⁶⁶ , SANS-06: W4 ⁵²⁶⁷ , SANS-07: S2 ⁵²⁶⁸	Kritičan	Instalirati Microsoft service pack Windows XP Service Pack 1 Uraditi download a zatim instalirati Microsoft patch WindowXP-KB921883-x86-ENU.EXE ⁵²⁶⁹
2.	MS03-039: Buffer Overrun In RPCSS Service Could Allow Code Execution (824146) (windows-hotfix-ms03-039)	Napadač koji bi uspešno iskoristio ove ranjivosti mogao bi da pokrene kôd sa privilegijama lokalnog sistema na napadnutom sistemu, ili bi mogao da prouzrokuje isključenje RPCSS servisa. Napadač bi tada bio u mogućnosti da preduzme bilo kakvu akciju na sistemu, uključujući instaliranje programa, pregledanje, menjanje ili brisanje podataka ili otvaranje novih naloga sa svih privilegijama. Da bi iskoristio ove ranjivosti, napadač bi morao da	CERT CA-2003-19 ⁵²⁷⁰ CERT CA-2003-23 ⁵²⁷¹ CERT-VN 254236 ⁵²⁷² CERT-VN 326746 ⁵²⁷³ CERT-VN 483492 ⁵²⁷⁴ CVE CVE-2003-0995 ⁵²⁷⁵ OVAL OVAL1118 ⁵²⁷⁶ OVAL OVAL1202 ⁵²⁷⁷ OVAL OVAL127 ⁵²⁷⁸ OVAL OVAL1813 ⁵²⁷⁹ OVAL OVAL20 ⁵²⁸⁰ OVAL OVAL264 ⁵²⁸¹ OVAL OVAL2884 ⁵²⁸²	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB824146-x86-ENU.exe (1543456 bytes) ⁵²⁹⁴ , Uraditi download a zatim instalirati Microsoft patch DirectX9-KB819696-x86-ENU.exe (970312 bytes) ⁵²⁹⁵

⁵²⁵⁸ <http://www.securityfocus.com/bid/19409>⁵²⁵⁹ <http://www.us-cert.gov/ncas/alerts/ta06-220a>⁵²⁶⁰ <http://www.kb.cert.org/vuls/id/650769>⁵²⁶¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:492>⁵²⁶² <http://secunia.com/advisories/21388/>⁵²⁶³ <http://xforce.iss.net/xforce/xfdb/28002>⁵²⁶⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-3439>⁵²⁶⁵ <http://technet.microsoft.com/en-us/security/bulletin/ms06-040>⁵²⁶⁶ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;921883>⁵²⁶⁷ <http://www.sans.org/critical-security-controls/#w4>⁵²⁶⁸ <http://www.sans.org/critical-security-controls/#s2>⁵²⁶⁹ download.microsoft.com/download/c/2/b/c2b41862-1113-4e40-a81a-d6971733e361/WindowsXP-KB921883-x86-ENU.exe⁵²⁷⁰ <http://www.us-cert.gov/ncas/alerts/ca-2003-19>⁵²⁷¹ <http://www.us-cert.gov/ncas/alerts/ca-2003-23>⁵²⁷² <http://www.kb.cert.org/vuls/id/254236>⁵²⁷³ <http://www.kb.cert.org/vuls/id/326746>⁵²⁷⁴ <http://www.kb.cert.org/vuls/id/483492>⁵²⁷⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0995>⁵²⁷⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1118>⁵²⁷⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1202>⁵²⁷⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:127>⁵²⁷⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1813>⁵²⁸⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:20>⁵²⁸¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:264>

		napravi program sa kojim bi poslao malicioznu RPC poruku ranjivom sistemu, ciljajući na RPCSS servis.	OVAL OVAL2968 ⁵²⁸³ OVAL OVAL3966 ⁵²⁸⁴ OVAL OVAL4224 ⁵²⁸⁵ OVAL OVAL494 ⁵²⁸⁶ XF win2k-message-queue-bo(13131) ⁵²⁸⁷ BID: 8458 ⁵²⁸⁸ , CVE: CVE-2003-0528 ⁵²⁸⁹ , CVE: CVE-2003-0605 ⁵²⁹⁰ , CVE: CVE-2003-0715 ⁵²⁹¹ , MSKB: 824146 ⁵²⁹² , MS: MS03-039 ⁵²⁹³		
3.	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (windows-hotfix-ms08-067)	172.23.202.105:139 172.23.202.105:445 Ovo ažuriranje bezbednosti rešava privatno prijavljenu ranjivost. Ova ranjivost bi mogla da omogući izvršenje udaljenog kôda ukoliko bi napadnuti sistem primio posebno kreiran RPC zahtev. Na sistemima Microsoft Windows 2000, Windows XP i Windows Server 2003, napadač bi mogao da iskoristi ovu ranjivost bez autentičnosti da pokrene proizvoljan kôd. Moguće je iskoristiti ovu ranjivost da se kreira eksploatacija. Dosadašnja praksa fajervola i standardne fajervol difolt konfiguracije mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan organizacije.	BID 31874 ⁵²⁹⁶ CERT TA08-297A ⁵²⁹⁷ CERT TA09-088A ⁵²⁹⁸ CERT-VN 827267 ⁵²⁹⁹ IAVM 2008-A-0081 ⁵³⁰⁰ OVAL OVAL6093 ⁵³⁰¹ XF 46040 ⁵³⁰² MS: MS08-067 ⁵³⁰³ MSKB: 958644 ⁵³⁰⁴ CVE: CVE-2008-4250 ⁵³⁰⁵ SECUNIA: 32326 ⁵³⁰⁶ URL1 ⁵³⁰⁷ URL2 ⁵³⁰⁸ URL3 ⁵³⁰⁹ URL4 ⁵³¹⁰	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB958644-x86-ENU.exe (648560 bytes) ⁵³¹¹

⁵²⁸² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2884>⁵²⁹⁴ www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb824146-x86-enu_b957699c7365c462446bd552cd6d203.exe⁵²⁹⁵ www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/directx9-kb819696-x86-enu_977f8cc86c1e151a0168d1296210913.exe⁵²⁸³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2968>⁵²⁸⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3966>⁵²⁸⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4224>⁵²⁸⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:494>⁵²⁸⁷ <http://xforce.iss.net/xforce/xfdb/13131>⁵²⁸⁸ <http://www.securityfocus.com/bid/8458>⁵²⁸⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0528>⁵²⁹⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0605>⁵²⁹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0715>⁵²⁹² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;824146>⁵²⁹³ <http://technet.microsoft.com/en-us/security/bulletin/ms03-039>⁵²⁹⁶ <http://www.securityfocus.com/bid/31874>⁵²⁹⁷ <http://www.us-cert.gov/ncas/alerts/ta08-297a>⁵²⁹⁸ <http://www.us-cert.gov/ncas/alerts/ta09-088a>⁵²⁹⁹ <http://www.kb.cert.org/vuls/id/827267>⁵³⁰⁰ <http://iase.disa.mil/stigs/iavm-cve.html>⁵³⁰¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6093>⁵³⁰² <http://xforce.iss.net/xforce/xfdb/46040>⁵³⁰³ <http://technet.microsoft.com/en-us/security/bulletin/ms08-067>⁵³⁰⁴ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958644>⁵³⁰⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4250>⁵³⁰⁶ <http://secunia.com/advisories/32326/>⁵³⁰⁷ blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx⁵³⁰⁸ <http://blogs.msdn.com/b/sdl/archive/2008/10/22/ms08-067.aspx>⁵³⁰⁹ <http://blogs.technet.com/b/msrc/archive/2008/10/23/ms08-067-released.aspx>⁵³¹⁰ <http://technet.microsoft.com/en-us/security/bulletin/MS08-067>⁵³¹¹ http://download.windowsupdate.com/msdownload/update/software/secu/2008/10/windowsxp-kb958644-x86-enu_5c135a8dae5721849430afe27af255f83e64f62b.exe

4.	MS09-001: Vulnerabilities in SMB Could Allow Remote Code Execution (windows-hotfix-ms09-001)	172.23.202.105:139 172.23.202.105:445 Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti koje su privatno prijavljene a odnose se na protokol Microsoft Server Message Block-a (SMB). Ranjivosti mogu da omoguće daljinsko izvršenje koda na ugroženim sistemima. Napadač koji je uspešno iskoristio ove ranjivosti može da instalira programe, pregleda, menja ili briše podatke ili otvara nove naloge sa potpunim korisničkim pravima. Praksa je pokazala da zaštitni zid i njegove standardne konfiguracije po defaultu mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan okvira organizacije. Za sisteme koji su stalno povezani na Internet preporuka je da imaju što manji broj izloženih portova.	BID 31179 ⁵³¹² BID 33121 ⁵³¹³ BID 33122 ⁵³¹⁴ CERT TA09-013A ⁵³¹⁵ OVAL OVAL5248 ⁵³¹⁶ OVAL OVAL5262 ⁵³¹⁷ OVAL OVAL5863 ⁵³¹⁸ OVAL OVAL6044 ⁵³¹⁹ XF 45146 ⁵³²⁰ MS: MS09-001 ⁵³²¹ MSKB: 958687 ⁵³²² CVE: CVE-2008-4114 ⁵³²³ CVE: CVE-2008-4835 ⁵³²⁴ CVE: CVE-2008-4834 ⁵³²⁵ SECUNIA: 31883 ⁵³²⁶ URL1 ⁵³²⁷ URL2 ⁵³²⁸ URL3 ⁵³²⁹	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB958687-x86-ENU.exe (658288 bytes) ⁵³³⁰
5.	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-012)	172.23.202.105:139 172.23.202.105:445 Ovo ažuriranje bezbednosti rešava nekoliko privatno prijavljenih ranjivosti na Microsoft Windows-u. Opasnost od ove ranjivosti leži u tome što bi ona omogućila daljinsko izvršavanje koda ukoliko bi napadač kreirao posebno opremljen SMB paket i poslao ga ugroženom sistemu. Dosadašnja praksa fajervola i standardne fajervol default konfiguracije mogu da pomognu u zaštiti mrežnih resursa od napada	CERT TA10-040A ⁵³³¹ OVAL OVAL7751 ⁵³³² OVAL OVAL8314 ⁵³³³ OVAL OVAL8438 ⁵³³⁴ OVAL OVAL8524 ⁵³³⁵ MS: MS10-012 ⁵³³⁶ MSKB - 971468 ⁵³³⁷ CVE: CVE-2010-0020 ⁵³³⁸ CVE: CVE-2010-0021 ⁵³³⁹ CVE: CVE-2010-0022 ⁵³⁴⁰ CVE CVE-2010-0231 ⁵³⁴¹ SECUNIA 38510 ⁵³⁴²	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB971468-x86-ENU.exe (664952 bytes) ⁵³⁴³

⁵³¹² <http://www.securityfocus.com/bid/31179>⁵³¹³ <http://www.securityfocus.com/bid/33121>⁵³¹⁴ <http://www.securityfocus.com/bid/33122>⁵³¹⁵ <http://www.us-cert.gov/ncas/alerts/ta09-013a>⁵³¹⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5248>⁵³¹⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5262>⁵³¹⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5863>⁵³¹⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6044>⁵³²⁰ <http://xforce.iss.net/xforce/xfdb/45146>⁵³²¹ <http://technet.microsoft.com/en-us/security/bulletin/MS09-001>⁵³²² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;958687>⁵³²³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4114>⁵³²⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4835>⁵³²⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4834>⁵³²⁶ <http://secunia.com/advisories/31883/>⁵³²⁷ http://www.vallejo.cc/proyectos/vista_SMB_write_DoS.htm⁵³²⁸ <http://www.zerodayinitiative.com/advisories/ZDI-09-001/>⁵³²⁹ <http://www.zerodayinitiative.com/advisories/ZDI-09-002/>⁵³³⁰ http://download.windowsupdate.com/msdownload/update/software/secu/2008/12/windowsxp-kb958687-x86-enu_a9b85264e9b75e552ae10cd212937b8686a96833.exe⁵³³¹ <http://www.us-cert.gov/ncas/alerts/ta10-040a>⁵³³² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7751>⁵³³³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8314>⁵³³⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8438>⁵³³⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8524>⁵³³⁶ <http://technet.microsoft.com/en-us/security/bulletin/MS10-012>⁵³³⁷ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;971468>⁵³³⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0020>⁵³³⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0021>⁵³⁴⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0022>⁵³⁴¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0231>⁵³⁴² <http://secunia.com/advisories/38510/>⁵³⁴³ http://download.windowsupdate.com/msdownload/update/software/secu/2010/01/windowsxp-kb971468-x86-enu_68d7899c8b8462219daf40f02c6fb9f362b1ee6b.exe

		(koji bi pokušali da iskoriste ove ranjivosti), a koji potiču izvan okvira organizacije.			
6.	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms10-054)	172.23.202.105:139 172.23.202.105:445 Opis je isti kao kod ranjivosti MS10-012	CERT TA10-222A ⁵³⁴⁴ OVAL OVAL11106 ⁵³⁴⁵ OVAL OVAL12015 ⁵³⁴⁶ OVAL OVAL12072 ⁵³⁴⁷ CVE: CVE-2010-2550 ⁵³⁴⁸ CVE: CVE-2010-2551 ⁵³⁴⁹ CVE: CVE-2010-2552 ⁵³⁵⁰ MS: MS10-054 ⁵³⁵¹ MSKB 982214 ⁵³⁵²	Kritičan	Uraditi download a zatim instalirati Microsoft patch windowsxp-kb982214-x86-enu.exe (661368 bytes) ⁵³⁵³
7.	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (windows-hotfix-ms11-020)	172.23.202.105:139 172.23.202.105:445 Opis je isti kao kod ranjivosti MS10-012	BID 47198 ⁵³⁵⁴ CERT TA11-102A ⁵³⁵⁵ IAVM 2011-A-0050 ⁵³⁵⁶ OSVDB 71781 ⁵³⁵⁷ OVAL OVAL12076 ⁵³⁵⁸ SECUNIA 44072 ⁵³⁵⁹ CVE: CVE-2011-0661 ⁵³⁶⁰ MS: MS11-020 ⁵³⁶¹ MSKB: 2508429 ⁵³⁶²	Kritičan	Uraditi download a zatim instalirati Microsoft patch windowsxp-kb2508429-x86-enu.exe (664960 bytes) ⁵³⁶³
8.	MS03-026: Buffer Overrun In RPC Interface Could Allow Code Execution (823980) (windows-hotfix-ms03-026)	Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti u Windows Distributed Component Object Model (DCOM) Remote Procedure Call (RPC). Napadač koji uspešno iskoristi ovu ranjivost, bio bi u mogućnosti da pokrene kôd sa privilegijama lokalnog sistema na napadnutom sistemu. Napadač bi bio u mogućnosti da preduzme bilo kakvu akciju na sistemu, uključujući instaliranje programa, pregledanje, menjanje ili brisanje podataka, ili pak kreiranje	CERT CA-2003-16 ⁵³⁶⁴ CERT CA-2003-19 ⁵³⁶⁵ CERT-VN 568148 ⁵³⁶⁶ OVAL OVAL194 ⁵³⁶⁷ OVAL OVAL2343 ⁵³⁶⁸ OVAL OVAL296 ⁵³⁶⁹ XF win-rpc-dcom-bo(12629) ⁵³⁷⁰ CVE: CVE-2003-0352 ⁵³⁷¹ MS: MS03-026 ⁵³⁷² BID: 8205 ⁵³⁷³ MSKB: 823980 ⁵³⁷⁴	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB823980-x86-ENU.exe (1291040 bytes) ⁵³⁷⁵

⁵³⁴⁴ <http://www.us-cert.gov/ncas/alerts/ta10-222a>⁵³⁴⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11106>⁵³⁴⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12015>⁵³⁴⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12072>⁵³⁴⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2550>⁵³⁴⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2551>⁵³⁵⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2552>⁵³⁵¹ <http://technet.microsoft.com/en-us/security/bulletin/MS10-054>⁵³⁵² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;982214>⁵³⁵³ http://download.windowsupdate.com/msdownload/update/software/secu/2010/07/windowsxp-kb982214-x86-enu_a24853f682dad3157da4e4a39372951a8ec1e407.exe⁵³⁵⁴ <http://www.securityfocus.com/bid/47198>⁵³⁵⁵ <http://www.us-cert.gov/ncas/alerts/ta11-102a>⁵³⁵⁶ <http://iase.disa.mil/stigs/iavm-cve.html>⁵³⁵⁷ <http://www.osvdb.org/71781>⁵³⁵⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12076>⁵³⁵⁹ <http://secunia.com/advisories/44072/>⁵³⁶⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661>⁵³⁶¹ <http://technet.microsoft.com/en-us/security/bulletin/ms11-020>⁵³⁶² <http://support.microsoft.com/default.aspx?scid=kb;EN-US;2508429>⁵³⁶³ http://download.windowsupdate.com/msdownload/update/software/secu/2011/03/windowsxp-kb2508429-x86-enu_e0b40d81f2ecc1bad43439a6bd0a9e2a0ab7dd56.exe⁵³⁶⁴ <http://www.us-cert.gov/ncas/alerts/ca-2003-16>⁵³⁶⁵ <http://www.us-cert.gov/ncas/alerts/ca-2003-19>⁵³⁶⁶ <http://www.kb.cert.org/vuls/id/568148>⁵³⁶⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:194>⁵³⁶⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2343>⁵³⁶⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:296>⁵³⁷⁰ <http://xforce.iss.net/xforce/xfdb/12629>⁵³⁷¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0352>⁵³⁷² <http://technet.microsoft.com/en-us/security/bulletin/ms03-026>⁵³⁷³ <http://www.securityfocus.com/bid/8205>⁵³⁷⁴ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;823980>⁵³⁷⁵ http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb823980-x86-enu_1d296adab6699e66210e5a350236381.exe

		novih naloga sa svim privilegijama. Da bi iskoristio ovu ranjivost, napadač bi morao da pošalje posebno kreiran zahtev udaljenom kompjuteru na specifične RPC portove.			
9.	MS04-011: Security Update for Microsoft Windows (835732) (windows-hotfix-ms04-011)	172.23.202.105:139 172.23.202.105:445 Ovo ažuriranje rešava nekoliko novootkrivenih ranjivosti. Napadač koji uspešno iskoristi ovu ranjivost bi mogao da preuzme potpunu kontrolu nad napadnutim sistemom, uključujući instaliranje programa, pregledanje, menjanje ili brisanje podataka ili čak otvaranje novih naloga sa svim privilegijama.	CERT TA04-104A⁵³⁷⁶ BID 10108⁵³⁷⁷ BID 10113⁵³⁷⁸ BID 10114⁵³⁷⁹ BID 10115⁵³⁸⁰ BID 10117⁵³⁸¹ BID 10118⁵³⁸² BID 10119⁵³⁸³ BID 10120⁵³⁸⁴ BID 10122⁵³⁸⁵ BID 10124⁵³⁸⁶ BID 10125⁵³⁸⁷ BID 10126⁵³⁸⁸ CERT-VN 122076⁵³⁸⁹ CERT-VN 150236⁵³⁹⁰ CERT-VN 206468⁵³⁹¹ CERT-VN 255924⁵³⁹² CERT-VN 260588⁵³⁹³ CERT-VN 353956⁵³⁹⁴ CERT-VN 471260⁵³⁹⁵ CERT-VN 526084⁵³⁹⁶ CERT-VN 547028⁵³⁹⁷ CERT-VN 586540⁵³⁹⁸ CERT-VN 638548⁵³⁹⁹ CERT-VN 639428⁵⁴⁰⁰ CVE CVE-2003-0663⁵⁴⁰¹ CVE CVE-2003-0719⁵⁴⁰² CVE CVE-2003-0806⁵⁴⁰³ CVE CVE-2003-0906⁵⁴⁰⁴ CVE CVE-2003-0907⁵⁴⁰⁵ CVE CVE-2003-0908⁵⁴⁰⁶ CVE CVE-2003-0909⁵⁴⁰⁷	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB835732-x86-ENU.EXE (2710296 bytes) ⁵⁴⁷²

⁵³⁷⁶ <http://www.us-cert.gov/ncas/alerts/ta04-104a>⁵³⁷⁷ <http://www.securityfocus.com/bid/10108>⁵³⁷⁸ <http://www.securityfocus.com/bid/10113>⁵³⁷⁹ <http://www.securityfocus.com/bid/10114>⁵³⁸⁰ <http://www.securityfocus.com/bid/10115>⁵³⁸¹ <http://www.securityfocus.com/bid/10117>⁵³⁸² <http://www.securityfocus.com/bid/10118>⁵³⁸³ <http://www.securityfocus.com/bid/10119>⁵³⁸⁴ <http://www.securityfocus.com/bid/10120>⁵³⁸⁵ <http://www.securityfocus.com/bid/10122>⁵³⁸⁶ <http://www.securityfocus.com/bid/10124>⁵³⁸⁷ <http://www.securityfocus.com/bid/10125>⁵³⁸⁸ <http://www.securityfocus.com/bid/10126>⁵³⁸⁹ <http://www.kb.cert.org/vuls/id/122076>⁵³⁹⁰ <http://www.kb.cert.org/vuls/id/150236>⁵³⁹¹ <http://www.kb.cert.org/vuls/id/206468>⁵³⁹² <http://www.kb.cert.org/vuls/id/255924>⁵³⁹³ <http://www.kb.cert.org/vuls/id/260588>⁵³⁹⁴ <http://www.kb.cert.org/vuls/id/353956>⁵³⁹⁵ <http://www.kb.cert.org/vuls/id/471260>⁵³⁹⁶ <http://www.kb.cert.org/vuls/id/526084>⁵³⁹⁷ <http://www.kb.cert.org/vuls/id/547028>⁵³⁹⁸ <http://www.kb.cert.org/vuls/id/586540>⁵³⁹⁹ <http://www.kb.cert.org/vuls/id/638548>⁵⁴⁰⁰ <http://www.kb.cert.org/vuls/id/639428>⁵⁴⁰¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0663>⁵⁴⁰² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0719>⁵⁴⁰³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0806>⁵⁴⁰⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0906>⁵⁴⁰⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0907>⁵⁴⁰⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0908>⁵⁴⁰⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0909>

			CVE CVE-2003-0910⁵⁴⁰⁸ CVE CVE-2004-0117⁵⁴⁰⁹ CVE CVE-2004-0118⁵⁴¹⁰ CVE CVE-2004-0119⁵⁴¹¹ CVE CVE-2004-0120⁵⁴¹² CVE CVE-2004-0123⁵⁴¹³ OVAL OVAL1004⁵⁴¹⁴ OVAL OVAL1007⁵⁴¹⁵ OVAL OVAL1016⁵⁴¹⁶ OVAL OVAL1046⁵⁴¹⁷ OVAL OVAL1054⁵⁴¹⁸ OVAL OVAL1064⁵⁴¹⁹ OVAL OVAL1076⁵⁴²⁰ OVAL OVAL1093⁵⁴²¹ OVAL OVAL1512⁵⁴²² OVAL OVAL1718⁵⁴²³ OVAL OVAL1808⁵⁴²⁴ OVAL OVAL1962⁵⁴²⁵ OVAL OVAL1997⁵⁴²⁶ OVAL OVAL883⁵⁴²⁷ OVAL OVAL885⁵⁴²⁸ OVAL OVAL886⁵⁴²⁹ OVAL OVAL889⁵⁴³⁰ OVAL OVAL890⁵⁴³¹ OVAL OVAL892⁵⁴³² OVAL OVAL895⁵⁴³³ OVAL OVAL896⁵⁴³⁴ OVAL OVAL897⁵⁴³⁵ OVAL OVAL898⁵⁴³⁶ OVAL OVAL903⁵⁴³⁷ OVAL OVAL904⁵⁴³⁸ OVAL OVAL907⁵⁴³⁹ OVAL OVAL911⁵⁴⁴⁰ OVAL OVAL919⁵⁴⁴¹		

⁵⁴⁷²http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb835732-x86-enu_99fc98fc8e8cbf6720f28028a1f05eb.exe

⁵⁴⁰⁸<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0910>
⁵⁴⁰⁹<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0117>
⁵⁴¹⁰<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0118>
⁵⁴¹¹<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0119>
⁵⁴¹²<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0120>
⁵⁴¹³<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0123>
⁵⁴¹⁴<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1004>
⁵⁴¹⁵<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1007>
⁵⁴¹⁶oval.mitre.org/oval/definitions/data/OVAL1016.html
⁵⁴¹⁷oval.mitre.org/oval/definitions/data/OVAL1046.html
⁵⁴¹⁸<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1054>
⁵⁴¹⁹<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1064>
⁵⁴²⁰<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1076>
⁵⁴²¹<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1093>
⁵⁴²²<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1512>
⁵⁴²³<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1718>
⁵⁴²⁴<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1808>
⁵⁴²⁵<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1962>
⁵⁴²⁶<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1997>
⁵⁴²⁷<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:883>
⁵⁴²⁸<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:885>
⁵⁴²⁹<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:886>
⁵⁴³⁰<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:889>
⁵⁴³¹<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:890>
⁵⁴³²<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:892>
⁵⁴³³<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:895>
⁵⁴³⁴<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:896>
⁵⁴³⁵<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:897>
⁵⁴³⁶<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:898>
⁵⁴³⁷<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:903>
⁵⁴³⁸<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:904>
⁵⁴³⁹<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:907>
⁵⁴⁴⁰<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:911>
⁵⁴⁴¹<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:919>

			OVAL OVAL924 ⁵⁴⁴² OVAL OVAL946 ⁵⁴⁴³ OVAL OVAL951 ⁵⁴⁴⁴ OVAL OVAL959 ⁵⁴⁴⁵ OVAL OVAL964 ⁵⁴⁴⁶ URL1 ⁵⁴⁴⁷ URL2 ⁵⁴⁴⁸ URL3 ⁵⁴⁴⁹ URL4 ⁵⁴⁵⁰ URL5 ⁵⁴⁵¹ URL6 ⁵⁴⁵² URL7 ⁵⁴⁵³ URL8 ⁵⁴⁵⁴ XF ssl-message- dos(15712) ⁵⁴⁵⁵ XF win-asn1-double- free(15713) ⁵⁴⁵⁶ XF win-h323- bo(15710) ⁵⁴⁵⁷ XF win-hcpurl-code- execution(15704) ⁵⁴⁵⁸ XF win-ldt-gain- privileges(15707) ⁵⁴⁵⁹ XF win-lsass- bo(15699) ⁵⁴⁶⁰ XF win-spp-bo(15715) ⁵⁴⁶¹ XF win-vdm-gain- privileges(15714) ⁵⁴⁶² XF win-winlogon- bo(15702) ⁵⁴⁶³ XF win2k-lsass-ldap- dos(15700) ⁵⁴⁶⁴ XF win2k-utilitymgr- gain-privileges(15632) MS: MS04-011 ⁵⁴⁶⁵ , CVE: CVE-2003-0533 ⁵⁴⁶⁶ MSKB: 835732 ⁵⁴⁶⁷ OVAL: OVAL1000 ⁵⁴⁶⁸ CERT-VN: 753212 ⁵⁴⁶⁹		

⁵⁴⁴² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:924>

⁵⁴⁴³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:946>

⁵⁴⁴⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:951>

⁵⁴⁴⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:959>

⁵⁴⁴⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:964>

⁵⁴⁴⁷ <http://archives.neohapsis.com/archives/vulnwatch/2004-q1/0081.html>

⁵⁴⁴⁸ <http://archives.neohapsis.com/archives/vulnwatch/2004-q1/0082.html>

⁵⁴⁴⁹ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020065.html>

⁵⁴⁵⁰ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020068.html>

⁵⁴⁵¹ <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020069.html>

⁵⁴⁵² <http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020070.html>

⁵⁴⁵³ <http://www.securiteam.com/windowsntfocus/5LP0C2ACKU.html>

⁵⁴⁵⁴ <http://www.securityfocus.com/archive/1/361836>

⁵⁴⁵⁵ <http://xforce.iss.net/xforce/xfdb/15712>

⁵⁴⁵⁶ <http://xforce.iss.net/xforce/xfdb/15713>

⁵⁴⁵⁷ <http://xforce.iss.net/xforce/xfdb/15710>

⁵⁴⁵⁸ <http://xforce.iss.net/xforce/xfdb/15704>

⁵⁴⁵⁹ <http://xforce.iss.net/xforce/xfdb/15707>

⁵⁴⁶⁰ <http://xforce.iss.net/xforce/xfdb/15699>

⁵⁴⁶¹ <http://xforce.iss.net/xforce/xfdb/15715>

⁵⁴⁶² <http://xforce.iss.net/xforce/xfdb/15714>

⁵⁴⁶³ <http://xforce.iss.net/xforce/xfdb/15702>

⁵⁴⁶⁴ <http://xforce.iss.net/xforce/xfdb/15700>

⁵⁴⁶⁵ <http://technet.microsoft.com/en-us/security/bulletin/ms04-011>

⁵⁴⁶⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-0533>

⁵⁴⁶⁷ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;835732>

⁵⁴⁶⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1000>

⁵⁴⁶⁹ <http://www.kb.cert.org/vuls/id/753212>

			CERT-VN: 783748 ⁵⁴⁷⁰ XF: winxp-task-gain-privileges(15678) ⁵⁴⁷¹		
10.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.105:139 172.23.202.105:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB: 887429 ⁵⁴⁷³ URL1 ⁵⁴⁷⁴	Ozbiljan	Metoda za konfiguracije SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429 ⁵⁴⁷⁵ . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing</i> = <i>auto</i> ili da se zahteva SMB potpisivanje: <i>server signing</i> = <i>mandatory</i> .
11.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.105:139 172.23.202.105:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti.
12.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	172.23.202.105:135: Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hедера i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183 ⁵⁴⁷⁶ CERT-VN: 415294 ⁵⁴⁷⁷ CVE CVE-2004-0230 ⁵⁴⁷⁸ MS: MS05-019 ⁵⁴⁷⁹ MS: MS06-064 ⁵⁴⁸⁰ NETBSD: NetBSD-SA2004-006 ⁵⁴⁸¹ OVAL: OVAL2689 ⁵⁴⁸² OVAL: OVAL270 ⁵⁴⁸³ OVAL OVAL3508 ⁵⁴⁸⁴ OVAL OVAL4791 ⁵⁴⁸⁵ OVAL OVAL5711 ⁵⁴⁸⁶ SECUNIA: 11440 ⁵⁴⁸⁷ SECUNIA: 22341 ⁵⁴⁸⁸ SGI 20040403-01-A ⁵⁴⁸⁹	Ozbiljan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB893066-v2-x86-ENU.exe (791280 bytes) ⁵⁴⁹⁰
13.	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa	BID: 494 ⁵⁴⁹¹ CVE: CVE-1999-0519 ⁵⁴⁹² MSKB: 143474 ⁵⁴⁹³	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod

⁵⁴⁷⁰ <http://www.kb.cert.org/vuls/id/783748>⁵⁴⁷¹ <http://xforce.iss.net/xforce/xfdb/15678>⁵⁴⁷³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429>⁵⁴⁷⁴ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>⁵⁴⁷⁵ <http://support.microsoft.com/kb/887429>⁵⁴⁷⁶ <http://www.securityfocus.com/bid/10183>⁵⁴⁷⁷ <http://www.kb.cert.org/vuls/id/415294>⁵⁴⁷⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁵⁴⁷⁹ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁵⁴⁸⁰ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁵⁴⁸¹ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁵⁴⁸² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>⁵⁴⁸³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>⁵⁴⁸⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>⁵⁴⁸⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>⁵⁴⁸⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>⁵⁴⁸⁷ <http://secunia.com/advisories/11440/>⁵⁴⁸⁸ <http://secunia.com/advisories/22341/>⁵⁴⁸⁹ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>⁵⁴⁹⁰ http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb893066-v2-x86-enu_3d2029a4300c0b7943b20c1287c8143087045d52.exe⁵⁴⁹¹ <http://www.securityfocus.com/bid/494>⁵⁴⁹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>⁵⁴⁹³ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>

		Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server. Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko poziva udaljenih procedura (RPC). Ovi servisi su i u prošlosti bili skloni ranjivostima.. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinjenije napade.	URL ⁵⁴⁹⁴		primerom Null session ranjivost.
14.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	OSVDB 95 ⁵⁴⁹⁵ CVE: CVE-1999-0524 ⁵⁴⁹⁶ XF: icmp-netmask(306) ⁵⁴⁹⁷ XF: icmp-timestamp(322) ⁵⁴⁹⁸	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
15.	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (windows-hotfixms06-035)	Ovo ažuriranje rešava nekoliko novootkrivenih ranjivosti. Preporučuje se da se odmah primeni update.	BID 18863 ⁵⁴⁹⁹ BID 18891 ⁵⁵⁰⁰ CERT TA06-192A ⁵⁵⁰¹ CERT-VN 189140 ⁵⁵⁰² CERT-VN 333636 ⁵⁵⁰³ CVE CVE-2006-1314 ⁵⁵⁰⁴ CVE CVE-2006-1315 ⁵⁵⁰⁵ MS MS06-035 ⁵⁵⁰⁶ MSKB 917159 ⁵⁵⁰⁷ OSVDB 27154 ⁵⁵⁰⁸ OSVDB 27155 ⁵⁵⁰⁹ OVAL OVAL3 ⁵⁵¹⁰ OVAL OVAL600 ⁵⁵¹¹ SECUNIA 21007 ⁵⁵¹² URL ⁵⁵¹³ XF win-mailslot-bo(26818) ⁵⁵¹⁴ XF win-smb-information-	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB917159-x86-ENU.exe (725304 bytes) ⁵⁵¹⁶

⁵⁴⁹⁴ http://www.hsc.fr/ressources/presentations/null_sessions/⁵⁴⁹⁵ <http://www.osvdb.org/95>⁵⁴⁹⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁵⁴⁹⁷ <http://xforce.iss.net/xforce/xfdb/306>⁵⁴⁹⁸ <http://xforce.iss.net/xforce/xfdb/322>⁵⁴⁹⁹ <http://www.securityfocus.com/bid/18863>⁵⁵⁰⁰ <http://www.securityfocus.com/bid/18891>⁵⁵⁰¹ <http://www.us-cert.gov/ncas/alerts/ta06-192a>⁵⁵⁰² <http://www.kb.cert.org/vuls/id/189140>⁵⁵⁰³ <http://www.kb.cert.org/vuls/id/333636>⁵⁵⁰⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1314>⁵⁵⁰⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1315>⁵⁵⁰⁶ <http://technet.microsoft.com/en-us/security/bulletin/ms06-035>⁵⁵⁰⁷ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;917159>⁵⁵⁰⁸ <http://www.osvdb.org/27154>⁵⁵⁰⁹ <http://www.osvdb.org/27155>⁵⁵¹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3>⁵⁵¹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:600>⁵⁵¹² <http://secunia.com/advisories/21007/>⁵⁵¹³ <http://technet.microsoft.com/en-us/security/bulletin/MS06-035>⁵⁵¹⁴ <http://xforce.iss.net/xforce/xfdb/26818>

disclosure(26820)⁵⁵¹⁵

Tabela 119. Windows OS sa IP adresama 172.23.202.115, 172.23.202.116, 172.23.202.100, 172.23.202.99, 172.23.202.98, 172.23.202.97, 172.23.202.96, 172.23.202.95, 172.23.202.94, 172.23.202.93, 172.23.202.92, 172.23.202.91, 172.23.202.90 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.115		OS: : Microsoft Windows 7 Ultimate SP1 x86 WIN7x86ULTSP1			4
IP adresa: 172.23.202.116		OS: : windows 7 ultimate x64, WIN7x64ULT			4
IP adresa: 172.23.202.100		OS: : Windows 7 Home Basic SP1 x64, WIN7x64HoBaSp1			4
IP adresa: 172.23.202.99		OS: : Windows 7 Home Basic SP1 x86, WIN7x86HoBaSp1			4
IP adresa: 172.23.202.98		OS: : Windows 7 Home Premium SP1 x64, WIN7x64HoPreSp1			4
IP adresa: 172.23.202.97		OS: : Windows 7 Home Premium SP1 x86, WIN7x86HoPreSp1			4
IP adresa: 172.23.202.96		OS: : Windows 7 Professional SP1 x64, WIN7x64ProSp1			4
IP adresa: 172.23.202.95		OS: : Windows 7 Professional SP1 x86, WIN7x86ProSp1			4
IP adresa: 172.23.202.94		OS: : Windows 7 starter, WIN7starter			4
IP adresa: 172.23.202.93		OS: : Windows 7 Professional N x64, WIN7ProNx64			4
IP adresa: 172.23.202.92		OS: : Windows 7 Professional N x86, WIN7ProNx86			4
IP adresa: 172.23.202.91		OS: : Windows 7 Professional x64, WIN7Prox64			4
IP adresa: 172.23.202.90		OS: : Windows 7 Professional x86, WIN7Prox86			4
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.115:139 172.23.202.115:445 172.23.202.116:139 172.23.202.116:445 172.23.202.100:139 172.23.202.100:445 172.23.202.99:139 172.23.202.99:445 172.23.202.98:139 172.23.202.98:445 172.23.202.97:139 172.23.202.97:445 172.23.202.96:139 172.23.202.96:445 172.23.202.95:139 172.23.202.95:445 172.23.202.94:139 172.23.202.94:445 172.23.202.93:139 172.23.202.93:445 172.23.202.92:139	MSKB 887429 URL1 ⁵⁵¹⁷	Ozbiljan	Metoda za konfiguracije SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429 ⁵⁵¹⁸ . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing</i> = <i>auto</i> ili da se zahteva SMB potpisivanje: <i>server signing</i> = <i>mandatory</i> .

⁵⁵¹⁶ www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/windowsxp-kb917159-x86-enu_5ed838e18ceae61a8d94f8c4be2462a8e19212d7.exe

⁵⁵¹⁵ <http://xforce.iss.net/xforce/xfdb/26820>

⁵⁵¹⁷ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>

⁵⁵¹⁸ <http://support.microsoft.com/kb/887429>

		172.23.202.92:445 172.23.202.91:139 172.23.202.91:445 172.23.202.90:139 172.23.202.90:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).			
2.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.115:139 172.23.202.115:445 172.23.202.116:139 172.23.202.116:445 172.23.202.100:139 172.23.202.100:445 172.23.202.99:139 172.23.202.99:445 172.23.202.98:139 172.23.202.98:445 172.23.202.97:139 172.23.202.97:445 172.23.202.96:139 172.23.202.96:445 172.23.202.95:139 172.23.202.95:445 172.23.202.94:139 172.23.202.94:445 172.23.202.93:139 172.23.202.93:445 172.23.202.92:139 172.23.202.92:445 172.23.202.91:139 172.23.202.91:445 172.23.202.90:139 172.23.202.90:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti.
3.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	OSVDB 95 ⁵⁵¹⁹ CVE: CVE-1999-0524 ⁵⁵²⁰ XF: icmp-netmask(306) ⁵⁵²¹ XF: icmp-timestamp(322) ⁵⁵²²	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.

⁵⁵¹⁹ <http://www.osvdb.org/95>⁵⁵²⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁵⁵²¹ <http://xforce.iss.net/xforce/xfdb/306>⁵⁵²² <http://xforce.iss.net/xforce/xfdb/322>

4.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1⁵⁵²³ URL2⁵⁵²⁴ URL3⁵⁵²⁵	Umeren	Onemogućavanje TCP timestamp odgovora na Windows OS. Podesiti Tcp1323Opts vrednost na sledećem ključu na 1: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters. Od Windows Viste onemogućavanje TCP timestamp nije moguće pa se to radi uz pomoć fajerevola.

Tabela 120. Windows OS sa IP adresom 172.23.202.118 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.118		OS: Microsoft Windows server 2008 Enterprise R2 SP1 x64 Updated Jun 2011, 2008entR2X64SP1			4
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.118:139 172.23.202.118:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB 887429 URL1⁵⁵²⁶	Ozbiljan	Metoda za konfiguraciju SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429 ⁵⁵²⁷ . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing</i> = <i>auto</i> ili da se zahteva SMB potpisivanje: <i>server signing</i> = <i>mandatory</i> .
2.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.118:139 172.23.202.118:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti.
3.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatišu slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov	OSVDB 95 ⁵⁵²⁸ CVE: CVE-1999-0524 ⁵⁵²⁹ XF: icmp-netmask(306) ⁵⁵³⁰ XF: icmp-timestamp(322) ⁵⁵³¹	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajerevola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.

⁵⁵²³ http://www.forensicswiki.org/wiki/TCP_timestamps⁵⁵²⁴ <http://www.ietf.org/rfc/rfc1323.txt>⁵⁵²⁵ <http://uptime.netcraft.com/>⁵⁵²⁶ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>⁵⁵²⁷ <http://support.microsoft.com/kb/887429>⁵⁵²⁸ <http://www.osvdb.org/95>⁵⁵²⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁵⁵³⁰ <http://xforce.iss.net/xforce/xfdb/306>⁵⁵³¹ <http://xforce.iss.net/xforce/xfdb/322>

		zahtev za vremenski pečat.			
4.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1 ⁵⁵³² URL2 ⁵⁵³³ URL3 ⁵⁵³⁴	Umeren	Onemogućavanje TCP timestamp odgovora na Windows OS. Podesiti Tcp1323Opts vrednost na sledećem ključu na 1: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters Od Windows Viste onemogućavanja TCP timestamp nije moguće pa se to radi uz pomoć fajerevola.

Tabela 121. Windows OS sa IP adresom 172.23.202.103 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.103		OS: Windows 98 se, WIN98SE			3
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	172.23.202.103:135: Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183 ⁵⁵³⁵ CERT TA04-111A ⁵⁵³⁶ CERT-VN: 415294 ⁵⁵³⁷ CVE CVE-2004-0230 ⁵⁵³⁸ MS: MS05-019 ⁵⁵³⁹ MS: MS06-064 ⁵⁵⁴⁰ NETBSD: NetBSD-SA2004-006 ⁵⁵⁴¹ OVAL: OVAL2689 ⁵⁵⁴² OVAL: OVAL270 ⁵⁵⁴³ OVAL OVAL3508 ⁵⁵⁴⁴ OVAL OVAL4791 ⁵⁵⁴⁵ OVAL OVAL5711 ⁵⁵⁴⁶ SECUNIA: 11440 ⁵⁵⁴⁷ SECUNIA: 22341 ⁵⁵⁴⁸ SECUNIA 11458 ⁵⁵⁴⁹ SGI 20040403-01-A ⁵⁵⁵⁰ XF tcp-rst-dos(15886) ⁵⁵⁵¹ URL1 ⁵⁵⁵² URL2 ⁵⁵⁵³	Ozbiljan	Nema adekvatne zakrpe osim osim blokiranja porta 135. Resenje je da se ažurira sistem novijom verzijom.

⁵⁵³² http://www.forensicswiki.org/wiki/TCP_timestamps⁵⁵³³ <http://www.ietf.org/rfc/rfc1323.txt>⁵⁵³⁴ <http://uptime.netcraft.com/>⁵⁵³⁵ <http://www.securityfocus.com/bid/10183>⁵⁵³⁶ <http://www.us-cert.gov/ncas/alerts/ta04-111a>⁵⁵³⁷ <http://www.kb.cert.org/vuls/id/415294>⁵⁵³⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁵⁵³⁹ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁵⁵⁴⁰ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁵⁵⁴¹ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁵⁵⁴² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>⁵⁵⁴³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>⁵⁵⁴⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>⁵⁵⁴⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>⁵⁵⁴⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>⁵⁵⁴⁷ <http://secunia.com/advisories/11440/>⁵⁵⁴⁸ <http://secunia.com/advisories/22341/>⁵⁵⁴⁹ <http://secunia.com/advisories/11458/>⁵⁵⁵⁰ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>⁵⁵⁵¹ <http://xforce.iss.net/xforce/xfdb/15886>⁵⁵⁵² <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁵⁵⁵³ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>

2.	ICMP netmask response (generic-icmp-netmask)	Received ICMP netmask response [255.255.255.0] from 172.23.202.103 Udaljeni host je odgovorio na ICMP-ov netmask zahtev. ICMP netmask odgovor sadrži mrežnu masku (network mask) udaljenog host-a (na mestu na kojem je obrađen zahtev). Ovu informaciju zlonamerni napadač može da iskoristi sa ciljem preciznijeg mapiranja strukture interne mreže. Takođe je moguće otkriti mrežne adrese koje se koriste, kao i informacije o ruterima koji su zaduženi za interne mreže. Zlonamernim napadačima je ovom ranjivošću olakšana realizacija napada "SMURF attack" (SMURF napad), koristeći usmerene broadcast ICMP ping pakete.	CVE CVE-1999-0524 OSVDB 95 XF icmp-netmask(306) XF icmp-timestamp(322)	Umeren	Konfigurisati fajervol tako da blokira ulazne i izlazne ICMP pakete sa ICMP tipovima 17 (netmask zahtev) i 18 (netmask odgovor).
3.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatišu slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	OSVDB 95 ⁵⁵⁵⁴ CVE: CVE-1999-0524 ⁵⁵⁵⁵ XF: icmp-netmask(306) ⁵⁵⁵⁶ XF: icmp-timestamp(322) ⁵⁵⁵⁷	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivosti.

Tabela 122. Windows OS sa IP adresom 172.23.202.104 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.104		OS: Windows ME, WINME			2
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	172.23.202.104:135: Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr.	BID: 10183 ⁵⁵⁵⁸ CERT TA04-111A ⁵⁵⁵⁹ CERT-VN: 415294 ⁵⁵⁶⁰ CVE CVE-2004-0230 ⁵⁵⁶¹ MS: MS05-019 ⁵⁵⁶² MS: MS06-064 ⁵⁵⁶³ NETBSD: NetBSD-SA2004-006 ⁵⁵⁶⁴ OVAL: OVAL2689 ⁵⁵⁶⁵	Ozbiljan	Nema adekvatne zakrpe osim osim blokiranja porta 135. Resenje je da se ažurira sistem novijom verzijom.

⁵⁵⁵⁴ <http://www.osvdb.org/95>⁵⁵⁵⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁵⁵⁵⁶ <http://xforce.iss.net/xforce/xfdb/306>⁵⁵⁵⁷ <http://xforce.iss.net/xforce/xfdb/322>⁵⁵⁵⁸ <http://www.securityfocus.com/bid/10183>⁵⁵⁵⁹ <http://www.us-cert.gov/ncas/alerts/ta04-111a>⁵⁵⁶⁰ <http://www.kb.cert.org/vuls/id/415294>⁵⁵⁶¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁵⁵⁶² <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁵⁵⁶³ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁵⁵⁶⁴ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁵⁵⁶⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>

		BGP.	OVAL: OVAL270 ⁵⁵⁶⁶ OVAL OVAL3508 ⁵⁵⁶⁷ OVAL OVAL4791 ⁵⁵⁶⁸ OVAL OVAL5711 ⁵⁵⁶⁹ SECUNIA: 11440 ⁵⁵⁷⁰ SECUNIA: 22341 ⁵⁵⁷¹ SECUNIA 11458 ⁵⁵⁷² SGI 20040403-01-A ⁵⁵⁷³ XF tcp-rst-dos(15886) ⁵⁵⁷⁴ URL1 ⁵⁵⁷⁵ URL2 ⁵⁵⁷⁶		
2.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	OSVDB 95⁵⁵⁷⁷ CVE: CVE-1999-0524⁵⁵⁷⁸ XF: icmp-netmask(306)⁵⁵⁷⁹ XF: icmp-timestamp(322)⁵⁵⁸⁰	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.

Tabela 123. Windows OS sa IP adresom 172.23.202.102 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.102		OS: Microsoft Windows 95 OSR 2.5, WIN95osr25			3
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	172.23.202.178:102: Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hедера i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr.	BID: 10183⁵⁵⁸¹ CERT TA04-111A⁵⁵⁸² CERT-VN: 415294⁵⁵⁸³ CVE CVE-2004-0230⁵⁵⁸⁴ MS: MS05-019⁵⁵⁸⁵ MS: MS06-064⁵⁵⁸⁶ NETBSD: NetBSD-SA2004-006⁵⁵⁸⁷ OVAL: OVAL2689⁵⁵⁸⁸	Ozbiljan	Nema adekvatne zakrpe osim osim blokiranja porta 135. Resenje je da se ažurira sistem novijom verzijom.

⁵⁵⁶⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>
⁵⁵⁶⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>
⁵⁵⁶⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>
⁵⁵⁶⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>
⁵⁵⁷⁰ <http://secunia.com/advisories/11440/>
⁵⁵⁷¹ <http://secunia.com/advisories/22341/>
⁵⁵⁷² <http://secunia.com/advisories/11458/>
⁵⁵⁷³ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>
⁵⁵⁷⁴ <http://xforce.iss.net/xforce/xfdb/15886>
⁵⁵⁷⁵ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>
⁵⁵⁷⁶ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>
⁵⁵⁷⁷ <http://www.osvdb.org/95>
⁵⁵⁷⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>
⁵⁵⁷⁹ <http://xforce.iss.net/xforce/xfdb/306>
⁵⁵⁸⁰ <http://xforce.iss.net/xforce/xfdb/322>
⁵⁵⁸¹ <http://www.securityfocus.com/bid/10183>
⁵⁵⁸² <http://www.us-cert.gov/ncas/alerts/ta04-111a>
⁵⁵⁸³ <http://www.kb.cert.org/vuls/id/415294>
⁵⁵⁸⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>
⁵⁵⁸⁵ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>
⁵⁵⁸⁶ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>
⁵⁵⁸⁷ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>
⁵⁵⁸⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>

		BGP.	OVAL: OVAL270⁵⁵⁸⁹ OVAL OVAL3508⁵⁵⁹⁰ OVAL OVAL4791⁵⁵⁹¹ OVAL OVAL5711⁵⁵⁹² SECUNIA: 11440⁵⁵⁹³ SECUNIA: 22341⁵⁵⁹⁴ SECUNIA 11458⁵⁵⁹⁵ SGI 20040403-01-A⁵⁵⁹⁶ XF tcp-rst-dos(15886)⁵⁵⁹⁷ URL1⁵⁵⁹⁸ URL2⁵⁵⁹⁹		
2.	ICMP netmask response (generic-icmp-netmask)	Received ICMP netmask response [255.255.255.0] from 172.23.202.102 Udaljeni host je odgovorio na ICMP-ov netmask zahtev. ICMP netmask odgovor sadrži mrežnu masku (network mask) udaljenog host-a (na mestu na kojem je obrađen zahtev). Ovu informaciju zlonamerni napadač može da iskoristi sa ciljem preciznijeg mapiranja strukture interne mreže. Takođe je moguće otkriti mrežne adrese koje se koriste, kao i informacije o ruterima koji su zaduženi za interne mreže. Zlonamernim napadačima je ovom ranjivošću olakšana realizacija napada "SMURF attack" (SMURF napad), koristeći usmerene broadcast ICMP ping pakete.	CVE CVE-1999-0524 OSVDB 95 XF icmp-netmask(306) XF icmp-timestamp(322)	Umeren	Konfigurisati fajervol tako da blokira ulazne i izlazne ICMP pakete sa ICMP tipovima 17 (netmask zahtev) i 18 (netmask odgovor).

4.3.4 LINUX OPERATIVNI SISTEMI - SKENIRANJE SERVISA NA RANJIVOSTI U 2013

Tabela 124. Linux OS sa IP adresama 172.23.202.124, 172.23.202.220 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.124		OS: Mandriva Linux Enterprise Server 5.2 x86, mandriva52enx86			58
IP adresa: 172.23.202.220		OS: Mandriva Linux Enterprise Server 5.2 x64, mandriva52enx64			58
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti

⁵⁵⁸⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>

⁵⁵⁹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>

⁵⁵⁹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>

⁵⁵⁹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>

⁵⁵⁹³ <http://secunia.com/advisories/11440/>

⁵⁵⁹⁴ <http://secunia.com/advisories/22341/>

⁵⁵⁹⁵ <http://secunia.com/advisories/11458/>

⁵⁵⁹⁶ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>

⁵⁵⁹⁷ <http://xforce.iss.net/xforce/xfdb/15886>

⁵⁵⁹⁸ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>

⁵⁵⁹⁹ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>

1.	Apache httpd mod_isapi module unload flaw (CVE-2010-0425) (apache-httpd-2_2_x-mod_isapi-moduleunload-flaw-cve-2010-0425)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 U modulu mod_isapi je pronađen propust koji će pokušati da ukloni ISAPI dll kada naiđe na greške. To može ostaviti povratne pozive u nedefinisanoj stanju greške i kao posledica može da se javi segmentation fault. Na Windows platformama koje koriste mod_isapi, udaljeni napadač bi mogao da pošalje zlonameran zahtev da pokrene ovaj problem, a kako win32 MPM pokreće samo jedan proces, to bi kao ishod imalo odbijanje servisa i potencijalno dozvolilo da se pokrene proizvoljan kôd. Napomena: Zahvaljujući Brett Gervasoni-ju iz "Sense of Security" ovaj problem je prijavljen i za njega je predložena zakrpa.	BID 38494 ⁵⁶⁰⁰ CERT-VN 280613 ⁵⁶⁰¹ CVE CVE-2010-0425 ⁵⁶⁰² OVAL OVAL8439 ⁵⁶⁰³ SECUNIA 38978 ⁵⁶⁰⁴ SECUNIA 39628 ⁵⁶⁰⁵ URL1 ⁵⁶⁰⁶ XF apache-http-modisapi-ocp-unspecified(56624) ⁵⁶⁰⁷	Kritičan	Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz
2.	Apache httpd APR apr_palloc heap overflow (CVE-2009-2412) (http-apache-apr_palloc-heap-overflow)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 U modulu apr_palloc() je pronađen propust u sklopu APR-a, koji može prouzrokovati velika preopterećenja u programima koji pokušaju da kontrolišu apr_palloc() veličinu zadatu od strane korisnika. Sam Apache HTTP server ne dopušta prolaz ka ovoj funkciji neproverenim veličinama koje zadaje korisnik, tako da se on može pokrenuti samo preko neke druge aplikacije koja koristi apr_palloc() na ranjiv način.	APPLE APPLE-SA-2009-11-09 ⁵⁶⁰⁸ BID 35949 ⁵⁶⁰⁹ CVE CVE-2009-2412 ⁵⁶¹⁰ OSVDB 56765 ⁵⁶¹¹ OSVDB 56766 ⁵⁶¹² OVAL OVAL8394 ⁵⁶¹³ OVAL OVAL9958 ⁵⁶¹⁴ SECUNIA 36138 ⁵⁶¹⁵ SECUNIA 36140 ⁵⁶¹⁶ SECUNIA 36166 ⁵⁶¹⁷ SECUNIA 36233 ⁵⁶¹⁸ SECUNIA 37152 ⁵⁶¹⁹ SECUNIA 37221 ⁵⁶²⁰ SUSE SUSE-SA:2009:050 ⁵⁶²¹ URL1 ⁵⁶²²	Kritičan	Mnoge platforme i mnogi distributeri daju unapred formirane binarne pakete za Apache. Ovi unapred formirani paketi su najčešće standardizovani i optimizirani za određenu distribuciju, pa se zato savetuje korišćenje paketa predefinisanih za određeni OS, ukoliko su dostupni. Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.13.tar.gz
3.	Apache HTTPD: mod_proxy_ftp FTP command injection	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80	APPLE APPLE-SA-2010-03-29 ⁵⁶²³ CVE CVE-2009-3095 ⁵⁶²⁴	Kritičan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati:

⁵⁶⁰⁰ <http://www.securityfocus.com/bid/38494>⁵⁶⁰¹ <http://www.kb.cert.org/vuls/id/280613>⁵⁶⁰² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0425>⁵⁶⁰³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8439>⁵⁶⁰⁴ <http://secunia.com/advisories/38978/>⁵⁶⁰⁵ <http://secunia.com/advisories/39628/>⁵⁶⁰⁶ http://httpd.apache.org/security/vulnerabilities_22.html⁵⁶⁰⁷ <http://xforce.iss.net/xforce/xfdb/56624>⁵⁶⁰⁸ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>⁵⁶⁰⁹ <http://www.securityfocus.com/bid/35949>⁵⁶¹⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2412>⁵⁶¹¹ <http://osvdb.org/56765>⁵⁶¹² <http://osvdb.org/56766>⁵⁶¹³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8394>⁵⁶¹⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9958>⁵⁶¹⁵ <http://secunia.com/advisories/36138/>⁵⁶¹⁶ <http://secunia.com/advisories/36140/>⁵⁶¹⁷ <http://secunia.com/advisories/36166/>⁵⁶¹⁸ <http://secunia.com/advisories/36233/>⁵⁶¹⁹ <http://secunia.com/advisories/37152/>⁵⁶²⁰ <http://secunia.com/advisories/37221/>⁵⁶²¹ <https://www.suse.com/support/security/advisories/>⁵⁶²² http://httpd.apache.org/security/vulnerabilities_22.html⁵⁶²³ <http://lists.apple.com/archives/security-announce/2010/Mar/msg00001.html>⁵⁶²⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3095>

	(CVE-2009-3095) (apache-httpd-cve-2009-3095)	172.23.202.220:443 U modulu mod_proxy_ftp je pronađen propust. U reverznoj proxy konfiguraciji, udaljeni napadač bi mogao da iskoristi ovaj defekt da zaobiđe uobičajenu zabranu pristupa tako što bi kreirao pažljivo izrađen HTTP Authorization heder, koji omogućava napadaču da šalje proizvoljne komande FTP serveru.	DEBIAN DSA-1934 ⁵⁶²⁵ OVAL OVAL8662 ⁵⁶²⁶ OVAL OVAL9363 ⁵⁶²⁷ SECUNIA 37152 ⁵⁶²⁸ SUSE SA:2009:050 ⁵⁶²⁹ URL1 ⁵⁶³⁰ URL2 ⁵⁶³¹		http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.gz Apache HTTPD >= 2.0 and < 2.0.64 Upgrade to Apache HTTPD version 2.0.64 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
4.	Apache HTTPD: APR-util XML DoS (CVE-2009-1955) (apache-httpd-cve-2009-1955)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Ranjivost na DOS napad otkrivena je u sklopu kopije kompleta APR-util library Extensible Markup Language (XML) prevodioca (eng. parser). Udaljeni napadač bi mogao da kreira posebno izrađen XML dokument koji bi prouzrokovao ogromno zauzeće memorije kada ga procesira XML decoding engine.	APPLE APPLE-SA-2009-11-09 ⁵⁶³² BID 35253 ⁵⁶³³ CVE CVE-2009-1955 ⁵⁶³⁴ DEBIAN DSA-1812 ⁵⁶³⁵ OVAL OVAL10270 ⁵⁶³⁶ REDHAT RHSA-2009:1107 ⁵⁶³⁷ REDHAT RHSA-2009:1108 ⁵⁶³⁸ SECUNIA 34724 ⁵⁶³⁹ SECUNIA 35284 ⁵⁶⁴⁰ SECUNIA 35360 ⁵⁶⁴¹ SECUNIA 35395 ⁵⁶⁴² SECUNIA 35444 ⁵⁶⁴³ SECUNIA 35487 ⁵⁶⁴⁴ SECUNIA 35565 ⁵⁶⁴⁵ SECUNIA 35710 ⁵⁶⁴⁶ SECUNIA 35797 ⁵⁶⁴⁷ SECUNIA 35843 ⁵⁶⁴⁸ SECUNIA 36473 ⁵⁶⁴⁹ SECUNIA 37221 ⁵⁶⁵⁰ URL1 ⁵⁶⁵¹	Kritičan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz
5.	Apache HTTPD: Range header remote DoS (CVE-2011-3192) (apache-httpd-cve-2011-3192)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Propust je otkriven u načinu na koji	APPLE APPLE-SA-2011-10-12-3 ⁵⁶⁵² BID 49303 ⁵⁶⁵³ CERT-VN 405811 ⁵⁶⁵⁴ CVE CVE-2011-3192 ⁵⁶⁵⁵ IAVM 2012-B-0056 ⁵⁶⁵⁶	Kritičan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati:

⁵⁶²⁵ <http://www.debian.org/security/DSA-/DSA-1934>
⁵⁶²⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8662>
⁵⁶²⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9363>
⁵⁶²⁸ <http://secunia.com/advisories/37152/>
⁵⁶²⁹ <https://www.suse.com/support/security/advisories/>
⁵⁶³⁰ http://httpd.apache.org/security/vulnerabilities_22.html
⁵⁶³¹ http://httpd.apache.org/security/vulnerabilities_20.html
⁵⁶³² <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>
⁵⁶³³ <http://www.securityfocus.com/bid/35253>
⁵⁶³⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1955>
⁵⁶³⁵ <http://lists.debian.org/debian-security-announce/2009/msg00124.html>
⁵⁶³⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10270>
⁵⁶³⁷ <http://rhn.redhat.com/errata/RHSA-2009-1107.html>
⁵⁶³⁸ <http://rhn.redhat.com/errata/RHSA-2009-1108.html>
⁵⁶³⁹ <http://secunia.com/advisories/34724/>
⁵⁶⁴⁰ <http://secunia.com/advisories/35284/>
⁵⁶⁴¹ <http://secunia.com/advisories/35360/>
⁵⁶⁴² <http://secunia.com/advisories/35395/>
⁵⁶⁴³ <http://secunia.com/advisories/35444/>
⁵⁶⁴⁴ <http://secunia.com/advisories/35487/>
⁵⁶⁴⁵ <http://secunia.com/advisories/35565/>
⁵⁶⁴⁶ <http://secunia.com/advisories/35710/>
⁵⁶⁴⁷ <http://secunia.com/advisories/35797/>
⁵⁶⁴⁸ <http://secunia.com/advisories/35843/>
⁵⁶⁴⁹ <http://secunia.com/advisories/36473/>
⁵⁶⁵⁰ <http://secunia.com/advisories/37221/>
⁵⁶⁵¹ http://httpd.apache.org/security/vulnerabilities_22.html
⁵⁶⁵² <http://lists.apple.com/archives/Security-announce/2011/Oct/msg00003.html>
⁵⁶⁵³ <http://www.securityfocus.com/bid/49303>
⁵⁶⁵⁴ <http://www.kb.cert.org/vuls/id/405811>
⁵⁶⁵⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3192>

		Apache HTTP Server obrađuje Range HTTP hedere. Zlonamerni napadač bi mogao da iskoristi ovaj propust i dovede do toga da http koristi veliku količinu memorije i CPU vremena preko HTTP zahteva sa posebno kreiranim Range hederom. Ovo bi moglo dovesti do napada odbijanja servisa. Advisory: CVE-2011-3192.txt	OSVDB 74721⁵⁶⁵⁷ OVAL OVAL14762⁵⁶⁵⁸ OVAL OVAL14824⁵⁶⁵⁹ OVAL OVAL18827⁵⁶⁶⁰ REDHAT RHSA-2011:1245⁵⁶⁶¹ REDHAT RHSA-2011:1294⁵⁶⁶² REDHAT RHSA-2011:1300⁵⁶⁶³ REDHAT RHSA-2011:1329⁵⁶⁶⁴ REDHAT RHSA-2011:1330⁵⁶⁶⁵ REDHAT RHSA-2011:1369⁵⁶⁶⁶ SECUNIA 45606⁵⁶⁶⁷ SECUNIA 45937⁵⁶⁶⁸ SECUNIA 46000⁵⁶⁶⁹ SECUNIA 46125⁵⁶⁷⁰ SECUNIA 46126⁵⁶⁷¹ XF 69396⁵⁶⁷² URL1⁵⁶⁷³ URL2⁵⁶⁷⁴		http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.20 Azurirati na Apache HTTPD version 2.2.20 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.20.tar.gz
6.	HTTP Basic Authentication Enabled (http-basic-auth-cleartext)	172.23.202.124:8080 172.23.202.220:8080 HTTP Basic Authentication šema se ne smatra sigurnom metodom autentifikacije korisnika (ukoliko se ne koristi u kombinaciji sa nekim spoljnim sigurnosnim sistemom, kao TLS/SSL), s obzirom da se korisničko ime i lozinka preko mreže prenose kao običan tekst. Primer: Pokretanje ranjivog HTTP servisa. http://localhost:8080/manager/jmxproxy/WS_FTP.LOG 1: Basic realm="Tomcat Manager Application"	URL1⁵⁶⁷⁵	Kritičan	Koristiti Osnovnu Autentifikaciju preko TLS/SSL (HTTPS). Omogućiti HTTPS na Web serveru. TLS/SSL protokol će zaštititi akreditivne osnovne autentifikacije u običnom tekstu. Koristiti Digest Authentication Replace Basic Authentication sa alternativnom Digest Authentication shemom. Po savremenim kriptografskim standardima, Digest Authentication je slaba. Ali za širok spektar namena, ona je korisna zamena za Basic Authentication (osnovnu autentifikaciju). Ona ispravlja neke, ali ne sve, slabosti Basic Authentication (osnovne

⁵⁶⁵⁶ <http://iase.disa.mil/stigs/iavm-cve.html>

⁵⁶⁵⁷ <http://www.osvdb.org/74721>

⁵⁶⁵⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14762>

⁵⁶⁵⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14824>

⁵⁶⁶⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18827>

⁵⁶⁶¹ <http://rhn.redhat.com/errata/RHSA-2011-1245.html>

⁵⁶⁶² <http://rhn.redhat.com/errata/RHSA-2011-1294.html>

⁵⁶⁶³ <http://rhn.redhat.com/errata/RHSA-2011-1300.html>

⁵⁶⁶⁴ <http://rhn.redhat.com/errata/RHSA-2011-1329.html>

⁵⁶⁶⁵ <http://rhn.redhat.com/errata/RHSA-2011-1330.html>

⁵⁶⁶⁶ <http://rhn.redhat.com/errata/RHSA-2011-1369.html>

⁵⁶⁶⁷ <http://secunia.com/advisories/45606/>

⁵⁶⁶⁸ <http://secunia.com/advisories/45937/>

⁵⁶⁶⁹ <http://secunia.com/advisories/46000/>

⁵⁶⁷⁰ <http://secunia.com/advisories/46125/>

⁵⁶⁷¹ <http://secunia.com/advisories/46126/>

⁵⁶⁷² <http://xforce.iss.net/xforce/xfdb/69396>

⁵⁶⁷³ http://httpd.apache.org/security/vulnerabilities_22.html

⁵⁶⁷⁴ http://httpd.apache.org/security/vulnerabilities_20.html

⁵⁶⁷⁵ <http://tools.ietf.org/html/rfc2617>

					autentifikacije). Videti RFC 2617 ⁵⁶⁷⁶ (odjeljak 4 Security Considerations) za više informacija.
7.	Apache httpd mod_deflate DoS (CVE-2009-1891) (httpd-apache-mod_deflate-dos)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Ranjivost na DOS napad otkrivena je u modulu mod_deflate. Ovaj modul nastavlja da kompresuje velike fajlove sve dok se kompresija ne završi, čak i kada je mrežna konekcija koja je zahtevala taj sadržaj prekinuta pre nego što je kompresija završena. To dovodi do toga da mod_deflate zauzima veliku količinu CPU-a ukoliko je mod_deflate bio omogućen za velike fajlove.	APPLE APPLE-SA-2009-11-09 ⁵⁶⁷⁷ CVE CVE-2009-1891 ⁵⁶⁷⁸ DEBIAN DSA-1834 ⁵⁶⁷⁹ OSVDB 55782 ⁵⁶⁸⁰ OVAL OVAL8632 ⁵⁶⁸¹ OVAL OVAL9248 ⁵⁶⁸² OVAL OVAL12361 ⁵⁶⁸³ REDHAT RHSA-2009-1148 ⁵⁶⁸⁴ REDHAT RHSA-2009-1156 ⁵⁶⁸⁵ SECUNIA 35721 ⁵⁶⁸⁶ SECUNIA 35781 ⁵⁶⁸⁷ SECUNIA 35793 ⁵⁶⁸⁸ SECUNIA 35865 ⁵⁶⁸⁹ SECUNIA 37152 ⁵⁶⁹⁰ SECUNIA 37221 ⁵⁶⁹¹ SUSE SA:2009:050 ⁵⁶⁹² URL1 ⁵⁶⁹³ URL2 ⁵⁶⁹⁴	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.12 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz Apache HTTPD >= 2.0 and < 2.0.64 Upgrade to Apache HTTPD version 2.0.64 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
8.	Apache HTTPD: insecure LD_LIBRARY_PATH handling (CVE-2012-0883) (apache-httpd-cve-2012-0883)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Otkrivena je nebezbedna obrada rute LD_LIBRARY_PATH koja bi mogla da dovede do toga da direktorijum koji trenutno radi traži DSO-ove. Ovo bi lokalnom korisniku omogućilo da izvrši kôd kao root ako je administrator pokrenuo apachectl sa nepoverljivog direktorijuma.	APPLE APPLE-SA-2013-09-12-1 ⁵⁶⁹⁵ CVE CVE-2012-0883 ⁵⁶⁹⁶ SECUNIA 48849 ⁵⁶⁹⁷ URL1 ⁵⁶⁹⁸ URL2 ⁵⁶⁹⁹	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.23 Ažurirati na Apache HTTPD version 2.2.23 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz Apache HTTPD >= 2.4 and < 2.4.2 Ažurirati na Apache HTTPD version 2.4.2 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.2.tar.gz
9.	Apache HTTPD: mod_proxy reverse	172.23.202.124:80 172.23.202.124:443	APPLE APPLE-SA-2009-11-09 ⁵⁷⁰⁰	Ozbiljan	Apache >= 2.2 and < 2.3 Uradi download a zatim

⁵⁶⁷⁶ <http://tools.ietf.org/html/rfc2617#section-4>⁵⁶⁷⁷ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>⁵⁶⁷⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1891>⁵⁶⁷⁹ <http://www.debian.org/security/2009/dsa-1834>⁵⁶⁸⁰ <http://osvdb.org/55782>⁵⁶⁸¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8632>⁵⁶⁸² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9248>⁵⁶⁸³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12361>⁵⁶⁸⁴ <http://rhn.redhat.com/errata/RHSA-2009-1148.html>⁵⁶⁸⁵ <http://rhn.redhat.com/errata/RHSA-2009-1156.html>⁵⁶⁸⁶ <http://secunia.com/advisories/35721/>⁵⁶⁸⁷ <http://secunia.com/advisories/35781/>⁵⁶⁸⁸ <http://secunia.com/advisories/35793/>⁵⁶⁸⁹ <http://secunia.com/advisories/35865/>⁵⁶⁹⁰ <http://secunia.com/advisories/37152/>⁵⁶⁹¹ <http://secunia.com/advisories/37221/>⁵⁶⁹² <https://www.suse.com/support/security/advisories/>⁵⁶⁹³ http://httpd.apache.org/security/vulnerabilities_22.html⁵⁶⁹⁴ http://httpd.apache.org/security/vulnerabilities_20.html⁵⁶⁹⁵ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁵⁶⁹⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0883>⁵⁶⁹⁷ <http://secunia.com/advisories/48849/>⁵⁶⁹⁸ http://httpd.apache.org/security/vulnerabilities_22.html⁵⁶⁹⁹ http://httpd.apache.org/security/vulnerabilities_24.html⁵⁷⁰⁰ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>

	proxy DoS (CVE-2009-1890) (apache-httpd-cve-2009-1890)	172.23.202.220:80 172.23.202.220:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja prisustva mod_proxy modula. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy. Zlonamerni napadač bi mogao da iskoristi ovaj propust na takav način da primora proxy proces da zauzme veliku količinu CPU vremena.	CVE CVE-2009-1890 ⁵⁷⁰¹ DEBIAN DSA-1834 ⁵⁷⁰² OSVDB 55553 ⁵⁷⁰³ OVAL OVAL12330 ⁵⁷⁰⁴ OVAL OVAL8616 ⁵⁷⁰⁵ OVAL OVAL9403 ⁵⁷⁰⁶ REDHAT RHSA-2009:1148 ⁵⁷⁰⁷ REDHAT RHSA-2009:1156 ⁵⁷⁰⁸ SECUNIA 35691 ⁵⁷⁰⁹ SECUNIA 35721 ⁵⁷¹⁰ SECUNIA 35793 ⁵⁷¹¹ SECUNIA 35865 ⁵⁷¹² SECUNIA 37152 ⁵⁷¹³ SECUNIA 37221 ⁵⁷¹⁴ SUSE SUSE-SA:2009:050 ⁵⁷¹⁵ URL1 ⁵⁷¹⁶		instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz
10.	Apache HTTPD: APR-util off-by-one overflow (CVE-2009-1956) (apache-httpd-cve-2009-1956)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja prisustva mod_proxy modula. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy. Zlonamerni napadač bi mogao da iskoristi ovaj propust na takav način da primora proxy proces da zauzme veliku količinu CPU vremena.	APPLE APPLE-SA-2009-11-09 ⁵⁷¹⁷ BID 35251 ⁵⁷¹⁸ CVE CVE-2009-1956 ⁵⁷¹⁹ OVAL OVAL11567 ⁵⁷²⁰ OVAL OVAL12237 ⁵⁷²¹ REDHAT RHSA-2009:1107 ⁵⁷²² REDHAT RHSA-2009:1108 ⁵⁷²³ SECUNIA 34724 ⁵⁷²⁴ SECUNIA 35284 ⁵⁷²⁵ SECUNIA 35395 ⁵⁷²⁶ SECUNIA 35487 ⁵⁷²⁷ SECUNIA 35565 ⁵⁷²⁸ SECUNIA 35710 ⁵⁷²⁹ SECUNIA 35797 ⁵⁷³⁰ SECUNIA 35843 ⁵⁷³¹ SECUNIA 37221 ⁵⁷³²	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

⁵⁷⁰¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1890>⁵⁷⁰² <http://www.debian.org/security/2009/dsa-1834>⁵⁷⁰³ <http://osvdb.org/55553>⁵⁷⁰⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12330>⁵⁷⁰⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8616>⁵⁷⁰⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9403>⁵⁷⁰⁷ <http://rhn.redhat.com/errata/RHSA-2009-1148.html>⁵⁷⁰⁸ <http://rhn.redhat.com/errata/RHSA-2009-1156.html>⁵⁷⁰⁹ <http://secunia.com/advisories/35691/>⁵⁷¹⁰ <http://secunia.com/advisories/35721/>⁵⁷¹¹ <http://secunia.com/advisories/35793/>⁵⁷¹² <http://secunia.com/advisories/35865/>⁵⁷¹³ <http://secunia.com/advisories/37152/>⁵⁷¹⁴ <http://secunia.com/advisories/37221/>⁵⁷¹⁵ <https://www.suse.com/support/security/advisories/>⁵⁷¹⁶ http://httpd.apache.org/security/vulnerabilities_22.html⁵⁷¹⁷ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>⁵⁷¹⁸ <http://www.securityfocus.com/bid/35251>⁵⁷¹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1956>⁵⁷²⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11567>⁵⁷²¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12237>⁵⁷²² <http://rhn.redhat.com/errata/RHSA-2009-1107.html>⁵⁷²³ <http://rhn.redhat.com/errata/RHSA-2009-1108.html>⁵⁷²⁴ <http://secunia.com/advisories/34724/>⁵⁷²⁵ <http://secunia.com/advisories/35284/>⁵⁷²⁶ <http://secunia.com/advisories/35395/>⁵⁷²⁷ <http://secunia.com/advisories/35487/>⁵⁷²⁸ <http://secunia.com/advisories/35565/>⁵⁷²⁹ <http://secunia.com/advisories/35710/>⁵⁷³⁰ <http://secunia.com/advisories/35797/>⁵⁷³¹ <http://secunia.com/advisories/35843/>

			URL ⁵⁷³³		
11.	Apache HTTPD: expat DoS (CVE-2009-3560) (apache-httpd-cve-2009-3560)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u mogućnosti da dovede do toga da Apache parsira nepoverljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	BID 37203 ⁵⁷³⁴ CVE CVE-2009-3560 ⁵⁷³⁵ DEBIAN DSA-1953 ⁵⁷³⁶ IAVM 2012-A-0020 ⁵⁷³⁷ OVAL OVAL10613 ⁵⁷³⁸ OVAL OVAL6883 ⁵⁷³⁹ OVAL OVAL12942 ⁵⁷⁴⁰ REDHAT RHSA-2011:0896 ⁵⁷⁴¹ SECUNIA 37537 ⁵⁷⁴² SECUNIA 38231 ⁵⁷⁴³ SECUNIA 38794 ⁵⁷⁴⁴ SECUNIA 38832 ⁵⁷⁴⁵ SECUNIA 38834 ⁵⁷⁴⁶ SECUNIA 39478 ⁵⁷⁴⁷ SECUNIA 41701 ⁵⁷⁴⁸ SECUNIA 43300 ⁵⁷⁴⁹ URL ⁵⁷⁵⁰	Ozbiljan	Mnoge platforme i mnogi distributeri daju unapred formirane binarne pakete za Apache. Ovi unapred formirani paketi su najčešće standardizovani i optimizirani za određenu distribuciju, pa se zato savetuje korišćenje paketa predefinisanih za određeni OS, ukoliko su dostupni. Uraditi download a zatim instalirati: Apache HTTPD >= 2.0 and < 2.0.64 Upgrade to Apache HTTPD version 2.0.64 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.17 Upgrade to Apache HTTPD version 2.2.17 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
12.	Apache httpd expat DoS (CVE-2009-3720) (apache-httpd-2_2_x-cve-2009-3720)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u mogućnosti da dovede do toga da Apache parsira nepoverljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer	CVE CVE-2009-3720 ⁵⁷⁵¹ OVAL OVAL11019 ⁵⁷⁵² OVAL OVAL7112 ⁵⁷⁵³ OVAL OVAL12719 ⁵⁷⁵⁴ IAVM 2012-A-0020 ⁵⁷⁵⁵ REDHAT RHSA-2010:0002 ⁵⁷⁵⁶ REDHAT RHSA-2011:0896 ⁵⁷⁵⁷ SECUNIA 37324 ⁵⁷⁵⁸ SECUNIA 37537 ⁵⁷⁵⁹ SECUNIA 37925 ⁵⁷⁶⁰	Ozbiljan	Mnoge platforme i mnogi distributeri daju unapred formirane binarne pakete za Apache. Ovi unapred formirani paketi su najčešće standardizovani i optimizirani za određenu distribuciju, pa se zato savetuje korišćenje paketa predefinisanih za određeni OS, ukoliko su dostupni. Apache HTTPD >= 2.0 and

⁵⁷³² <http://secunia.com/advisories/37221/>⁵⁷³³ http://httpd.apache.org/security/vulnerabilities_22.html⁵⁷³⁴ <http://www.securityfocus.com/bid/37203>⁵⁷³⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3560>⁵⁷³⁶ <http://www.debian.org/security/2009/dsa-1953>⁵⁷³⁷ <http://iase.disa.mil/stigs/iavm-cve.html>⁵⁷³⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10613>⁵⁷³⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6883>⁵⁷⁴⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12942>⁵⁷⁴¹ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁵⁷⁴² <http://secunia.com/advisories/37537/>⁵⁷⁴³ <http://secunia.com/advisories/38231/>⁵⁷⁴⁴ <http://secunia.com/advisories/38794/>⁵⁷⁴⁵ <http://secunia.com/advisories/38832/>⁵⁷⁴⁶ <http://secunia.com/advisories/38834/>⁵⁷⁴⁷ <http://secunia.com/advisories/39478/>⁵⁷⁴⁸ <http://secunia.com/advisories/41701/>⁵⁷⁴⁹ <http://secunia.com/advisories/43300/>⁵⁷⁵⁰ http://httpd.apache.org/security/vulnerabilities_22.html⁵⁷⁵¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3720>⁵⁷⁵² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11019>⁵⁷⁵³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7112>⁵⁷⁵⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12719>⁵⁷⁵⁵ <http://iase.disa.mil/stigs/iavm-cve.html>⁵⁷⁵⁶ <http://rhn.redhat.com/errata/RHSA-2010-0002.html>⁵⁷⁵⁷ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁵⁷⁵⁸ <http://secunia.com/advisories/37324/>⁵⁷⁵⁹ <http://secunia.com/advisories/37537/>⁵⁷⁶⁰ <http://secunia.com/advisories/37925/>

		over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	SECUNIA 38050 ⁵⁷⁶¹ SECUNIA 38231 ⁵⁷⁶² SECUNIA 38794 ⁵⁷⁶³ SECUNIA 38832 ⁵⁷⁶⁴ SECUNIA 38834 ⁵⁷⁶⁵ SECUNIA 39478 ⁵⁷⁶⁶ SECUNIA 41701 ⁵⁷⁶⁷ SECUNIA 43300 ⁵⁷⁶⁸ SECUNIA 42326 ⁵⁷⁶⁹ SECUNIA 42338 ⁵⁷⁷⁰ URL1 ⁵⁷⁷¹		< 2.0.64 Upgrade to Apache HTTPD version 2.0.64 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.17 Upgrade to Apache HTTPD version 2.2.17. Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
13.	Apache HTTPD: apr_bridage_split_line DoS (CVE-2010-1623) (apache-httpd-cve-2010-1623)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je osjetljiv na ovu ranjivost SAMO ako Apache procesira ne-SSL zahteve. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_brigade_split_line() u sklopu APR-util library, koji se koristi za procesiranje ne-SSL zahteva. Zlonamerni napadač bi mogao da šalje zahteve, pažljivo izrađujući tajming za pojedinačne bajtove, što bi polako zauzimalo memoriju i potencijalno dovelo do odbijanja servisa.	BID 43673 ⁵⁷⁷² CVE CVE-2010-1623 ⁵⁷⁷³ IAVM 2012-B-0056 ⁵⁷⁷⁴ OVAL OVAL12800 ⁵⁷⁷⁵ REDHAT RHSA-2010-0950 ⁵⁷⁷⁶ REDHAT RHSA-2011-0896 ⁵⁷⁷⁷ REDHAT RHSA-2011-0897 ⁵⁷⁷⁸ SECUNIA 41701 ⁵⁷⁷⁹ SECUNIA 42015 ⁵⁷⁸⁰ SECUNIA 42361 ⁵⁷⁸¹ SECUNIA 42367 ⁵⁷⁸² SECUNIA 42403 ⁵⁷⁸³ SECUNIA 42537 ⁵⁷⁸⁴ SECUNIA 43211 ⁵⁷⁸⁵ SECUNIA 43285 ⁵⁷⁸⁶ URL1 ⁵⁷⁸⁷	Ozbiljan	Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
14.	Apache httpd mod_cache and mod_dav DoS (CVE-2010-1452) (apache-httpd-2_2_x-	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je osjetljiv na ovu	APPLE APPLE-SA-2011-03-21 ⁵⁷⁸⁸ CVE CVE-2010-1452 ⁵⁷⁸⁹ IAVM 2012-B-0056 ⁵⁷⁹⁰ OVAL OVAL12341 ⁵⁷⁹¹	Ozbiljan	Mnoge platforme i mnogi distributeri daju unapred formirane binarne pakete za Apache. Ovi unapred formirani paketi su najčešće

⁵⁷⁶¹ <http://secunia.com/advisories/38050/>⁵⁷⁶² <http://secunia.com/advisories/38231/>⁵⁷⁶³ <http://secunia.com/advisories/38794/>⁵⁷⁶⁴ <http://secunia.com/advisories/38832/>⁵⁷⁶⁵ <http://secunia.com/advisories/38834/>⁵⁷⁶⁶ <http://secunia.com/advisories/39478/>⁵⁷⁶⁷ <http://secunia.com/advisories/41701/>⁵⁷⁶⁸ <http://secunia.com/advisories/43300/>⁵⁷⁶⁹ <http://secunia.com/advisories/42326/>⁵⁷⁷⁰ <http://secunia.com/advisories/42338/>⁵⁷⁷¹ http://httpd.apache.org/security/vulnerabilities_22.html⁵⁷⁷² <http://www.securityfocus.com/bid/43673>⁵⁷⁷³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1623>⁵⁷⁷⁴ <http://iase.disa.mil/stigs/iavm-cve.html>⁵⁷⁷⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12800>⁵⁷⁷⁶ <http://rhn.redhat.com/errata/RHSA-2010-0950.html>⁵⁷⁷⁷ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁵⁷⁷⁸ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>⁵⁷⁷⁹ <http://secunia.com/advisories/41701/>⁵⁷⁸⁰ <http://secunia.com/advisories/42015/>⁵⁷⁸¹ <http://secunia.com/advisories/42361/>⁵⁷⁸² <http://secunia.com/advisories/42367/>⁵⁷⁸³ <http://secunia.com/advisories/42403/>⁵⁷⁸⁴ <http://secunia.com/advisories/42537/>⁵⁷⁸⁵ <http://secunia.com/advisories/43211/>⁵⁷⁸⁶ <http://secunia.com/advisories/43285/>⁵⁷⁸⁷ http://httpd.apache.org/security/vulnerabilities_22.html⁵⁷⁸⁸ <http://lists.apple.com/archives/security-announce/2011/Mar/msg00006.html>⁵⁷⁸⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1452>⁵⁷⁹⁰ <http://iase.disa.mil/stigs/iavm-cve.html>⁵⁷⁹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12341>

	mod_cache-andmod_dav-dos-cve-2010-1452)	ranjivost SAMO ako web server izvršava jedan od sledećih modula: mod_cache, mod_dav. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u obradi zahteva od strane mod_cache i mod_dav. Zlonameran napadač bi mogao da pošalje pažljivo izrađen zahtev i prouzrokuje da httpd child proces krahira. Ovakvo krahiranje bi se manifestovalo samo kao odbijanje servisa ako se koristi Worker MPM. Ovaj problem se dalje može ublažiti ako na mod_dav samo utiču zahtevi za koje postoji mogućnost autentifikovanja, a mod_cache je pod uticajem samo ako se koristi neuobičajena „CacheIgnoreURLSessionIdentifiers“ direktiva, uvedena u verziji 2.2.14. Ovaj problem je prijavio Mark Drayton.	REDHAT 2011:0896 ⁵⁷⁹² REDHAT 2011:0897 ⁵⁷⁹³ OVAL OVAL11683 ⁵⁷⁹⁴ REDHAT 2010:0659 ⁵⁷⁹⁵ SECUNIA 42367 ⁵⁷⁹⁶ URL1 ⁵⁷⁹⁷		standardizovani i optimizirani za određenu distribuciju, pa se zato savetuje korišćenje paketa predefinisanih za određeni OS, ukoliko su dostupni. Apache HTTPD >= 2.2 and < 2.2.16Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.16.tar.gz Apache HTTPD >= 2.0 and < 2.0.64 Upgrade to Apache HTTPD version 2.0.64 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
15.	Apache httpd Timeout detection flaw (mod_proxy_http) (CVE-2010-2068) (apache-httpd-2_2_x-timeoutdetection-flaw-mod_proxy_http-cve-2010-2068)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Propust sa kojim je omogućeno otkrivanje informacija je otkriven u modulu mod_proxy_http na verzijama 2.2.9 do 2.2.15, 2.3.4-alpha i 2.3.5-alpha. Pod određenim tajmout uslovima, server bi mogao da uzvрати odgovorom koji je namenjen drugom korisniku. Ugrožene su one konfiguracije koje pokreću korišćenje proxy worker pool-ova. Na ranijim verzijama nije bilo ranjivosti, jer proxy pool-ovi još nisu bili uvedeni. Zahvaljujući Loren Anderson-u ovaj problem je prijavljen, a najjednostavniji način njegovog izbegavanja jeste opšte konfigurisanje.	APPLE APPLE-SA-2011-03-21 ⁵⁷⁹⁸ BID 40827 ⁵⁷⁹⁹ CVE CVE-2010-2068 ⁵⁸⁰⁰ OVAL OVAL11491 ⁵⁸⁰¹ OVAL OVAL6931 ⁵⁸⁰² SECUNIA 40206 ⁵⁸⁰³ SECUNIA 41480 ⁵⁸⁰⁴ SECUNIA 41490 ⁵⁸⁰⁵ SECUNIA 41722 ⁵⁸⁰⁶ XF apache-modproxyhttp-timeout-info-disc(59413) ⁵⁸⁰⁷ URL1 ⁵⁸⁰⁸	Ozbiljan	Mnoge platforme i mnogi distributeri daju unapred formirane binarne pakete za Apache. Ovi unapred formirani paketi su najčešće standardizovani i optimizirani za određenu distribuciju, pa se zato savetuje korišćenje paketa predefinisanih za određeni OS, ukoliko su dostupni. Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.16.tar.gz
16.	Apache httpd Timeout detection flaw (mod_proxy_http) (CVE-2010-2791) (apache-httpd-2_2_x-	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je osetljiv na ovu	BID 42102 ⁵⁸⁰⁹ CVE CVE-2010-2791 ⁵⁸¹⁰ IAVM 2012-B-0056 ⁵⁸¹¹ REDHAT 2010:0659 ⁵⁸¹² RHS-	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.10 Uradi download a zatim instalirati: http://archive.apache.org/dis

⁵⁷⁹² <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁵⁷⁹³ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>⁵⁷⁹⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11683>⁵⁷⁹⁵ <http://rhn.redhat.com/errata/RHSA-2010-0659.html>⁵⁷⁹⁶ <http://secunia.com/advisories/42367/>⁵⁷⁹⁷ http://httpd.apache.org/security/vulnerabilities_22.html⁵⁷⁹⁸ <http://lists.apple.com/archives/security-announce/2011/Mar/msg00006.html>⁵⁷⁹⁹ <http://www.securityfocus.com/bid/40827>⁵⁸⁰⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2068>⁵⁸⁰¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11491>⁵⁸⁰² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6931>⁵⁸⁰³ <http://secunia.com/advisories/40206/>⁵⁸⁰⁴ <http://secunia.com/advisories/41480/>⁵⁸⁰⁵ <http://secunia.com/advisories/41490/>⁵⁸⁰⁶ <http://secunia.com/advisories/41722/>⁵⁸⁰⁷ <http://xforce.iss.net/xforce/xfdb/59413>⁵⁸⁰⁸ http://httpd.apache.org/security/vulnerabilities_22.html⁵⁸⁰⁹ <http://www.securityfocus.com/bid/42102>⁵⁸¹⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2791>⁵⁸¹¹ <http://iase.disa.mil/stigs/iavm-cve.html>

	timeoutdetection-flaw-mod_proxy_http-cve-2010-2791)	ranjivost SAMO ako web server izvršava jedan od sledećih modula: mod_proxy_http. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust sa kojim je omogućeno otkrivanje informacija je otkriven u modulu mod_proxy_http, samo u verziji 2.2.9 na Unix platformama. Pod određenim tajmaut uslovima, server bi mogao da uzvрати odgovorom koji je namenjen drugom korisniku. Ugrožene su samo one konfiguracije koje pokreću korišćenje proxy worker pool-ova. Na ranijim verzijama nije bilo ranjivosti, jer proxy pool-ovi još nisu bili uvedeni.	XF apache-modproxy-info-disclosure(60883) ⁵⁸¹³ URL ⁵⁸¹⁴		t/httpd/httpd-2.2.10.tar.gz
17.	X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch)	172.23.202.124:443 172.23.202.220:443 Pre izdavanja sertifikata, Certification Authority (CA) mora da proveriti identitet pojedinca koji potražuje sertifikat, kako je navedeno u CA-ovom Certification Practice Statement (CPS). Zbog toga, uobičajene procedure validacije sertifikata zahtevaju da rubrika sertifikata sa CN subjektom odgovara pravom imenu pojedinca koji prikazuje sertifikat. Na primer, u sertifikatu prikazanom na „https://www.example.com/“, naziv subjekta (CN) treba da bude „www.example.com“. U cilju otkrivanja i sprečavanja napada prisluškivanja, validnost sertifikata mora da bude overena, jer bi u suprotnom napadač mogao da otpočne napad preko posrednika i da stekne potpunu kontrolu nad protokom podataka. Od posebne važnosti je validnost naziva subjekta (CN), koji treba da se poklapa sa imenom pojedinca (imenom host-a). Neodgovarajući CN se najčešće javlja usled greške u konfiguraciji, iako on takođe može da ukazuje na to da se sprovodi napad preko posrednika.		Ozbiljan	Rubrika sa uobičajenim nazivom subjekta (CN) u sertifikatu X.509 treba da bude podešena da sadrži ime pojedinca koji prikazuje sertifikat (npr. ime hosta). To se postiže izradom novog sertifikata, koji najčešće potpisuje Certification Authority (CA), koji je od poverenja kako za klijenta, tako i za server.
18.	X.509 Server Certificate Is Invalid/Expired (tls-server-cert-expired)	Sertifikat X.509 na TLS/SSL serveru sadrži početni datum iz budućnosti ili je istekao. Proveriti proof za više detalja.		Ozbiljan	Nabaviti novi TLS/SSL serverov sertifikat i instalirati ga na server. Precizna uputstva za dobijanje novog sertifikata zavise od zahteva organizacije. Uopšteno, treba napraviti zahtev za sertifikat i taj zahtev sačuvati kao fajl. Ovaj fajl se zatim šalje Certificate Authority-ju (CA) na obradu. Proveriti da li su početni i završni datumi na novom sertifikatu validni. Organizacija možda

⁵⁸¹² <http://rhn.redhat.com/errata/RHSA-2010-0659.html>⁵⁸¹³ <http://xforce.iss.net/xforce/xfdb/60883>⁵⁸¹⁴ http://httpd.apache.org/security/vulnerabilities_22.html

					posедује sopstveni interni Certificate Authority. U suprotnom, potrebno je platiti sertifikat iz spoljnog poverljivog Certificate Authority-ja. Nakon prijema novog sertifikata od Certificate Authority-ja, potrebno je instalirati ga na TLS/SSL server. Tačna uputstva za instaliranje su za svaki proizvod različita. Proveriti njihovu dokumentaciju.
19.	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368) (apache-httpd-cve-2011-3368)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja prisustva mod_proxy modula. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy. Zlonamerni napadač bi mogao da iskoristi ovaj propust na takav način da primora proxy proces da se poveže sa proizvoljnim serverom i potencijalno objavi osetljive informacije sa internih web servera koje inače napadaču nisu direktno dostupne. Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/	APPLE APPLE-SA-2012-09-19-2 ⁵⁸¹⁵ BID 49957 ⁵⁸¹⁶ CVE CVE-2011-3368 ⁵⁸¹⁷ IAVM 2012-A-0017 ⁵⁸¹⁸ IAVM 2012-A-0152 ⁵⁸¹⁹ IAVM 2012-B-0056 ⁵⁸²⁰ OSVDB 76079 ⁵⁸²¹ REDHAT RHSA-2011:1391 ⁵⁸²² REDHAT RHSA-2011:1392 ⁵⁸²³ SECUNIA 46288 ⁵⁸²⁴ SECUNIA 46414 ⁵⁸²⁵ SECUNIA 48551 ⁵⁸²⁶ XF 70336 ⁵⁸²⁷ URL1 5828 URL2 5829 URL3 5830	Ozbiljan	Apache HTTPD >= 1.3 and < 2 Apply the patch for CVE-2011-3368 to 1.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
20.	Apache HTTPD: scoreboard parent DoS (CVE-2012-0031) (apache-httpd-cve-	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Propust je otkriven u obradi	APPLE APPLE-SA-2012-09-19-2 ⁵⁸³¹ BID 51407 ⁵⁸³² CVE CVE-2012-0031 ⁵⁸³³ IAVM 2012-A-0017 ⁵⁸³⁴	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim

⁵⁸¹⁵ [http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html](https://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html)⁵⁸¹⁶ <http://www.securityfocus.com/bid/49957>⁵⁸¹⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3368>⁵⁸¹⁸ <http://iase.disa.mil/stigs/iavm-cve.html>⁵⁸¹⁹ <http://iase.disa.mil/stigs/iavm-cve.html>⁵⁸²⁰ <http://iase.disa.mil/stigs/iavm-cve.html>⁵⁸²¹ <http://www.osvdb.org/76079>⁵⁸²² <http://rhn.redhat.com/errata/RHSA-2011-1391.html>⁵⁸²³ <http://rhn.redhat.com/errata/RHSA-2011-1392.html>⁵⁸²⁴ <http://secunia.com/advisories/46288/>⁵⁸²⁵ <http://secunia.com/advisories/46414/>⁵⁸²⁶ <http://secunia.com/advisories/48551/>⁵⁸²⁷ <http://xforce.iss.net/xforce/xfdb/70336>⁵⁸²⁸ http://httpd.apache.org/security/vulnerabilities_13.html⁵⁸²⁹ http://httpd.apache.org/security/vulnerabilities_20.html⁵⁸³⁰ http://httpd.apache.org/security/vulnerabilities_22.html⁵⁸³¹ [http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html](https://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html)⁵⁸³² <http://www.securityfocus.com/bid/51407>⁵⁸³³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0031>

	2012-0031)	scoreboard-a. Neprivilegovani child proces bi mogao da dovede do toga da parent proces krahira prilikom gašenja.	REDHAT 2012:0128 ⁵⁸³⁵ RHSA-2012:0128 ⁵⁸³⁵ SECUNIA 47410 ⁵⁸³⁶ SECUNIA 48551 ⁵⁸³⁷ URL1 ⁵⁸³⁸ URL2 ⁵⁸³⁹		instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
21.	Apache HTTPD: mod_rewrite log escape filtering (CVE-2013-1862) (apache-httpd-cve-2013-1862)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_rewrite. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Modul mod_rewrite ne filtrira završne izlazne sekvence iz logova, što zlonamenrom napadaču olakšava da ubace takve sekvence u završne emulatore koji sadrže ranjivosti koje se odnose na izlazne sekvence.	CVE CVE-2013-1862 ⁵⁸⁴⁰ OVAL OVAL18790 ⁵⁸⁴¹ REDHAT 2013:0815 ⁵⁸⁴² RHSA-2013:0815 ⁵⁸⁴² REDHAT 2013:1207 ⁵⁸⁴³ RHSA-2013:1207 ⁵⁸⁴³ REDHAT 2013:1208 ⁵⁸⁴⁴ RHSA-2013:1208 ⁵⁸⁴⁴ REDHAT 2013:1209 ⁵⁸⁴⁵ RHSA-2013:1209 ⁵⁸⁴⁵ SECUNIA 55032 ⁵⁸⁴⁶ URL1 ⁵⁸⁴⁷ URL2 ⁵⁸⁴⁸	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.25 Ažurirati na Apache HTTPD version 2.2.25 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.25.tar.gz
22.	Apache Tomcat default installation/welcome page installed (apache-tomcat-default-install-page)	172.23.202.124:8080 172.23.202.220:8080 Tomcat difoltna instalacija ili „Welcome“ stranica je instalirana na serveru. To obično ukazuje na novoinstalirani server. U mnogim slučajevima, Tomcat se instalira zajedno sa drugim aplikacijama i korisnik možda nije svestan da je web server pokrenut. Ovakvi serveri se retko patch-uju i još rede nadgledaju, što zlonamernim napadačima postaje pogodna meta koja najverovatnije neće pokrenuti nikakvo upozorenje.		Ozbiljan	Ako se od servera zahteva da obezbedi neophodnu funkcionalnost, onda difoltnu stranicu treba zameniti odgovarajućim sadržajem. U suprotnom, ovakav server treba ukloniti sa mreže, prateći bezbednosni princip minimalne složenosti (više složenosti = manja bezbednost).
23.	Apache HTTPD: mod_setenvif .htaccess privilege escalation (CVE-2011-3607) (apache-httpd-cve-2011-3607)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je ranjiv ukoliko je	APPLE APPLE-SA-2012-09-19-2 ⁵⁸⁴⁹ BID 50494 ⁵⁸⁵⁰ CVE CVE-2011-3607 ⁵⁸⁵¹ IAVM 2012-A-0017 ⁵⁸⁵² IAVM 2012-A-0152 ⁵⁸⁵³	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati:

⁵⁸³⁴ <http://iase.disa.mil/stigs/iavm-cve.html>⁵⁸³⁵ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁵⁸³⁶ <http://secunia.com/advisories/47410/>⁵⁸³⁷ <http://secunia.com/advisories/48551/>⁵⁸³⁸ http://httpd.apache.org/security/vulnerabilities_20.html⁵⁸³⁹ http://httpd.apache.org/security/vulnerabilities_22.html⁵⁸⁴⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1862>⁵⁸⁴¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18790>⁵⁸⁴² <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁵⁸⁴³ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁵⁸⁴⁴ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁵⁸⁴⁵ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁵⁸⁴⁶ <http://secunia.com/advisories/55032/>⁵⁸⁴⁷ http://httpd.apache.org/security/vulnerabilities_20.html⁵⁸⁴⁸ http://httpd.apache.org/security/vulnerabilities_22.html⁵⁸⁴⁹ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁵⁸⁵⁰ <http://www.securityfocus.com/bid/50494>⁵⁸⁵¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3607>⁵⁸⁵² <http://iase.disa.mil/stigs/iavm-cve.html>⁵⁸⁵³ <http://iase.disa.mil/stigs/iavm-cve.html>

	3607)	na njemu pokrenut modul: mod_setenvif. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust preopterećenja je otkriven kada je omogućen modul mod_setenvif, što lokalnim korisnicima omogućava da dobiju privilegije preko fajla .htaccess.	OSVDB 76744 REDHAT RHSA-2012:0128 ⁵⁸⁵⁴ SECUNIA 45793 ⁵⁸⁵⁵ SECUNIA 48551 ⁵⁸⁵⁶ XF 71093 ⁵⁸⁵⁷ URL1 ⁵⁸⁵⁸ URL2 ⁵⁸⁵⁹		http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
24.	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-4317) (apache-httpd-cve-2011-4317)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja prisustva mod_proxy modula. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy. Zlonamerni napadač bi mogao da iskoristi ovaj propust na takav način da primora proxy proces da se poveže sa proizvoljnim serverom i potencijalno objavi osetljive informacije sa internih web servera koje inače napadaču nisu direktno dostupne.	APPLE APPLE-SA-2012-09-19-2 ⁵⁸⁶⁰ CVE CVE-2011-4317 ⁵⁸⁶¹ IAVM 2012-A-0017 ⁵⁸⁶² IAVM 2012-A-0152 ⁵⁸⁶³ REDHAT RHSA-2012:0128 ⁵⁸⁶⁴ SECUNIA 48551 ⁵⁸⁶⁵ URL1 ⁵⁸⁶⁶	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
25.	Apache HTTPD: error responses can expose cookies (CVE-2012-0053) (apache-httpd-cve-2012-0053)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Propust je otkriven u difoltnom pogrešnom odgovoru za statusni kôd 400. Zlonamerni napadač bi mogao da iskoristi ovaj propust da objavi "httpOnly" kolačiće ako nije određen dokument custom ErrorDocument.	APPLE APPLE-SA-2012-09-19-2 ⁵⁸⁶⁷ BID 51706 ⁵⁸⁶⁸ CVE CVE-2012-0053 ⁵⁸⁶⁹ IAVM 2012-A-0017 ⁵⁸⁷⁰ REDHAT RHSA-2012:0128 ⁵⁸⁷¹ SECUNIA 48551 ⁵⁸⁷² URL1 ⁵⁸⁷³ URL2 ⁵⁸⁷⁴	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
26.	Apache HTTPD: XSS due to unescaped	172.23.202.124:80 172.23.202.124:443	APPLE APPLE-SA-2013-09-12-1 ⁵⁸⁷⁵	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.24

⁵⁸⁵⁴ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁵⁸⁵⁵ <http://secunia.com/advisories/45793/>⁵⁸⁵⁶ <http://secunia.com/advisories/48551/>⁵⁸⁵⁷ <http://xforce.iss.net/xforce/xfdb/71093>⁵⁸⁵⁸ http://httpd.apache.org/security/vulnerabilities_20.html⁵⁸⁵⁹ http://httpd.apache.org/security/vulnerabilities_22.html⁵⁸⁶⁰ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁵⁸⁶¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4317>⁵⁸⁶² <http://iase.disa.mil/stigs/iavm-cve.html>⁵⁸⁶³ <http://iase.disa.mil/stigs/iavm-cve.html>⁵⁸⁶⁴ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁵⁸⁶⁵ <http://secunia.com/advisories/48551/>⁵⁸⁶⁶ http://httpd.apache.org/security/vulnerabilities_22.html⁵⁸⁶⁷ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁵⁸⁶⁸ <http://www.securityfocus.com/bid/51706>⁵⁸⁶⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0053>⁵⁸⁷⁰ <http://iase.disa.mil/stigs/iavm-cve.html>⁵⁸⁷¹ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁵⁸⁷² <http://secunia.com/advisories/48551/>⁵⁸⁷³ http://httpd.apache.org/security/vulnerabilities_20.html⁵⁸⁷⁴ http://httpd.apache.org/security/vulnerabilities_22.html⁵⁸⁷⁵ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>

	hostnames (CVE-2012-3499) (apache-httpd-cve-2012-3499)	172.23.202.220:80 172.23.202.220:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut jedan od sledećih modula: mod_imagemap, mod_info, mod_ldap, mod_proxy_ftp, mod_status. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Različiti XSS propusti usled nenapuštenih host imena i URI-ja HTML output-a u mod_info, mod_status, mod_imagemap, mod_ldap i mod_proxy_ftp.	CVE CVE-2012-3499 ⁵⁸⁷⁶ DEBIAN DSA-2637 ⁵⁸⁷⁷ REDHAT RHSA-2013:0815 ⁵⁸⁷⁸ REDHAT RHSA-2013:1207 ⁵⁸⁷⁹ REDHAT RHSA-2013:1208 ⁵⁸⁸⁰ REDHAT RHSA-2013:1209 ⁵⁸⁸¹ SECUNIA 55032 ⁵⁸⁸² URL1 ⁵⁸⁸³ URL2 ⁵⁸⁸⁴		Ažurirati na Apache HTTPD version 2.2.24 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz Apache HTTPD >= 2.4 and < 2.4.4 Ažurirati na Apache HTTPD version 2.4.4 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz
27.	Apache HTTPD: XSS in mod_proxy_balancer (CVE-2012-4558) (apache-httpd-cve-2012-4558)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy_balancer. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. XSS propust je uticao na manager interfejs mod_proxy_balancer-a.	APPLE APPLE-SA-2013-09-12-1 ⁵⁸⁸⁵ CVE CVE-2012-4558 ⁵⁸⁸⁶ DEBIAN DSA-2637 ⁵⁸⁸⁷ REDHAT RHSA-2013:0815 ⁵⁸⁸⁸ REDHAT RHSA-2013:1207 ⁵⁸⁸⁹ REDHAT RHSA-2013:1208 ⁵⁸⁹⁰ REDHAT RHSA-2013:1209 ⁵⁸⁹¹ URL1 ⁵⁸⁹² URL2 ⁵⁸⁹³	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.24 Ažurirati na Apache HTTPD version 2.2.24 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz Apache HTTPD >= 2.4 and < 2.4.4 Ažurirati na Apache HTTPD version 2.4.4 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz
28.	Apache HTTPD: mod_dav crash (CVE-2013-1896) (apache-httpd-cve-2013-1896)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_dav_svn. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Slanje MERGE zahteva URI-ju koji obrađuje mod_dav_svn sa izvorom href (poslato kao deo zahteva XML) ciljajući na URI koji	CVE CVE-2013-1896 ⁵⁸⁹⁴ OVAL OVAL18835 ⁵⁸⁹⁵ REDHAT RHSA-2013:1156 ⁵⁸⁹⁶ REDHAT RHSA-2013:1207 ⁵⁸⁹⁷ REDHAT RHSA-2013:1208 ⁵⁸⁹⁸ REDHAT RHSA-2013:1209 ⁵⁸⁹⁹ SECUNIA 55032 ⁵⁹⁰⁰ URL1 ⁵⁹⁰¹	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.25 Ažurirati na Apache HTTPD version 2.2.25 Apache HTTPD >= 2.4 and < 2.4.6 Ažurirati na Apache HTTPD version 2.4.6 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.6.tar.gz

⁵⁸⁷⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3499>⁵⁸⁷⁷ <http://www.debian.org/security/2013/dsa-2637>⁵⁸⁷⁸ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁵⁸⁷⁹ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁵⁸⁸⁰ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁵⁸⁸¹ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁵⁸⁸² <http://secunia.com/advisories/55032/>⁵⁸⁸³ http://httpd.apache.org/security/vulnerabilities_22.html⁵⁸⁸⁴ http://httpd.apache.org/security/vulnerabilities_24.html⁵⁸⁸⁵ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁵⁸⁸⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4558>⁵⁸⁸⁷ <http://www.debian.org/security/2013/dsa-2637>⁵⁸⁸⁸ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁵⁸⁸⁹ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁵⁸⁹⁰ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁵⁸⁹¹ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁵⁸⁹² http://httpd.apache.org/security/vulnerabilities_22.html⁵⁸⁹³ http://httpd.apache.org/security/vulnerabilities_24.html⁵⁸⁹⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1896>⁵⁸⁹⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18835>⁵⁸⁹⁶ <http://rhn.redhat.com/errata/RHSA-2013-1156.html>⁵⁸⁹⁷ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁵⁸⁹⁸ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁵⁸⁹⁹ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁵⁹⁰⁰ <http://secunia.com/advisories/55032/>⁵⁹⁰¹ http://httpd.apache.org/security/vulnerabilities_22.html

		nije konfigurisan za DAV prouzrokuje segmentation fault (segfault).	URL ⁵⁹⁰²		
29.	FTP access with ftp account (ftp-generic-0001)	172.23.202.124:21 172.23.202.220:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisničkim ID-jem „ftp“ i šifrom „ftp“. Dosadašnja praksa je pokazala da treba ukloniti difoltnu naloge, ako je to moguće. Za naloge koje zahteva sistem, treba promeniti difoltnu šifru.	CVE CVE-1999-0497 ⁵⁹⁰³	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko to nije kritično za dalje funkcionisanje sistema. U suprotnom, treba promeniti lozinku u nedifoltnu vrednost.
30.	FTP access with anonymous account (ftp-generic-0002)	172.23.202.124:21 172.23.202.220:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisničkim ID-jem „anonymous“ i šifrom „ftp@“. Dosadašnja praksa je pokazala da treba ukloniti difoltnu naloge, ako je to moguće. Za naloge koje zahteva sistem, treba promeniti difoltnu šifru.	CVE CVE-1999-0497 ⁵⁹⁰⁴	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko to nije kritično za dalje funkcionisanje sistema. U suprotnom, treba promeniti lozinku u nedifoltnu vrednost.
31..	FTP server does not support AUTH command (ftp-generic-0007)	172.23.202.124:21 172.23.202.220:21 Klijenti na FTP server po difoltu šalju poverljive podatke (korisnički ID i šifru) u vidu čitkog teksta. Ova okolnost dozvoljava zlonamernim korisnicima omogućava da presreću poverljive podatke ukoliko prisluškuju vezu. Noviji FTP serveri podržavaju komandu AUTH, koja daje veće opcije autentifikacije, kao TLS, Kerberos, GSSAPI, itd. Njih treba koristiti da bi se sprečilo prisluškivanje na FTP vezama.		Ozbiljan	Nadograditi/Ažurirati na a FTP server koji podržava komandu AUTH.
32.	Apache HTTPD: AllowOverride Options handling bypass (CVE-2009-1195) (apache-httpd-cve-2009-1195)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako web server izvršava direktivu AllowOverride sa određenim opcijama koje se koriste. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u obradi direktiva „Options“ i „AllowOverride“. U konfiguracijama koje koriste direktivu „AllowOverride“ sa određenim „Options“ argumentima, lokalni korisnici mogu da izvršavaju	APPLE APPLE-SA-2009-11-09 ⁵⁹⁰⁵ BID 35115 ⁵⁹⁰⁶ CVE CVE-2009-1195 ⁵⁹⁰⁷ DEBIAN DSA-1816 ⁵⁹⁰⁸ OSVDB 54733 ⁵⁹⁰⁹ OVAL OVAL11094 ⁵⁹¹⁰ OVAL OVAL8704 ⁵⁹¹¹ OVAL OVAL12377 ⁵⁹¹² REDHAT RHSA-2009:1075 ⁵⁹¹³ REDHAT RHSA-2009:1156 ⁵⁹¹⁴ SECUNIA 35261 ⁵⁹¹⁵ SECUNIA 35264 ⁵⁹¹⁶ SECUNIA 35395 ⁵⁹¹⁷	Ozbiljan	Apache >= 2.2 and < 2.3 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

⁵⁹⁰² http://httpd.apache.org/security/vulnerabilities_24.html⁵⁹⁰³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>⁵⁹⁰⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>⁵⁹⁰⁵ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>⁵⁹⁰⁶ <http://www.securityfocus.com/bid/35115>⁵⁹⁰⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1195>⁵⁹⁰⁸ <http://www.debian.org/security/2009/dsa-1816>⁵⁹⁰⁹ <http://osvdb.org/54733>⁵⁹¹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11094>⁵⁹¹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8704>⁵⁹¹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12377>⁵⁹¹³ <http://rhn.redhat.com/errata/RHSA-2009-1075.html>⁵⁹¹⁴ <http://rhn.redhat.com/errata/RHSA-2009-1156.html>⁵⁹¹⁵ <http://secunia.com/advisories/35261/>⁵⁹¹⁶ <http://secunia.com/advisories/35264/>⁵⁹¹⁷ <http://secunia.com/advisories/35395/>

		komande iz web-serverskih skripti.	SECUNIA 35453 ⁵⁹¹⁸ SECUNIA 35721 ⁵⁹¹⁹ SECUNIA 37152 ⁵⁹²⁰ SUSE SUSE- SA:2009:050 ⁵⁹²¹ XF apache- allowoverrides-security- bypass(50808) ⁵⁹²² URL1 ⁵⁹²³		
33.	Apache HTTPD: mod_proxy_ajp DoS (CVE-2010-0408) (apache-httpd-cve- 2010-0408)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je osjetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ajp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Mod_proxy_ajp će vratiti pogrešan kôd statusa ako naiđe na grešku, prouzrokujući da backend server bude stavljen u status greške dok ne istekne vreme za ponovni pokušaj. Udaljeni napadač bi mogao da pošalje zlonameran zahtev da bi pokrenuo ovaj problem, što bi dovelo do odbijanja servisa. Zahvaljujući Niku Toivola iz Sulake Corporation ovaj problem je prijavljen uz predloženu adekvatnu meru zaštite u vidu zakrpe.	BID 38491 ⁵⁹²⁴ CVE CVE-2010-0408 ⁵⁹²⁵ DEBIAN DSA-2035 ⁵⁹²⁶ OVAL OVAL8619 ⁵⁹²⁷ OVAL OVAL9935 ⁵⁹²⁸ REDHAT RHSA- 2010:0168 ⁵⁹²⁹ SECUNIA 39100 ⁵⁹³⁰ SECUNIA 39501 ⁵⁹³¹ SECUNIA 39628 ⁵⁹³² SECUNIA 39632 ⁵⁹³³ SECUNIA 39656 ⁵⁹³⁴ SECUNIA 40096 ⁵⁹³⁵ URL1 ⁵⁹³⁶	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz
34.	Apache httpd mod_proxy_ftp DoS (CVE-2009-3094) (http- apache-mod_proxy_ftp- dos)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je osjetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ftp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust NULL pointer dereference (pointer sa NULL vrednošću upotrebljen kao da ukazuje na validnu	CVE CVE-2009-3094 ⁵⁹³⁷ DEBIAN DSA-1934 ⁵⁹³⁸ OVAL OVAL10981 ⁵⁹³⁹ OVAL OVAL8087 ⁵⁹⁴⁰ SECUNIA 36549 ⁵⁹⁴¹ SECUNIA 37152 ⁵⁹⁴² SUSE SUSE- SA:2009:050 ⁵⁹⁴³ URL1 ⁵⁹⁴⁴	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.64 Ažurirati na Apache HTTPD version 2.0.64 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.14 Ažurirati na Apache HTTPD version 2.2.14

⁵⁹¹⁸ <http://secunia.com/advisories/35453/>
⁵⁹¹⁹ <http://secunia.com/advisories/35721/>
⁵⁹²⁰ <http://secunia.com/advisories/37152/>
⁵⁹²¹ <https://www.suse.com/support/security/advisories/>
⁵⁹²² <http://xforce.iss.net/xforce/xfdb/50808>
⁵⁹²³ http://httpd.apache.org/security/vulnerabilities_22.html
⁵⁹²⁴ <http://www.securityfocus.com/bid/38491>
⁵⁹²⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0408>
⁵⁹²⁶ <http://www.debian.org/security/2010/dsa-2035>
⁵⁹²⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8619>
⁵⁹²⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9935>
⁵⁹²⁹ <http://rhn.redhat.com/errata/RHSA-2010-0168.html>
⁵⁹³⁰ <http://secunia.com/advisories/39100/>
⁵⁹³¹ <http://secunia.com/advisories/39501/>
⁵⁹³² <http://secunia.com/advisories/39628/>
⁵⁹³³ <http://secunia.com/advisories/39632/>
⁵⁹³⁴ <http://secunia.com/advisories/39656/>
⁵⁹³⁵ <http://secunia.com/advisories/40096/>
⁵⁹³⁶ http://httpd.apache.org/security/vulnerabilities_22.html
⁵⁹³⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3094>
⁵⁹³⁸ <http://www.debian.org/security/2009/dsa-1934>
⁵⁹³⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10981>
⁵⁹⁴⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8087>
⁵⁹⁴¹ <http://secunia.com/advisories/36549/>
⁵⁹⁴² <http://secunia.com/advisories/37152/>
⁵⁹⁴³ <https://www.suse.com/support/security/advisories/>
⁵⁹⁴⁴ http://httpd.apache.org/security/vulnerabilities_22.html

		memorijsku oblast) otkriven je u modulu mod_proxy_ftp. Zlonamerni FTP server, kojem su zahtevi proksirani, mogao bi da iskoristi ovaj propust u smislu obaranja http child procesa uz pomoć namerno izmenjenog odgovora EPSV ili PASV komandi, što bi dovelo do delimičnog odbijanja servisa.			Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.gz
35.	Apache httpd Solaris pollset DoS (CVE-2009-2699) (http://apache-solaris-pollset-dos)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Naden je propust koji utiče na Solaris pollset podršku (Event Port backend), a koji uzrokuje propust u APR-u. azlonamerni napadač bi mogao da pokrene ovaj problem na Solaris serverima koji bi koristio MPM-ove i doveo do odbijanja servisa.	BID 36596 ⁵⁹⁴⁵ CVE CVE-2009-2699 ⁵⁹⁴⁶ XF apache-solaris-pollset-dos(53666) ⁵⁹⁴⁷ URL1 ⁵⁹⁴⁸	Ozbiljan	Mnoge platforme i mnogi distributeri daju unapred formirane binarne pakete za Apache. Ovi unapred formirani paketi su najčešće standardizovani i optimizirani za određenu distribuciju, pa se zato savetuje korišćenje paketa predefinisanih za određeni OS, ukoliko su dostupni. Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.gz
36.	Browsable web directory (http-generic-browsable-dir)	172.23.202.124:8080 172.23.202.220:8080 Otkriven je direktorijum na web serveru koji može biti pretraživan, što znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice - spajdering (prateći hiperlinkove), ili -kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute force napadom na liste uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skrivenne“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice.		Ozbiljan	Za Apache: onemogućiti pretraživanje direktorijuma mreže za sve direktorijume i poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume. Za Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote: Onemogućiti pretraživanje direktorijuma za sve direktorijume i poddirektorijume. Uključiti Tomcat-ov web.xml file. U odeljku „default“, promeniti parametar „listings“ iz „true“ u „false“. Restartovati server.

⁵⁹⁴⁵ <http://www.securityfocus.com/bid/36596>⁵⁹⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2699>⁵⁹⁴⁷ <http://xforce.iss.net/xforce/xfdb/53666>⁵⁹⁴⁸ http://httpd.apache.org/security/vulnerabilities_22.html

					Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripta i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume.
37.	WebDAV PROPFIND Method Allows Web Directory Browsing (http-generic-propfind-dir-browsing)	172.23.202.124:8080 172.23.202.220:8080 Moguće je koristiti WebDAV PROPFIND metodu da bi se pretraživali web direktorijumi na serveru, što za posledicu ima otkrivanje sadržaja koji bi trebalo da bude sakriven. Ovo bi potencijalno omogućilo napadaču da dođe do osetljivih informacija, kao što su fajlovi podataka i backup fajlovi, ili bi dobio informacije o strukturi direktorijuma, koje bi se kasnije mogle koristiti za mnogo prefinjeniji napad. Sledeći HTTP objekti su preuzeti korišćenjem PROPFIND kroz /webdav/ /webdav//webdav/tomcat.gif/webdav/tomcat-power.gif/webdav/index.html		Ozbiljan	Apache ograničena HTTP PROPFIND Metoda za Apache. PROPFIND metoda bi trebalo da bude nedostupna za anonimne zahteve. Isključiti autentifikaciju na WebDAV direktorijumu tako da samo ovlašćeni korisnici mogu da pozovu ovu metodu i realizuju legitimne akcije, kao: <Location /webdav_dir/*> <LimitExcept GET HEAD OPTIONS POST> AuthType Basic AuthName „WebDAV Authentication“ AuthUserFile /path/to/userfile AuthGroupFile /path/to/groupfile potražujte grupne webdav korisnike </LimitExcept> </Location> Zatim napraviti fajl za lozinku i fajl za grupu: htpasswd -cs /path/to/userfile bob echo „webdavusers: bob“ > /path/to/groupfile Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote Ograničena HTTP PROPFIND metoda za Tomcat: U konfiguracionom fajlu web.xml za WebDAV-onemogućeni direktorijum, dodati sledeće da bi se ograničila funkcionalnost WebDAV za određenog korisnika (korisnike): <security-constraint> <web-resource-collection> <web-resource-name>WebDav Directory</web-resource-name>

					<pre> <url-pattern>/*</url-pattern> </web-resource-collection> <auth-constraint> <role-name>webdav-user</role-name> </auth-constraint> </security-constraint> <login-config> <auth-method>BASIC</auth-method> <realm-name>WebDAVRealm</realm-name> </login-config> <security-role> <description> Ovlastiti WebDAV korisnike </description> <role-name>webdav-user</role-name> </security-role> U fajlu conf/tomcat-users.xml, dodati WebDAV korisnika kao: <?xml version='1.0' encoding='utf-8'?> <tomcat-users> <role rolename="webdav-user"/> <user username="bob" password="b0bsp455w0rdy0!" roles="webdav-user"/> </tomcat-users> </pre>
38.	Form action submits sensitive data in the clear (http-generic-sensitive-form-data-unencrypted)	172.23.202.124:8080 172.23.202.220:8080 Web forma sadrži rubrike sa podacima koji su možda po prirodi osetljivi. Ovakvi podaci se prenose preko nezaštićene veze, koja bi mogla da omogući zlonamernim napadačima da prisluškujući mrežu pregledaju podatke u vidu običnog teksta. Formatiranje preko <code>http://localhost:8080/examples/jsp/security/protected/_vti_shm/j_security_check</code> prosleđuje sledeće nezaštićene osetljive rubrike: <code>j_password</code>		Ozbiljan	Isključiti HTTPS protokol na serveru. Promeniti „action“ URL na oznaci rubrike da koristi HTTPS protokol („https://...“) umesto samo HTTP protokol („http://...“). Sve osetljive podatke treba slati preko HTTPS umesto preko HTTP.
39.	TLS/SSL Server Supports Weak Cipher Algorithms (ssl-weak-ciphers)	172.23.202.124:443, 172.23.202.220:443 negotiated the SSL_DHE_RSA_WITH_DES_CBC_SHA cipher suite TLS/SSL server podržava šifre koje se zasnivaju na slabim algoritmima. To napadaču može omogućiti da pokrene napade preko posrednika i da pregleda ili čačka osetljive podatke. Uopšteno, sledeće šifre se smatraju slabim: Tzv. „null“ (nula) šifre, jer ne šifruju podatke. Eksportne šifre koje koriste dužine tajnih ključeva ograničene na 40 bitova. Na to najčešće ukazuje reč EXP/EXPORT u nazivu šifre.		Ozbiljan	Konfigurisati server tako da onemogući podršku za slabe šifre. Za Apache web servere sa mod_ssl, uključiti fajl Apache konfiguracije i izmeniti liniju <code>SSLCipherSuite</code> tako da u njoj piše: <code>SSLCipherSuite ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM</code>

		Zastareli algoritmi za šifrovanje čije se dužine tajnih ključeva po današnjim standardima smatraju kratkim, npr. DES ili RC4 sa 56-bitnim ključevima.			
40.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	TCP reset with incorrect sequence number triggered this fault on 172.23.202.124:3306 172.23.202.220:3306: Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hедера i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183 ⁵⁹⁴⁹ CERT TA04-111A ⁵⁹⁵⁰ CERT-VN: 415294 ⁵⁹⁵¹ CVE CVE-2004-0230 ⁵⁹⁵² MS: MS05-019 ⁵⁹⁵³ MS: MS06-064 ⁵⁹⁵⁴ NETBSD: NetBSD-SA2004-006 ⁵⁹⁵⁵ OSVDB 4030 ⁵⁹⁵⁶ OVAL: OVAL2689 ⁵⁹⁵⁷ OVAL: OVAL270 ⁵⁹⁵⁸ OVAL OVAL3508 ⁵⁹⁵⁹ OVAL OVAL4791 ⁵⁹⁶⁰ OVAL OVAL5711 ⁵⁹⁶¹ SECUNIA: 11440 ⁵⁹⁶² SECUNIA 11458 ⁵⁹⁶³ SECUNIA: 22341 ⁵⁹⁶⁴ SGI 20040403-01-A ⁵⁹⁶⁵ XF tcp-rst-dos(15886) ⁵⁹⁶⁶ URL1 ⁵⁹⁶⁷ URL2 ⁵⁹⁶⁸	Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC 2385 ⁵⁹⁶⁹ . Ono je napravljeno da smanji opasnost od određenih napada na BGP, kao što su TCP reseti.
41.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podesi na jedinstvenu vrednost i da se koristi u rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da fingerprint-uje operativni sistem.	BID 4314 ⁵⁹⁷⁰ CVE CVE-2002-0510 ⁵⁹⁷¹ XF linux-udp-fingerprint(8588) ⁵⁹⁷²	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili pak ranjivost koju treba popravljati, tako da ne postoje rešenja koja se mogu kupiti. Jedino se može postaviti fajervol ili neka druga sprava za filtriranje između napadnutog i neprijateljskog napada koji je u mogućnosti da randomizuje IP ID-jeve.
42.	Apache httpd mod_proxy_ftp globbing XSS (CVE-2008-2939) (apache-)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443	APPLE APPLE-SA-2009-05-12 ⁵⁹⁷³ BID 30560 ⁵⁹⁷⁴ CERT TA09-133A ⁵⁹⁷⁵	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.64 Ažurirati na Apache HTTPD version 2.0.64

⁵⁹⁴⁹ <http://www.securityfocus.com/bid/10183>⁵⁹⁵⁰ <http://www.us-cert.gov/ncas/alerts/ta04-111a>⁵⁹⁵¹ <http://www.kb.cert.org/vuls/id/415294>⁵⁹⁵² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁵⁹⁵³ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁵⁹⁵⁴ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁵⁹⁵⁵ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁵⁹⁵⁶ <http://www.osvdb.org/4030>⁵⁹⁵⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>⁵⁹⁵⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>⁵⁹⁵⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>⁵⁹⁶⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>⁵⁹⁶¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>⁵⁹⁶² <http://secunia.com/advisories/11440/>⁵⁹⁶³ <http://secunia.com/advisories/11458/>⁵⁹⁶⁴ <http://secunia.com/advisories/22341/>⁵⁹⁶⁵ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>⁵⁹⁶⁶ <http://xforce.iss.net/xforce/xfdb/15886>⁵⁹⁶⁷ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁵⁹⁶⁸ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>⁵⁹⁶⁹ <http://www.ietf.org/rfc/rfc2385.txt>⁵⁹⁷⁰ <http://www.securityfocus.com/bid/4314>⁵⁹⁷¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>⁵⁹⁷² <http://xforce.iss.net/xforce/xfdb/8588>⁵⁹⁷³ <http://lists.apple.com/archives/security-announce/2009/May/msg00001.html>⁵⁹⁷⁴ <http://www.securityfocus.com/bid/30560>⁵⁹⁷⁵ <http://www.us-cert.gov/ncas/alerts/TA09-133A>

	httpd-2_2_x-mod_proxy_ftpglobbing - xss-cve-2008-2939)	Skenirani sistem je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ftp. Pregledajte konfiguraciju vašeg web servera radi validacije. Propust je otkriven u modulu mod_proxy_ftp prilikom obrade "wildcard"-a ukoliko se on nađe na putanji FTP URL. Ukoliko je mod_proxy_ftp omogućen da podržava FTP-over-HTTP, zahtevi koji sadrže specijalne karaktere mogu da dovedu do cross-site scripting-a (XSS).	CERT-VN 663763 ⁵⁹⁷⁶ CVE CVE-2008-2939 ⁵⁹⁷⁷ OVAL OVAL11316 ⁵⁹⁷⁸ OVAL OVAL7716 ⁵⁹⁷⁹ REDHAT RHSA-2008:0966 ⁵⁹⁸⁰ REDHAT RHSA-2008:0967 ⁵⁹⁸¹ SECUNIA 31384 ⁵⁹⁸² SECUNIA 31673 ⁵⁹⁸³ SECUNIA 32685 ⁵⁹⁸⁴ SECUNIA 32838 ⁵⁹⁸⁵ SECUNIA 33156 ⁵⁹⁸⁶ SECUNIA 33797 ⁵⁹⁸⁷ SECUNIA 34219 ⁵⁹⁸⁸ SECUNIA 35074 ⁵⁹⁸⁹ XF apache-modproxyftp-xss(44223) ⁵⁹⁹⁰ URL1 ⁵⁹⁹¹		Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.10 Ažurirati na Apache HTTPD version 2.2.10 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.10.tar.gz
43.	Apache HTTPD: apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpdcve-2011-0419)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_autoindex. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_fnmatch() u sklopu APR biblioteke. Ako je omogućen mod_autoindex, a indeksi direktorijuma mod_autoindex su sadržavali fajlove sa dovoljno dugim nazivima, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do preterane upotrebe CPU-a. Ovo bi moglo da bude iskorišćeno u napadu odbijanja servisa. Zahvaljujući Maksymilian Arciemowicz prijavljen je ovaj propust.	CVE CVE-2011-0419 ⁵⁹⁹² DEBIAN DSA-2237 ⁵⁹⁹³ IAVM 2012-B-0056 ⁵⁹⁹⁴ OVAL OVAL14638 ⁵⁹⁹⁵ OVAL OVAL14804 ⁵⁹⁹⁶ REDHAT RHSA-2011:0896 ⁵⁹⁹⁷ REDHAT RHSA-2011:0897 ⁵⁹⁹⁸ REDHAT RHSA-2011:0507 ⁵⁹⁹⁹ SECUNIA 44490 ⁶⁰⁰⁰ SECUNIA 44564 ⁶⁰⁰¹ SECUNIA 44574 ⁶⁰⁰² URL1 ⁶⁰⁰³	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.19 Ažurirati na Apache HTTPD version 2.2.19 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.19.tar.gz

⁵⁹⁷⁶ <http://www.kb.cert.org/vuls/id/663763>⁵⁹⁷⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-2939>⁵⁹⁷⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11316>⁵⁹⁷⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7716>⁵⁹⁸⁰ <http://rhn.redhat.com/errata/RHSA-2008-0966.html>⁵⁹⁸¹ <http://rhn.redhat.com/errata/RHSA-2008-0967.html>⁵⁹⁸² <http://secunia.com/advisories/31384/>⁵⁹⁸³ <http://secunia.com/advisories/31673/>⁵⁹⁸⁴ <http://secunia.com/advisories/32685/>⁵⁹⁸⁵ <http://secunia.com/advisories/32838/>⁵⁹⁸⁶ <http://secunia.com/advisories/33156/>⁵⁹⁸⁷ <http://secunia.com/advisories/33797/>⁵⁹⁸⁸ <http://secunia.com/advisories/34219/>⁵⁹⁸⁹ <http://secunia.com/advisories/35074/>⁵⁹⁹⁰ <http://xforce.iss.net/xforce/xfdb/44223>⁵⁹⁹¹ http://httpd.apache.org/security/vulnerabilities_22.html⁵⁹⁹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419>⁵⁹⁹³ <http://www.debian.org/security/2011/dsa-2237>⁵⁹⁹⁴ <http://iase.disa.mil/stigs/iavm-cve.html>⁵⁹⁹⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14638>⁵⁹⁹⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14804>⁵⁹⁹⁷ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁵⁹⁹⁸ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>⁵⁹⁹⁹ <http://rhn.redhat.com/errata/RHSA-2011-0507.html>⁶⁰⁰⁰ <http://secunia.com/advisories/44490/>⁶⁰⁰¹ <http://secunia.com/advisories/44564/>⁶⁰⁰² <http://secunia.com/advisories/44574/>⁶⁰⁰³ http://httpd.apache.org/security/vulnerabilities_22.html

44.	Apache HTTPD: APR-util heap underwrite (CVE-2009-0023) (apache-httpd-cve-2009-0023)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako napadač poseduje posebno kreiranu ključnu reč za pretraživanje one funkcije koja upravlja kompajliranjem formi zahteva pretrage. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u načinu na koji komplet APR-biblioteke kompajlira forme zahtevanih pretraživanja. Napadač bi mogao da kreira posebno izrađenu ključnu reč pretraživanja, koja bi se proizvoljnim prepisivanjem gomilala u memoriji prilikom obrađivanja zahteva za pretragu.	BID 35221 ⁶⁰⁰⁴ CVE CVE-2009-0023 ⁶⁰⁰⁵ DEBIAN DSA-1812 ⁶⁰⁰⁶ OVAL OVAL10968 ⁶⁰⁰⁷ OVAL OVAL12321 ⁶⁰⁰⁸ REDHAT RHSA-2009:1107 ⁶⁰⁰⁹ REDHAT RHSA-2009:1108 ⁶⁰¹⁰ SECUNIA 34724 ⁶⁰¹¹ SECUNIA 35284 ⁶⁰¹² SECUNIA 35360 ⁶⁰¹³ SECUNIA 35395 ⁶⁰¹⁴ SECUNIA 35444 ⁶⁰¹⁵ SECUNIA 35487 ⁶⁰¹⁶ SECUNIA 35565 ⁶⁰¹⁷ SECUNIA 35710 ⁶⁰¹⁸ SECUNIA 35797 ⁶⁰¹⁹ SECUNIA 35843 ⁶⁰²⁰ SECUNIA 37221 ⁶⁰²¹ XF apache-aprstrmatchprecompile-dos(50964) ⁶⁰²² URL1 ⁶⁰²³	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz
45.	Apache HTTPD: ETag Inode Information Leakage (CVE-2003-1418) (apache-httpd-cve-2003-1418)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 U određenim konfiguracijama, Apache HTTP server dozvoljava udaljenim napadačima da dobiju poverljive informacije preko (1) Etag heder-a, koji otkriva broj inoda ili (2) razdvajanje višedelnih MIME-a, koja ukazuje na ID child procesa (PID). Određene verzije Apache-a koriste zahtevani broj čvorova fajla da bi konstruisali 'Etag' heder za odgovor. Iako sama po sebi nije ranjivost, ova informacija olakšava sprovođenje određenih NFS napada. „Running vulnerable HTTP service: Apache 2.2.9. http://172.23.202.124/	BID 6939 ⁶⁰²⁴ BID 6943 ⁶⁰²⁵ CVE CVE-2003-1418 ⁶⁰²⁶ XF apache-mime-information-disclosure(11438) ⁶⁰²⁷	Ozbiljan	Onemogućiti Etag mehanizam tipa "inod-based" konfiguraciji Apache-a. Takođe, inod informacije je moguće ukloniti iz Etag heder-a tako što će se dodati direktiva u Apache konfiguraciju: <i>FileETag Mtime Size</i>

⁶⁰⁰⁴ <http://www.securityfocus.com/bid/35221>⁶⁰⁰⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-0023>⁶⁰⁰⁶ <http://lists.debian.org/debian-security-announce/2009/msg00124.html>⁶⁰⁰⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10968>⁶⁰⁰⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12321>⁶⁰⁰⁹ <http://rhn.redhat.com/errata/RHSA-2009-1107.html>⁶⁰¹⁰ <http://rhn.redhat.com/errata/RHSA-2009-1108.html>⁶⁰¹¹ <http://secunia.com/advisories/34724/>⁶⁰¹² <http://secunia.com/advisories/35284/>⁶⁰¹³ <http://secunia.com/advisories/35360/>⁶⁰¹⁴ <http://secunia.com/advisories/35395/>⁶⁰¹⁵ <http://secunia.com/advisories/35444/>⁶⁰¹⁶ <http://secunia.com/advisories/35487/>⁶⁰¹⁷ <http://secunia.com/advisories/35565/>⁶⁰¹⁸ <http://secunia.com/advisories/35710/>⁶⁰¹⁹ <http://secunia.com/advisories/35797/>⁶⁰²⁰ <http://secunia.com/advisories/35843/>⁶⁰²¹ <http://secunia.com/advisories/37221/>⁶⁰²² <http://xforce.iss.net/xforce/xfdb/50964>⁶⁰²³ http://httpd.apache.org/security/vulnerabilities_22.html⁶⁰²⁴ <http://www.securityfocus.com/bid/6939>⁶⁰²⁵ <http://www.securityfocus.com/bid/6943>⁶⁰²⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-1418>⁶⁰²⁷ <http://xforce.iss.net/xforce/xfdb/11438>

		1: "3e008-d7-47c90fa668440""			
46.	Apache httpd Subrequest handling of request headers (mod_headers) (CVE- 2010-0434) (http- apacherequest- header-info-disclosure)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_headers. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust u jezgru "subrequest process code" može dovesti do greške tipa segmentation fault-a ili do otkrivanja podataka iz nekog drugog zahteva na thread-ovima servera, kao što su worker ili winnt MPM-ovi. Zahvaljujući Philip Pickett-u iz Vmware, ovaj propust je prijavljen i predložen je način ispravke.	BID 38494 ⁶⁰²⁸ CVE CVE-2010-0434 ⁶⁰²⁹ DEBIAN DSA-2035 ⁶⁰³⁰ OVAL OVAL10358 ⁶⁰³¹ OVAL OVAL8695 ⁶⁰³² REDHAT RHSA- 2010:0168 ⁶⁰³³ REDHAT RHSA- 2010:0175 ⁶⁰³⁴ SECUNIA 39100 ⁶⁰³⁵ SECUNIA 39115 ⁶⁰³⁶ SECUNIA 39501 ⁶⁰³⁷ SECUNIA 39628 ⁶⁰³⁸ SECUNIA 39632 ⁶⁰³⁹ SECUNIA 39656 ⁶⁰⁴⁰ SECUNIA 40096 ⁶⁰⁴¹ XF apache-http-rh-info- disclosure(56625) ⁶⁰⁴² URL1 ⁶⁰⁴³	Ozbiljan	Mnoge platforme i mnogi distributeri daju unapred formirane binarne pakete za Apache. Ovi unapred formirani paketi su najčešće standardizovani i optimizirani za određenu distribuciju, pa se zato savetuje korišćenje paketa predefinisanih za određeni OS, ukoliko su dostupni. Apache HTTPD >= 2.2 and < 2.2.15 Ažurirati na Apache HTTPD version 2.2.15 Uraditi download a zatim instalirati: http://archive.apache.org/dis t/httpd/httpd-2.2.15.tar.gz Apache HTTPD >= 2.0 and < 2.0.64 Ažurirati na Apache HTTPD version 2.0.64 Uraditi download a zatim instalirati: http://archive.apache.org/dis t/httpd/httpd-2.0.64.tar.gz
47.	Apache Tomcat v4.x Example Scripts Information Leakage (http-tomcat-0005)	172.23.202.124:8080 172.23.202.220:8080 Sledeće skripte su navedene kao primeri koji dolaze sa Apache Tomcat-om v4.x, a koje napadači mogu da iskoriste da dobiju informacije o sistemu. Poznato je da su ove skripte ranjive na napad tipa "cross site scripting" (XSS): /examples/jsp/num/numguess.jsp /examples/jsp/dates/date.jsp /examples/jsp/snp/snoop.jsp /examples/jsp/error/error.html /examples/jsp/sessions/carts.html /examples/jsp/checkbox/check.html /examples/jsp/colors/colors.html /examples/jsp/cal/login.html /examples/jsp/include/include.jsp /examples/jsp/forward/forward.jsp /examples/jsp/plugin/plugin.jsp /examples/jsp/jsptoserv/jsptoservlet.js p /examples/jsp/simpletag/foo.jsp		Kritičan	U potpunosti obrisati ove skripte. Primeri skripta nikad ne treba da budu instalirani na serverima koji su u produkciji.

⁶⁰²⁸ <http://www.securityfocus.com/bid/38494>⁶⁰²⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0434>⁶⁰³⁰ <http://www.debian.org/security/2010/dsa-2035>⁶⁰³¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10358>⁶⁰³² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8695>⁶⁰³³ <http://rhn.redhat.com/errata/RHSA-2010-0168.html>⁶⁰³⁴ <http://rhn.redhat.com/errata/RHSA-2010-0175.html>⁶⁰³⁵ <http://secunia.com/advisories/39100/>⁶⁰³⁶ <http://secunia.com/advisories/39115/>⁶⁰³⁷ <http://secunia.com/advisories/39501/>⁶⁰³⁸ <http://secunia.com/advisories/39628/>⁶⁰³⁹ <http://secunia.com/advisories/39632/>⁶⁰⁴⁰ <http://secunia.com/advisories/39656/>⁶⁰⁴¹ <http://secunia.com/advisories/40096/>⁶⁰⁴² <http://xforce.iss.net/xforce/xfdb/56625>⁶⁰⁴³ http://httpd.apache.org/security/vulnerabilities_22.html

		/examples/jsp/mail/sendmail.jsp /examples/servlet/HelloWorldExample /examples/servlet/RequestInfoExample /examples/servlet/RequestHeaderExample /examples/servlet/RequestParamExample /examples/servlet/CookieExample /examples/servlet/IndiServlet /examples/servlet/SessionExample /tomcat-docs/appdev/sample/web/hello.jsp			
48.	OpenSSH CBC Mode Information Disclosure Vulnerability (ssh-openssh-cbc-mode-info-disclosure)	172.23.202.124:22 172.23.202.220:22 Određene verzije OpenSSH-a poseduju ranjivu implementaciju bloka šifarskog algoritma u CBC modu (Cipher Block Chaining). Ovo bi udaljenom napadaču moglo omogućiti da preko nepoznatih vektora pridobije određene podatke u vidu običnog teksta iz proizvoljnog bloka šifrovanog teksta u SSH sesiji.	BID 32319 ⁶⁰⁴⁴ CVE CVE-2008-5161 ⁶⁰⁴⁵ SECUNIA 32760 ⁶⁰⁴⁶ URL1 ⁶⁰⁴⁷ URL2 ⁶⁰⁴⁸	Ozbiljan	Uraditi download a zatim instalirati: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-5.2p1.tar.gz OpenSSH verzija 5.2 je puštena u promet 22. februara 2009.
49.	Self-signed TLS/SSL certificate (ssl-self-signed-certificate)	172.23.202.124:443 172.23.202.220:443 TLS/SSL-a sertifikat servera je samopotpisan. Samopotpisani sertifikati po defaultu nisu od poverenja, naročito zato što napadi na TLS/SSL preko posrednika obično koriste samopotpisane sertifikate da prisluškuju TLS/SSL veze.		Ozbiljan	Nabaviti novi TLS/SSL serverov sertifikat koji NIJE samopotpisan i instalirati ga na server. Precizna uputstva za dobijanje novog sertifikata zavise od zahteva organizacije. Uopšteno, treba napraviti zahtev za sertifikat i taj zahtev sačuvati kao fajl. Ovaj fajl se zatim šalje Certificate Authority-ju (CA) na obradu. Organizacija možda poseduje sopstveni interni Certificate Authority. U suprotnom, potrebno je platiti sertifikat iz spoljnog poverljivog Certificate Authority-ja, kao što su Thawte, Verisign.
50.	Autocomplete enabled for sensitive HTML form fields (spider-sensitive-form-data-autocomplete-enabled)	172.23.202.124:8080 172.23.202.220:8080 Web forma sadrži lozinke i druge rubrike sa osetljivim tekstom za koje je otvorena mogućnost auto-complete od strane web pretraživača. Funkcija auto-complete skladišti forme popunjenih rubrika i lozinke lokalno, na web pretraživaču, tako da se ove rubrike automatski popunjavaju kada korisnik ponovo poseti sajt. Osetljivi podaci i lozinke mogu biti ukradeni ako je korisnikov sistem kompromitovan. Međutim, treba imati u vidu da forma auto-complete nije standardna i da je		Umeren	Za svaku osetljivu rubriku u HTML, stavku „autocomplete“ potrebno je podesiti na „off“. Na primer: <input type=“password“ autocomplete=“off“ name=“pw“> Ako ima previše rubrika, možda je brže podesiti stavku „autocomplete“ na „off“ u spoljnom tagu <form>. Na primer: <form action=“/login.jsp“ autocomplete=“off“ name=“pw“> <input type=“password“

⁶⁰⁴⁴ <http://www.securityfocus.com/bid/32319>⁶⁰⁴⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-5161>⁶⁰⁴⁶ <http://secunia.com/advisories/32760/>⁶⁰⁴⁷ http://www.cpni.gov.uk/Docs/Vulnerability_Advisory_SSH.txt, pristupljeno 20.12.2011⁶⁰⁴⁸ <http://www.openssh.com/txt/cbc.adv>

		to karakteristika web pretraživača koju svaki web pretraživač tretira na različit način. Na primer Opera zanemaruje ovu opciju i zahteva od korisnika da unese poverljive podatke svaki put kada posećuje određeni web sajt.			name="pw"></form>
51.	Apache Tomcat default installation/welcome page installed (http-tomcat-default-install-page)	172.23.202.124:8080 172.23.202.220:8080 Tomcat difoltna instalacija ili „Welcome“ stranica je instalirana na serveru. To obično ukazuje na novoinstalirani server. U mnogim slučajevima, Tomcat se instalira zajedno sa drugim aplikacijama i korisnik možda nije svestan da je web server pokrenut. Ovakvi serveri se retko patch-uju i još rede nadgledaju, što zlonamernim napadačima postaje pogodna meta koja najverovatnije neće pokrenuti nikakvo upozorenje.		Umeren	Ako se od servera zahteva da obezbedi neophodnu funkcionalnost, onda difoltnu stranicu treba zameniti odgovarajućim sadržajem. U suprotnom, ovakav server treba ukloniti sa mreže, prateći bezbednosni princip minimalne složenosti (više složenosti = manja bezbednost).
52.	Database Open Access (database-open-access)	172.23.202.124:3306 172.23.202.220:3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7.	URL1 ⁶⁰⁴⁹	Umeren	Konfigurisati server baze podataka tako da se dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.
53.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatišu slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	CVE CVE-1999-0524 ⁶⁰⁵⁰ OSVDB 95 ⁶⁰⁵¹ XF icmp-netmask(306) ⁶⁰⁵² XF icmp-timestamp(322) ⁶⁰⁵³	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
54.	WebDAV Extensions are Enabled (http-generic-webdav-enabled)	172.23.202.124:8080 172.23.202.220:8080 WebDAV je skup ekstenzija za HTTP protokol koji omogućava korisnicima da zajednički edituju i obrađuju fajlove na udaljenim web serverima.		Umeren	Apache: Potrebno je onemogućiti WebDAV (eng. Web-based Distributed Authoring and Versioning) za Apache. Proveriti da li je mod_dav modul isključen ili utvrditi

⁶⁰⁴⁹ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf⁶⁰⁵⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁶⁰⁵¹ <http://www.osvdb.org/95>⁶⁰⁵² <http://xforce.iss.net/xforce/xfdb/306>⁶⁰⁵³ <http://xforce.iss.net/xforce/xfdb/322>

		Mnogi web serveri po difoltu omogućavaju WebDAV ekstenzije, čak i kada nisu potrebne. S obzirom na dodatnu složenost, dosadašnja praksa je pokazala da treba onemogućiti WebDAV ukoliko se trenutno ne koristi.			da li postoji zahtevana autentifikacija na direktorijumima nad kojima se zahteva DAV. Apache Tomcat, Tomcat, Tomcat Web Server Onemogućiti WebDAV za Apache Tomcat. Isključiti WebDAV Servlet za sve web aplikacije koje se nalaze na web serveru. To se može uraditi tako što se ukloni definicija servlet-a za WebDAV (kategorija org.apache.catalina.servlets.WebdavServlet) i uklone sve servlet mape koje se pozivaju na WebDAV servlet.
55.	Apache HTTPD: CRLF injection in mod_negotiation when untrusted uploads are supported (CVE-2008-0456) (apache-httpd-cve-2008-0456)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_negotiation. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Moguće je ubaciti CRLF (Carriage Return and Line Feed) koji omogućava CRLF Injection napade (poznatih kao HTTP Response Splitting) za sajtove koji koriste mod_negotiation, omogućavajući neproverene aploudove na lokacije na kojima je omogućen MultiViews (višestruko pregledanje).	APPLE APPLE-SA-2009-05-12 ⁶⁰⁵⁴ BID 27409 ⁶⁰⁵⁵ CERT TA09-133A ⁶⁰⁵⁶ CVE CVE-2008-0456 ⁶⁰⁵⁷ REDHAT RHSA-2013:0130 ⁶⁰⁵⁸ SECUNIA 29348 ⁶⁰⁵⁹ SECUNIA 35074 ⁶⁰⁶⁰ XF 39893 ⁶⁰⁶¹ URL1 ⁶⁰⁶²	Umeren	Apache HTTPD >= 2.2 and < 2.2.12 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz
56.	Apache HTTPD: XSS in mod_negotiation when untrusted uploads are supported (CVE-2012-2687) (apachehttpd-cve-2012-2687)	172.23.202.124:80 172.23.202.124:443 172.23.202.220:80 172.23.202.220:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_negotiation. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Mogući XSS napadi za sajtove koji koriste mod_negotiation, omogućavajući neproverene	APPLE APPLE-SA-2013-09-12-1 ⁶⁰⁶³ BID 55131 ⁶⁰⁶⁴ CVE CVE-2012-2687 ⁶⁰⁶⁵ IAVM 2012-A-0139 ⁶⁰⁶⁶ REDHAT RHSA-2012:1591 ⁶⁰⁶⁷ REDHAT RHSA-2012:1592 ⁶⁰⁶⁸ REDHAT RHSA-2012:1594 ⁶⁰⁶⁹ REDHAT RHSA-2013:0130 ⁶⁰⁷⁰	Umeren	Apache HTTPD >= 2.2 and < 2.2.23 Ažurirati na Apache HTTPD version 2.2.23 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz Apache HTTPD >= 2.4 and < 2.4.3 Ažurirati na Apache HTTPD version 2.4.3 Uradi download a zatim

⁶⁰⁵⁴ <http://lists.apple.com/archives/security-announce/2009/May/msg00001.html>⁶⁰⁵⁵ <http://www.securityfocus.com/bid/27409>⁶⁰⁵⁶ <http://www.us-cert.gov/ncas/alerts/ta09-133a>⁶⁰⁵⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0456>⁶⁰⁵⁸ <http://rhn.redhat.com/errata/RHSA-2013-0130.html>⁶⁰⁵⁹ <http://secunia.com/advisories/29348/>⁶⁰⁶⁰ <http://secunia.com/advisories/35074/>⁶⁰⁶¹ <http://xforce.iss.net/xforce/xfdb/39893>⁶⁰⁶² http://httpd.apache.org/security/vulnerabilities_22.html⁶⁰⁶³ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁶⁰⁶⁴ <http://www.securityfocus.com/bid/55131>⁶⁰⁶⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2687>⁶⁰⁶⁶ <http://iase.disa.mil/stigs/iavm-cve.html>⁶⁰⁶⁷ <http://rhn.redhat.com/errata/RHSA-2012-1591.html>⁶⁰⁶⁸ <http://rhn.redhat.com/errata/RHSA-2012-1592.html>⁶⁰⁶⁹ <http://rhn.redhat.com/errata/RHSA-2012-1594.html>

		aploudove na lokacije na kojima je omogućen MultiViews (višestruko pregledanje). Napomena: Ovaj problem je takođe poznat kao CVE-2008-0455.	SECUNIA 50894 ⁶⁰⁷¹ SECUNIA 51607 ⁶⁰⁷² URL1 ⁶⁰⁷³ URL2 ⁶⁰⁷⁴		instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.3.tar.gz
57.	Weak Cryptographic Key (weak-crypto-key)	172.23.202.124:443 172.23.202.220:443 Dužina RSA modula u sertifikatu X.509: 1024 bita (manje od 2047 bita). Dužina tajnog ključa koju koristi kriptografski algoritam određuje najviši mogući nivo bezbednosti. Nedavno otkriveni teoretski napadi i sve napredniji hardware stalno snižavaju nivo bezbednosti. Zbog ovoga, od 2011-te godine, vladine, akademske i privatne organizacije koje se bave kriptografskom bezbednošću, kao National Institute of Standards and Technology (NIST), European Network of Excellence in Cryptology II (ECRYPT II), daju sledeće preporuke da bi se obezbedila kratkoročna ili duža bezbednost čak i od najbolje opremljenih napadača (npr. agencije inteligencije): Dužine simetričnih tajnih ključeva od minimum 80-112 bitova. Dužine eliptičnih tajnih ključeva od minimum 160-224 bitova. Dužine RSA tajnih ključeva od minimum 1248-2048 bitova. CA/Browser Forum Extended Validation (EV) Guidelines izričito zahteva da dužina tajnog ključa bude minimum 2048 bitova. Ispitivanja pokazuju da je izrada 1024-bitnog RSA modula praktično dostupna. Dužine DSA tajnih ključeva od minimum 2048 bitova. Dodatno, od 2014-te, Certificate Authority/Browser Forum zahteva da SSL sertifikati i kôd potpisivanje više ne podržavaju 1024-bitne RSA tajne ključeve.	URL1 ⁶⁰⁷⁵ URL2 ⁶⁰⁷⁶ URL3 ⁶⁰⁷⁷ URL4 ⁶⁰⁷⁸ URL5 ⁶⁰⁷⁹ URL6 ⁶⁰⁸⁰ URL7 ⁶⁰⁸¹	Umeren	Slab tajni ključ se koristi u sertifikatu X.509 (npr. za HTTPS server), da generiše duži tajni ključ i osveži sertifikat. Pogledati NIST's preporuke za kriptografske algoritme i dužine tajnih ključeva . ⁶⁰⁸²
58.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada	URL1 ⁶⁰⁸³ URL2 ⁶⁰⁸⁴ URL3 ⁶⁰⁸⁵	Umeren	Onemogućavanje TCP timestamp odgovora na Linux OS. Podesiti net.ipv4.tcp_timestamps

⁶⁰⁷⁰ <http://rhn.redhat.com/errata/RHSA-2013-0130.html>⁶⁰⁷¹ <http://secunia.com/advisories/50894/>⁶⁰⁷² <http://secunia.com/advisories/51607/>⁶⁰⁷³ http://httpd.apache.org/security/vulnerabilities_22.html⁶⁰⁷⁴ http://httpd.apache.org/security/vulnerabilities_24.html⁶⁰⁷⁵ <http://www.symantec.com/page.jsp?id=1024-bit-certificate-support>⁶⁰⁷⁶ <http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf>⁶⁰⁷⁷ http://csrc.nist.gov/groups/ST/toolkit/key_management.html⁶⁰⁷⁸www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2011_2_AlgoKat.pdf⁶⁰⁷⁹⁶⁰⁷⁹ <http://www.ecrypt.eu.org/documents/D.SPA.17.pdf>⁶⁰⁸⁰ <http://www.keylength.com/>⁶⁰⁸¹ http://www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf⁶⁰⁸² <http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf>⁶⁰⁸³ http://www.forensicswiki.org/wiki/TCP_timestamps⁶⁰⁸⁴ <http://www.ietf.org/rfc/rfc1323.txt>⁶⁰⁸⁵ <http://uptime.netcraft.com/>

		udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.			vrednost na sledećem ključu na 0 pokretanjem sledeće komande: sysctl -w net.ipv4.tcp_timestamps=0 Dodatno, sledeću vrednost u difoltnom sysctl konfiguracionom fajlu, generally sysctl.conf: net.ipv4.tcp_timestamps=0

Tabela 125. Linux OS sa IP adresama 172.23.202.126, 172.23.202.225 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.126		OS: Red Hat Enterprise Linux 4.8 AS x64, rhel48asx64			56
IP adresa: 172.23.202.225		OS: Red Hat Enterprise Linux 4.8 AS x86, rhel48asx86			56
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Apache httpd APR apr_palloc heap overflow (CVE-2009-2412) (apache-httpd-cve-2009-2412)	172.23.202.126:80 172.23.202.225:80 U modulu apr_palloc() je pronađen propust u sklopu APR-a, koji može prouzrokovati velika preopterećenja u programima koji pokušaju da kontrolišu apr_palloc() veličinu zadate od strane korisnika. Sam Apache HTTP server ne dopušta prolaz ka ovoj funkciji neproverenim veličinama koje zadaje korisnik, tako da se on može pokrenuti samo preko neke druge aplikacije koja koristi apr_palloc() na ranjiv način.	APPLE APPLE-SA-2009-11-09 ⁶⁰⁸⁶ BID 35949 ⁶⁰⁸⁷ CVE CVE-2009-2412 ⁶⁰⁸⁸ OSVDB 56765 ⁶⁰⁸⁹ OSVDB 56766 ⁶⁰⁹⁰ OVAL OVAL8394 ⁶⁰⁹¹ OVAL OVAL9958 ⁶⁰⁹² SECUNIA 36138 ⁶⁰⁹³ SECUNIA 36140 ⁶⁰⁹⁴ SECUNIA 36166 ⁶⁰⁹⁵ SECUNIA 36233 ⁶⁰⁹⁶ SECUNIA 37152 ⁶⁰⁹⁷ SECUNIA 37221 ⁶⁰⁹⁸ SUSE-SA:2009:050 ⁶⁰⁹⁹ URL1 ⁶¹⁰⁰	Kritičan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.13 Ažurirati na Apache HTTPD version 2.2.13 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.13.tar.gz
2.	Apache httpd mod_isapi module unload flaw (CVE-2010-0425) (http-apache-mod_isapi-module-unload-flaw)	172.23.202.126:80 172.23.202.225:80 U modulu mod_isapi je pronađen propust koji će pokušati da ukloni ISAPI dll kada naiđe na greške. To može ostaviti povratne pozive u nedefinisanom stanju greške i kao posledica može da se javi	BID 38494 ⁶¹⁰¹ CERT-VN 280613 ⁶¹⁰² CVE CVE-2010-0425 ⁶¹⁰³ OVAL OVAL8439 ⁶¹⁰⁴ SECUNIA 38978 ⁶¹⁰⁵ SECUNIA 39628 ⁶¹⁰⁶ XF apache-http-modisapi-ocp-	Kritičan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz

⁶⁰⁸⁶ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>⁶⁰⁸⁷ <http://www.securityfocus.com/bid/35949>⁶⁰⁸⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2412>⁶⁰⁸⁹ <http://osvdb.org/56765>⁶⁰⁹⁰ <http://osvdb.org/56766>⁶⁰⁹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8394>⁶⁰⁹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9958>⁶⁰⁹³ <http://secunia.com/advisories/36138/>⁶⁰⁹⁴ <http://secunia.com/advisories/36140/>⁶⁰⁹⁵ <http://secunia.com/advisories/36166/>⁶⁰⁹⁶ <http://secunia.com/advisories/36233/>⁶⁰⁹⁷ <http://secunia.com/advisories/37152/>⁶⁰⁹⁸ <http://secunia.com/advisories/37221/>⁶⁰⁹⁹ <https://www.suse.com/support/security/advisories/>⁶¹⁰⁰ http://httpd.apache.org/security/vulnerabilities_20.html⁶¹⁰¹ <http://www.securityfocus.com/bid/38494>⁶¹⁰² <http://www.kb.cert.org/vuls/id/280613>⁶¹⁰³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0425>⁶¹⁰⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8439>⁶¹⁰⁵ <http://secunia.com/advisories/38978/>⁶¹⁰⁶ <http://secunia.com/advisories/39628/>

		segmentation fault. Na Windows platformama koje koriste mod_isapi, udaljeni napadač bi mogao da pošalje zlonameran zahtev da pokrene ovaj problem, a kako win32 MPM pokreće samo jedan proces, to bi kao ishod imalo odbijanje servisa i potencijalno dozvolilo da se pokrene proizvoljan kôd. Napomena: Zahvaljujući Brett Gervasoni-ju iz "Sense of Security" ovaj problem je prijavljen i za njega je predložena zakrpa.	unspecified(56624) ⁶¹⁰⁷ URL1 ⁶¹⁰⁸		
3.	Apache httpd SSLVerifyClient bypass (CVE-2005-2700) (httpd-mod_ssl-client-auth-bypass)	172.23.202.126:80 172.23.202.225:80 Otkriven je propust u modulu mod_ssl pri obradi direktive "SSLVerifyClient". Ovaj propust se javlja ukoliko virtuelan host uradio konfiguraciju koristeći "SSLVerifyClient optional", a zatim je direktiva "SSLVerifyClient required" podešena za specifičnu lokaciju. Kod servera konfigurisanih na ovaj način, zlonamerni napadač bi bio u mogućnosti da pristupi resursima koji bi inače bili zaštićeni tako što ne bi davao klijentov sertifikat prilikom uspostavljanja veze.	BID 14721 ⁶¹⁰⁹ CERT-VN 744929 ⁶¹¹⁰ CVE CVE-2005-2700 ⁶¹¹¹ OSVDB 19188 ⁶¹¹² DEBIAN DSA-805 ⁶¹¹³ DEBIAN DSA-807 ⁶¹¹⁴ OVAL OVAL10416 ⁶¹¹⁵ REDHAT RHSA-2005:608 ⁶¹¹⁶ REDHAT RHSA-2005:773 ⁶¹¹⁷ REDHAT RHSA-2005:816 ⁶¹¹⁸ SECUNIA 16700 ⁶¹¹⁹ SECUNIA 16705 ⁶¹²⁰ SECUNIA 16714 ⁶¹²¹ SECUNIA 16743 ⁶¹²² SECUNIA 16746 ⁶¹²³ SECUNIA 16748 ⁶¹²⁴ SECUNIA 16753 ⁶¹²⁵ SECUNIA 16754 ⁶¹²⁶ SECUNIA 16769 ⁶¹²⁷ SECUNIA 16771 ⁶¹²⁸ SECUNIA 16789 ⁶¹²⁹ SECUNIA 16864 ⁶¹³⁰ SECUNIA 16956 ⁶¹³¹ SECUNIA 17088 ⁶¹³² SECUNIA 17288 ⁶¹³³ SECUNIA 17311 ⁶¹³⁴ SECUNIA 17813 ⁶¹³⁵	Kritičan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.55.tar.gz

⁶¹⁰⁷ <http://xforce.iss.net/xforce/xfdb/56624>⁶¹⁰⁸ http://httpd.apache.org/security/vulnerabilities_20.html⁶¹⁰⁹ <http://www.securityfocus.com/bid/14721>⁶¹¹⁰ <http://www.kb.cert.org/vuls/id/744929>⁶¹¹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2700>⁶¹¹² <http://www.osvdb.org/19188>⁶¹¹³ <http://www.debian.org/security/2005/dsa-805>⁶¹¹⁴ <http://www.debian.org/security/2005/dsa-807>⁶¹¹⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10416>⁶¹¹⁶ <http://rhn.redhat.com/errata/RHSA-2005-608.html>⁶¹¹⁷ <http://rhn.redhat.com/errata/RHSA-2005-773.html>⁶¹¹⁸ <http://rhn.redhat.com/errata/RHSA-2005-816.html>⁶¹¹⁹ <http://secunia.com/advisories/16700/>⁶¹²⁰ <http://secunia.com/advisories/16705/>⁶¹²¹ <http://secunia.com/advisories/16714/>⁶¹²² <http://secunia.com/advisories/16743/>⁶¹²³ <http://secunia.com/advisories/16746/>⁶¹²⁴ <http://secunia.com/advisories/16748/>⁶¹²⁵ <http://secunia.com/advisories/16753/>⁶¹²⁶ <http://secunia.com/advisories/16754/>⁶¹²⁷ <http://secunia.com/advisories/16769/>⁶¹²⁸ <http://secunia.com/advisories/16771/>⁶¹²⁹ <http://secunia.com/advisories/16789/>⁶¹³⁰ <http://secunia.com/advisories/16864/>⁶¹³¹ <http://secunia.com/advisories/16956/>⁶¹³² <http://secunia.com/advisories/17088/>⁶¹³³ <http://secunia.com/advisories/17288/>⁶¹³⁴ <http://secunia.com/advisories/17311/>

			SECUNIA 19072 ⁶¹³⁶ SECUNIA 19073 ⁶¹³⁷ SECUNIA 21848 ⁶¹³⁸ SECUNIA 22523 ⁶¹³⁹ SUSE SA:2005:051 ⁶¹⁴⁰ SUSE SA:2005:052 ⁶¹⁴¹ SUSE SA:2006:051 ⁶¹⁴² SUSE SA:2006:051 ⁶¹⁴³ URL1 ⁶¹⁴⁴		
4.	Apache httpd mod_proxy_ftp FTP command injection (CVE-2009-3095) (apache-httpd- 2_0_xmod_proxy_ftp- ftp-command-injection- cve-2009-3095)	172.23.202.126:80 172.23.202.225:80 U modulu mod_proxy_ftp je pronađen propust. U reverznoj proxy konfiguraciji, udaljeni napadač bi mogao da iskoristi ovaj defekt da zaobiđe uobičajenu zabranu pristupa tako što bi kreirao pažljivo izrađen HTTP Authorization heder, koji omogućava napadaču da šalje proizvoljne komande FTP serveru.	APPLE APPLE-SA- 2010-03-29 ⁶¹⁴⁵ CVE CVE-2009-3095 ⁶¹⁴⁶ DEBIAN DSA-1934 ⁶¹⁴⁷ OVAL OVAL8662 ⁶¹⁴⁸ OVAL OVAL9363 ⁶¹⁴⁹ SECUNIA 37152 ⁶¹⁵⁰ SUSE SA:2009:050 ⁶¹⁵¹ URL1 ⁶¹⁵²	Kritičan	Apache >= 2.0 and < 2.1 Uradi download a zatim instalirati: http://archive.apache.org/dis t/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.0 and < 2.0.64 Ažurirati na Apache HTTPD version 2.0.64 Uradi download a zatim instalirati: <a href="http://archive.apache.org/dis
t/httpd/httpd-2.0.64.tar.gz">http://archive.apache.org/dis t/httpd/httpd-2.0.64.tar.gz
5.	Apache httpd mod_rewrite off-by-one error (CVE-2006-3747) (http-apache-mod- rewrite-bof)	172.23.202.126:80 172.23.202.225:80 Propust prepunjavanja bafera off-by- one je otkriven u modulu mod_rewrite. U zavisnosti od toga na koji je način kompajliran Apache httpd, ovaj propust softvera može dovesti do ranjivosti koja bi, u kombinaciji sa određenim tipovima pravila Rewrite-a u konfiguracionim fajlovima web servera, mogla biti aktivirana iz daleka. Posledice ove od ranjivosti bi mogle uključivati	APPLE APPLE-SA- 2008-03-18 ⁶¹⁵³ BID 19204 ⁶¹⁵⁴ CERT TA08-150A ⁶¹⁵⁵ CERT-VN 395412 ⁶¹⁵⁶ CVE CVE-2006-3747 ⁶¹⁵⁷ DEBIAN DSA-1131 ⁶¹⁵⁸ DEBIAN DSA-1132 ⁶¹⁵⁹ OSVDB 27588 ⁶¹⁶⁰ SECUNIA 21197 ⁶¹⁶¹ SECUNIA 21241 ⁶¹⁶² SECUNIA 21245 ⁶¹⁶³ SECUNIA 21247 ⁶¹⁶⁴ SECUNIA 21266 ⁶¹⁶⁵	Kritičan	Apache >= 2.0 and < 2.1 Uradi download a zatim instalirati: <a href="http://archive.apache.org/dis
t/httpd/httpd-2.0.59.tar.gz">http://archive.apache.org/dis t/httpd/httpd-2.0.59.tar.gz Apache HTTPD >= 1.3 and < 1.3.37 Ažurirati na Apache HTTPD version 1.3.37 Uradi download a zatim instalirati: <a href="http://archive.apache.org/dis
t/httpd/apache-1.3.37.tar.gz">http://archive.apache.org/dis t/httpd/apache-1.3.37.tar.gz

⁶¹³⁵ <http://secunia.com/advisories/17813/>⁶¹³⁶ <http://secunia.com/advisories/19072/>⁶¹³⁷ <http://secunia.com/advisories/19073/>⁶¹³⁸ <http://secunia.com/advisories/21848/>⁶¹³⁹ <http://secunia.com/advisories/22523/>⁶¹⁴⁰ <https://www.suse.com/support/security/advisories/>⁶¹⁴¹ <https://www.suse.com/support/security/advisories/>⁶¹⁴² <https://www.suse.com/support/security/advisories/>⁶¹⁴³ <https://www.suse.com/support/security/advisories/>⁶¹⁴⁴ http://httpd.apache.org/security/vulnerabilities_20.html⁶¹⁴⁵ <http://lists.apple.com/archives/security-announce/2010/Mar/msg00001.html>⁶¹⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3095>⁶¹⁴⁷ <http://www.debian.org/security/2009/dsa-1934>⁶¹⁴⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8662>⁶¹⁴⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9363>⁶¹⁵⁰ <http://secunia.com/advisories/37152/>⁶¹⁵¹ <https://www.suse.com/support/security/advisories/>⁶¹⁵² http://httpd.apache.org/security/vulnerabilities_20.html⁶¹⁵³ <http://lists.apple.com/archives/security-announce/2008/Mar/msg00000.html>⁶¹⁵⁴ <http://www.securityfocus.com/bid/19204>⁶¹⁵⁵ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>⁶¹⁵⁶ <http://www.kb.cert.org/vuls/id/395412>⁶¹⁵⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-3747>⁶¹⁵⁸ <http://lists.debian.org/debian-security-announce/2006/msg00219.html>⁶¹⁵⁹ <http://lists.debian.org/debian-security/2006/08/msg00000.html>⁶¹⁶⁰ <http://www.osvdb.org/27588>⁶¹⁶¹ <http://secunia.com/advisories/21197/>⁶¹⁶² <http://secunia.com/advisories/21241/>⁶¹⁶³ <http://secunia.com/advisories/21245/>⁶¹⁶⁴ <http://secunia.com/advisories/21247/>

		odbijanje servisa (obaranje procesa web servera) ili potencijalno omogućavanje pokretanja proizvoljnog kôda.	SECUNIA 21273 ⁶¹⁶⁶ SECUNIA 21284 ⁶¹⁶⁷ SECUNIA 21307 ⁶¹⁶⁸ SECUNIA 21313 ⁶¹⁶⁹ SECUNIA 21315 ⁶¹⁷⁰ SECUNIA 21346 ⁶¹⁷¹ SECUNIA 21478 ⁶¹⁷² SECUNIA 21509 ⁶¹⁷³ SECUNIA 22262 ⁶¹⁷⁴ SECUNIA 22368 ⁶¹⁷⁵ SECUNIA 22388 ⁶¹⁷⁶ SECUNIA 22523 ⁶¹⁷⁷ SECUNIA 23028 ⁶¹⁷⁸ SECUNIA 23260 ⁶¹⁷⁹ SECUNIA 26329 ⁶¹⁸⁰ SECUNIA 29420 ⁶¹⁸¹ SECUNIA 29849 ⁶¹⁸² SECUNIA 30430 ⁶¹⁸³ SUSE SA:2006:043 ⁶¹⁸⁴ XF apache-modrewrite-offbyone-bo(28063) ⁶¹⁸⁵ URL1 ⁶¹⁸⁶		
6.	Apache httpd SSLCipherSuite bypass (CVE-2004-0885) (http://apache2-mod-ssl-ciphersuite-bypass)	172.23.202.126:80 172.23.202.225:80 Problem je otkriven u modulu mod_ssl ukoliko je konfigurisan tako da koristi „SSLCipherSuite“ direktivu u kontekstu direktorijuma ili lokacije. Ako je određena lokacija konfigurisana tako da zahteva određene skupove šifara, onda će klijent biti u mogućnosti da pristupi toj lokaciji koristeći bilo koji skup šifara koji dozvoljava virtuelna konfiguracija host-a.	BID 11360 ⁶¹⁸⁷ CVE CVE-2004-0885 ⁶¹⁸⁸ OVAL OVAL10384 ⁶¹⁸⁹ REDHAT RHSA-2004:562 ⁶¹⁹⁰ REDHAT RHSA-2004:600 ⁶¹⁹¹ REDHAT RHSA-2005:816 ⁶¹⁹² REDHAT RHSA-2008:0261 ⁶¹⁹³ SECUNIA 19072 ⁶¹⁹⁴ XF apache-sslciphersuite-restriction-bypass(17671) ⁶¹⁹⁵ URL1 ⁶¹⁹⁶	Kritičan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.53.tar.gz

⁶¹⁶⁵ <http://secunia.com/advisories/21266/>⁶¹⁶⁶ <http://secunia.com/advisories/21273/>⁶¹⁶⁷ <http://secunia.com/advisories/21284/>⁶¹⁶⁸ <http://secunia.com/advisories/21307/>⁶¹⁶⁹ <http://secunia.com/advisories/21313/>⁶¹⁷⁰ <http://secunia.com/advisories/21315/>⁶¹⁷¹ <http://secunia.com/advisories/21346/>⁶¹⁷² <http://secunia.com/advisories/21478/>⁶¹⁷³ <http://secunia.com/advisories/21509/>⁶¹⁷⁴ <http://secunia.com/advisories/22262/>⁶¹⁷⁵ <http://secunia.com/advisories/22368/>⁶¹⁷⁶ <http://secunia.com/advisories/22388/>⁶¹⁷⁷ <http://secunia.com/advisories/22523/>⁶¹⁷⁸ <http://secunia.com/advisories/23028/>⁶¹⁷⁹ <http://secunia.com/advisories/23260/>⁶¹⁸⁰ <http://secunia.com/advisories/26329/>⁶¹⁸¹ <http://secunia.com/advisories/29420/>⁶¹⁸² <http://secunia.com/advisories/29849/>⁶¹⁸³ <http://secunia.com/advisories/30430/>⁶¹⁸⁴ <https://www.suse.com/support/security/advisories/>⁶¹⁸⁵ <http://xforce.iss.net/xforce/xfdb/28063>⁶¹⁸⁶ http://httpd.apache.org/security/vulnerabilities_20.html⁶¹⁸⁷ <http://www.securityfocus.com/bid/11360>⁶¹⁸⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0885>⁶¹⁸⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10384>⁶¹⁹⁰ <http://rhn.redhat.com/errata/RHSA-2004-562.html>⁶¹⁹¹ <http://rhn.redhat.com/errata/RHSA-2004-600.html>⁶¹⁹² <http://rhn.redhat.com/errata/RHSA-2005-816.html>⁶¹⁹³ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>⁶¹⁹⁴ <http://secunia.com/advisories/19072/>⁶¹⁹⁵ <http://xforce.iss.net/xforce/xfdb/17671>

7.	Apache httpd PCRE overflow (CVE-2005-2491) (http-apache2-pcre-bof)	172.23.202.126:80 172.23.202.225:80 Ranjivost tipa "Integer Overflow" je otkriven u PCRE (Perl compatible regular expression) biblioteci uključenoj u httpd. Lokalni korisnik koji ima mogućnost da kreira .htaccess fajlove mogao bi da kreira zlonamerno izrađen regularan izraz tako da dobije privilegije nad child procesima httpd servisa.	BID 14620 ⁶¹⁹⁷ BID 15647 ⁶¹⁹⁸ CVE CVE-2005-2491 ⁶¹⁹⁹ DEBIAN DSA-800 ⁶²⁰⁰ DEBIAN DSA-817 ⁶²⁰¹ DEBIAN DSA-819 ⁶²⁰² DEBIAN DSA-821 ⁶²⁰³ OVAL OVAL11516 ⁶²⁰⁴ OVAL OVAL1496 ⁶²⁰⁵ OVAL OVAL1659 ⁶²⁰⁶ OVAL OVAL735 ⁶²⁰⁷ REDHAT RHSA-2005:358 ⁶²⁰⁸ REDHAT RHSA-2005:761 ⁶²⁰⁹ REDHAT RHSA-2006:0197 ⁶²¹⁰ SECUNIA 16502 ⁶²¹¹ SECUNIA 16679 ⁶²¹² SECUNIA 17252 ⁶²¹³ SECUNIA 17813 ⁶²¹⁴ SECUNIA 19072 ⁶²¹⁵ SECUNIA 19193 ⁶²¹⁶ SECUNIA 19532 ⁶²¹⁷ SECUNIA 21522 ⁶²¹⁸ SECUNIA 22691 ⁶²¹⁹ SECUNIA 22875 ⁶²²⁰ SGI 20060401-01-U ⁶²²¹ SUSE SUSE-SA:2005:048 ⁶²²² SUSE SUSE-SA:2005:049 ⁶²²³ SUSE SUSE-SA:2005:051 ⁶²²⁴ SUSE SUSE-SA:2005:052 ⁶²²⁵ URL1 ⁶²²⁶	Kritičan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.55.tar.gz

⁶¹⁹⁶ http://httpd.apache.org/security/vulnerabilities_20.html⁶¹⁹⁷ <http://www.securityfocus.com/bid/14620> pristupljeno 18.12.2011.⁶¹⁹⁸ <http://www.securityfocus.com/bid/15647> pristupljeno 18.12.2011.⁶¹⁹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2491>⁶²⁰⁰ <http://www.debian.org/security/DSA-/DSA-800> pristupljeno 18.12.2011.⁶²⁰¹ <http://www.debian.org/security/DSA-/DSA-817> pristupljeno 18.12.2011.⁶²⁰² <http://www.debian.org/security/DSA-/DSA-819> pristupljeno 18.12.2011.⁶²⁰³ <http://www.debian.org/security/DSA-/DSA-821> pristupljeno 18.12.2011.⁶²⁰⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11516>⁶²⁰⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1496>⁶²⁰⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1659>⁶²⁰⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:735>⁶²⁰⁸ <http://rhn.redhat.com/errata/RHSA-2005-358.html>⁶²⁰⁹ <http://rhn.redhat.com/errata/RHSA-2005-761.html>⁶²¹⁰ <http://rhn.redhat.com/errata/RHSA-2006-0197.html>⁶²¹¹ <http://secunia.com/advisories/16502/>⁶²¹² <http://secunia.com/advisories/16679/>⁶²¹³ <http://secunia.com/advisories/17252/>⁶²¹⁴ <http://secunia.com/advisories/17813/>⁶²¹⁵ <http://secunia.com/advisories/19072/>⁶²¹⁶ <http://secunia.com/advisories/19193/>⁶²¹⁷ <http://secunia.com/advisories/19532/>⁶²¹⁸ <http://secunia.com/advisories/21522/>⁶²¹⁹ <http://secunia.com/advisories/22691/>⁶²²⁰ <http://secunia.com/advisories/22875/>⁶²²¹ <ftp://patches.sgi.com/support/free/security/advisories/20060401-01-U> pristupljeno 18.12.2011⁶²²² <https://www.suse.com/support/security/advisories/>⁶²²³ <https://www.suse.com/support/security/advisories/>⁶²²⁴ <https://www.suse.com/support/security/advisories/>⁶²²⁵ <https://www.suse.com/support/security/advisories/>⁶²²⁶ http://httpd.apache.org/security/vulnerabilities_20.html

8.	OpenSSH X11 Cookie Local Authentication Bypass Vulnerability (openssh-x11-cookie-auth-bypass)	172.23.202.126:22 172.23.202.225:22 Pre verzije 4.7, OpenSSH nije adekvatno radio kada nepoverljivi kolačić (cookie) nije mogao biti kreiran. Umesto njega, koristi se poverljivi X11 kolačić. To omogućava napadačima da naruše ciljanu polisu i dobiju privilegije korisnika, što kao posledicu servis tretira klijenta X kao poverljivog.	CVE CVE-2007-4752 ⁶²²⁷ BID 25628 ⁶²²⁸ XF openssh-x11cookie-privilege-escalation(36637) ⁶²²⁹	Kritičan	Uraditi download a zatim instalirati: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-4.7p1.tar.gz Verzija 4.7 OpenSSH-a je puštena u promet 4. septembra 2007.
9.	OpenSSH GSSAPI Credentials Leak (ssh-openssh-gssapi-credentials-leak)	172.23.202.126:22 172.23.202.225:22 Određene verzije OpenSSH greškom prosleđuju Kerberos poverljive podatke udaljenom host-u čak i kada se korisnička autentifikacija proverava drugim mehanizmima. Tako ako korisnik ima konfigurisanu GSSAPI autentifikaciju sa omogućenom opcijom GSSAPIDelegateCredentials, udaljeni napadač bi verovatno mogao da dođe do korisnikovih poverljivih podataka.	CVE CVE-2005-2798 ⁶²³⁰ BID 14729 ⁶²³¹	Kritičan	Nadograditi na najnoviju verziju OpenSSH-a. Najnovija verzija OpenSSH-a je 5.2 (OpenBSD izvor) i 5.2p1 (prenosivi izvor).
10.	Apache HTTPD: mod_deflate DoS (CVE-2009-1891) (apache-httpd-cve-2009-1891)	172.23.202.126:80 172.23.202.225:80 Ranjivost na DOS napad otkrivena je u modulu mod_deflate. Ovaj modul nastavlja da kompresuje velike fajlove sve dok se kompresija ne završi, čak i kada je mrežna konekcija koja je zahtevala taj sadržaj prekinuta pre nego što je kompresija završena. To dovodi do toga da mod_deflate zauzima veliku količinu CPU-a ukoliko je mod_deflate bio omogućen za velike fajlove.	APPLE APPLE-SA-2009-11-09 ⁶²³² CVE CVE-2009-1891 ⁶²³³ DEBIAN DSA-1834 ⁶²³⁴ OSVDB 55782 ⁶²³⁵ OVAL OVAL8632 ⁶²³⁶ OVAL OVAL9248 ⁶²³⁷ OVAL OVAL12361 ⁶²³⁸ REDHAT RHSA-2009-1148 ⁶²³⁹ REDHAT RHSA-2009-1156 ⁶²⁴⁰ SECUNIA 35721 ⁶²⁴¹ SECUNIA 35781 ⁶²⁴² SECUNIA 35793 ⁶²⁴³ SECUNIA 35865 ⁶²⁴⁴ SECUNIA 37152 ⁶²⁴⁵ SECUNIA 37221 ⁶²⁴⁶ SUSE SA:2009:050 ⁶²⁴⁷ URL ⁶²⁴⁸	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.12 Ažurirati na Apache HTTPD version 2.2.12 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

⁶²²⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-4752>⁶²²⁸ <http://www.securityfocus.com/bid/25628>⁶²²⁹ <http://xforce.iss.net/xforce/xfdb/36637>⁶²³⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2798>⁶²³¹ <http://www.securityfocus.com/bid/14729>⁶²³² <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>⁶²³³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1891>⁶²³⁴ <http://www.debian.org/security/DSA-/DSA-1834> pristupljeno 18.12.2011⁶²³⁵ <http://osvdb.org/55782>⁶²³⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8632>⁶²³⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9248>⁶²³⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12361>⁶²³⁹ <http://rhn.redhat.com/errata/RHSA-2009-1148.html>⁶²⁴⁰ <http://rhn.redhat.com/errata/RHSA-2009-1156.html>⁶²⁴¹ <http://secunia.com/advisories/35721/>⁶²⁴² <http://secunia.com/advisories/35781/>⁶²⁴³ <http://secunia.com/advisories/35793/>⁶²⁴⁴ <http://secunia.com/advisories/35865/>⁶²⁴⁵ <http://secunia.com/advisories/37152/>⁶²⁴⁶ <http://secunia.com/advisories/37221/>⁶²⁴⁷ <https://www.suse.com/support/security/advisories/>⁶²⁴⁸ http://httpd.apache.org/security/vulnerabilities_20.html

11.	OpenSSH X11 Forwarding Information Disclosure Vulnerability (ssh-openssh-x11-fowarding-infodisclosure)	172.23.202.126:22 172.23.202.225:22 Određene verzije OpenSSH-a ne povezuju ispravno TCP portove na lokalnom IPv6 interfejsu ako se koriste zahtevani IPv4 portovi. Ovo bi loklanom napadaču moglo da omogući da preuzme prosleđenu X11 sesiju putem otvaranja TCP port-a 6010 (IPv4).	BID 28444 ⁶²⁴⁹ CVE CVE-2008-1483 ⁶²⁵⁰ SECUNIA 29522 ⁶²⁵¹ URL1 ⁶²⁵²	Ozbiljan	Nadograditi na najnoviju verziju OpenSSH-a. Najnovija verzija OpenSSH-a je 5.2 (OpenBSD izvor) i 5.2p1 (prenosivi izvor).
12.	Apache HTTPD: expat DoS (CVE-2009-3560) (apache-httpd-cve-2009-3560)	172.23.202.126:80 172.23.202.225:80 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepoverljivi XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	BID 37203 ⁶²⁵³ CVE CVE-2009-3560 ⁶²⁵⁴ DEBIAN DSA-1953 ⁶²⁵⁵ IAVM 2012-A-0020 ⁶²⁵⁶ OVAL OVAL12942 ⁶²⁵⁷ REDHAT RHSA-2011:0896 ⁶²⁵⁸ OVAL OVAL10613 ⁶²⁵⁹ OVAL OVAL6883 ⁶²⁶⁰ SECUNIA 37537 ⁶²⁶¹ SECUNIA 38231 ⁶²⁶² SECUNIA 38794 ⁶²⁶³ SECUNIA 38832 ⁶²⁶⁴ SECUNIA 38834 ⁶²⁶⁵ SECUNIA 39478 ⁶²⁶⁶ SECUNIA 41701 ⁶²⁶⁷ SECUNIA 43300 ⁶²⁶⁸ URL1 ⁶²⁶⁹	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.17 Ažurirati na Apache HTTPD version 2.2.17 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
13.	Apache HTTPD: expat DoS (CVE-2009-3720) (apache-httpd-cve-2009-3720)	172.23.202.126:80 172.23.202.225:80 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer	IAVM 2012-A-0020 ⁶²⁷⁰ OVAL OVAL12719 ⁶²⁷¹ REDHAT RHSA-2011:0896 ⁶²⁷² CVE CVE-2009-3720 ⁶²⁷³ OVAL OVAL11019 ⁶²⁷⁴ OVAL OVAL7112 ⁶²⁷⁵ REDHAT RHSA-2010:0002 ⁶²⁷⁶	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.17 Ažurirati na Apache HTTPD version 2.2.17 Uraditi download a zatim

⁶²⁴⁹ <http://www.securityfocus.com/bid/28444>⁶²⁵⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-1483>⁶²⁵¹ <http://secunia.com/advisories/29522/>⁶²⁵² <http://www.openssh.org/txt/release-5.0>⁶²⁵³ <http://www.securityfocus.com/bid/37203>⁶²⁵⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3560>⁶²⁵⁵ <http://www.debian.org/security/DSA-/DSA-1953> pristupljeno dana 18.12.2011⁶²⁵⁶ <http://iase.disa.mil/stigs/iavm-cve.html>⁶²⁵⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12942>⁶²⁵⁸ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁶²⁵⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10613>⁶²⁶⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6883>⁶²⁶¹ <http://secunia.com/advisories/37537/>⁶²⁶² <http://secunia.com/advisories/38231/>⁶²⁶³ <http://secunia.com/advisories/38794/>⁶²⁶⁴ <http://secunia.com/advisories/38832/>⁶²⁶⁵ <http://secunia.com/advisories/38834/>⁶²⁶⁶ <http://secunia.com/advisories/39478/>⁶²⁶⁷ <http://secunia.com/advisories/41701/>⁶²⁶⁸ <http://secunia.com/advisories/43300/>⁶²⁶⁹ http://httpd.apache.org/security/vulnerabilities_20.html⁶²⁷⁰ <http://iase.disa.mil/stigs/iavm-cve.html>⁶²⁷¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12719>⁶²⁷² <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁶²⁷³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3720>⁶²⁷⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11019>⁶²⁷⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7112>⁶²⁷⁶ <http://rhn.redhat.com/errata/RHSA-2010-0002.html>

		over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepoverljivi XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	SECUNIA 37324 ⁶²⁷⁷ SECUNIA 37537 ⁶²⁷⁸ SECUNIA 37925 ⁶²⁷⁹ SECUNIA 38050 ⁶²⁸⁰ SECUNIA 38231 ⁶²⁸¹ SECUNIA 38794 ⁶²⁸² SECUNIA 38832 ⁶²⁸³ SECUNIA 38834 ⁶²⁸⁴ SECUNIA 39478 ⁶²⁸⁵ SECUNIA 41701 ⁶²⁸⁶ SECUNIA 43300 ⁶²⁸⁷ URL1 ⁶²⁸⁸		instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
14.	Apache HTTPD: mod_dav DoS (CVE-2010-1452) (apache-httpd-cve-2010-1452)	172.23.202.126:80 172.23.202.225:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako web server izvršava jedan od sledećih modula: mod_cache, mod_dav. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u obradi zahteva od strane mod_cache i mod_dav. Zlonameran napadač bi mogao da pošalje pažljivo izrađen zahtev i prouzrokuje da httpd child proces krahira. Ovakvo krahiranje bi se manifestovalo samo kao odbijanje servisa ako se koristi Worker MPM. Ovaj problem se dalje može ublažiti ako na mod_dav samo utiču zahtevi za koje postoji mogućnost autentifikovanja, a mod_cache je pod uticajem samo ako se koristi neuobičajena „CacheIgnoreURLSessionIdentifiers“ direktiva, uvedena u verziji 2.2.14. Ovaj problem je prijavio Mark Drayton.	IAVM 2012-B-0056 ⁶²⁸⁹ OVAL OVAL12341 ⁶²⁹⁰ REDHAT RHSA-2011:0896 ⁶²⁹¹ REDHAT RHSA-2011:0897 ⁶²⁹² APPLE APPLE-SA-2011-03-21 ⁶²⁹³ CVE CVE-2010-1452 ⁶²⁹⁴ OVAL OVAL11683 ⁶²⁹⁵ REDHAT RHSA-2010:0659 ⁶²⁹⁶ SECUNIA 42367 ⁶²⁹⁷ URL1 ⁶²⁹⁸	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.16 Ažurirati na Apache HTTPD version 2.2.16 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.16.tar.gz
15.	Apache HTTPD: apr_bridage_split_line DoS (CVE-2010-1623) (apache-httpd-cve-2010-1623)	172.23.202.126:80 172.23.202.225:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako Apache	IAVM 2012-B-0056 ⁶²⁹⁹ OVAL OVAL12800 ⁶³⁰⁰ REDHAT RHSA-2011:0896 ⁶³⁰¹ REDHAT RHSA-	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz

⁶²⁷⁷ <http://secunia.com/advisories/37324/>
⁶²⁷⁸ <http://secunia.com/advisories/37537/>
⁶²⁷⁹ <http://secunia.com/advisories/37925/>
⁶²⁸⁰ <http://secunia.com/advisories/38050/>
⁶²⁸¹ <http://secunia.com/advisories/38231/>
⁶²⁸² <http://secunia.com/advisories/38794/>
⁶²⁸³ <http://secunia.com/advisories/38832/>
⁶²⁸⁴ <http://secunia.com/advisories/38834/>
⁶²⁸⁵ <http://secunia.com/advisories/39478/>
⁶²⁸⁶ <http://secunia.com/advisories/41701/>
⁶²⁸⁷ <http://secunia.com/advisories/43300/>
⁶²⁸⁸ http://httpd.apache.org/security/vulnerabilities_20.html
⁶²⁸⁹ <http://iase.disa.mil/stigs/iavm-cve.html>
⁶²⁹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12341>
⁶²⁹¹ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>
⁶²⁹² <http://rhn.redhat.com/errata/RHSA-2011-0897.html>
⁶²⁹³ <http://lists.apple.com/archives/security-announce/2011/Mar/msg00006.html>
⁶²⁹⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1452>
⁶²⁹⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11683>
⁶²⁹⁶ <http://rhn.redhat.com/errata/RHSA-2010-0659.html>
⁶²⁹⁷ <http://secunia.com/advisories/42367/>
⁶²⁹⁸ http://httpd.apache.org/security/vulnerabilities_20.html
⁶²⁹⁹ <http://iase.disa.mil/stigs/iavm-cve.html>
⁶³⁰⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12800>
⁶³⁰¹ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>

		procesira ne-SSL zahteve. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji <code>apr_brigade_split_line()</code> u sklopu kompleta APR-util library, koji se koristi za procesiranje ne-SSL zahteva. Udaljeni napadač bi mogao da šalje zahteve, pažljivo izrađujući tajming za pojedinačne bajtove, što bi polako zauzimalo memoriju i potencijalno dovelo do odbijanja servisa.	2011:0897 ⁶³⁰² BID 43673 ⁶³⁰³ CVE CVE-2010-1623 ⁶³⁰⁴ REDHAT RHSA-2010:0950 ⁶³⁰⁵ SECUNIA 41701 ⁶³⁰⁶ SECUNIA 42015 ⁶³⁰⁷ SECUNIA 42361 ⁶³⁰⁸ SECUNIA 42367 ⁶³⁰⁹ SECUNIA 42403 ⁶³¹⁰ SECUNIA 42537 ⁶³¹¹ SECUNIA 43211 ⁶³¹² SECUNIA 43285 ⁶³¹³ URL1 ⁶³¹⁴		Apache HTTPD >= 2.2 and < 2.2.17 Ažurirati na Apache HTTPD version 2.2.17 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
16.	Apache HTTPD: mod_cache proxy DoS (CVE-2007-1863) (apache-httpd-cve-2007-1863)	172.23.202.126:80 172.23.202.225:80 Propust je otkriven u modulu mod_cache. Na sajtovima na kojima je omogućeno keširanje, udaljeni napadač bi mogao da pošalje pažljivo izrađen zahtev koji bi doveo do toga da child proces Apache-a koji to obrađuje krahira. To može dovesti samo do odbijanja servisa ako se koristi threaded MPM.	BID 24649 ⁶³¹⁵ CERT TA08-150A ⁶³¹⁶ CVE CVE-2007-1863 ⁶³¹⁷ OSVDB 37079 ⁶³¹⁸ OVAL OVAL9824 ⁶³¹⁹ REDHAT RHSA-2007:0533 ⁶³²⁰ REDHAT RHSA-2007:0534 ⁶³²¹ REDHAT RHSA-2007:0556 ⁶³²² REDHAT RHSA-2007:0557 ⁶³²³ SECUNIA 25830 ⁶³²⁴ SECUNIA 25873 ⁶³²⁵ SECUNIA 25920 ⁶³²⁶ SECUNIA 26273 ⁶³²⁷ SECUNIA 26443 ⁶³²⁸ SECUNIA 26508 ⁶³²⁹ SECUNIA 26822 ⁶³³⁰ SECUNIA 26842 ⁶³³¹ SECUNIA 26993 ⁶³³²	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.61.tar.gz

⁶³⁰² <http://rhn.redhat.com/errata/RHSA-2011-0897.html>⁶³⁰³ <http://www.securityfocus.com/bid/43673>⁶³⁰⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1623>⁶³⁰⁵ <http://rhn.redhat.com/errata/RHSA-2010-0950.html>⁶³⁰⁶ <http://secunia.com/advisories/41701/>⁶³⁰⁷ <http://secunia.com/advisories/42015/>⁶³⁰⁸ <http://secunia.com/advisories/42361/>⁶³⁰⁹ <http://secunia.com/advisories/42367/>⁶³¹⁰ <http://secunia.com/advisories/42403/>⁶³¹¹ <http://secunia.com/advisories/42537/>⁶³¹² <http://secunia.com/advisories/43211/>⁶³¹³ <http://secunia.com/advisories/43285/>⁶³¹⁴ http://httpd.apache.org/security/vulnerabilities_20.html⁶³¹⁵ <http://www.securityfocus.com/bid/24649>⁶³¹⁶ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>⁶³¹⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-1863>⁶³¹⁸ <http://www.osvdb.org/37079>⁶³¹⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9824>⁶³²⁰ <http://rhn.redhat.com/errata/RHSA-2007-0533.html>⁶³²¹ <http://rhn.redhat.com/errata/RHSA-2007-0534.html>⁶³²² <http://rhn.redhat.com/errata/RHSA-2007-0556.html>⁶³²³ <http://rhn.redhat.com/errata/RHSA-2007-0557.html>⁶³²⁴ <http://secunia.com/advisories/25830/>⁶³²⁵ <http://secunia.com/advisories/25873/>⁶³²⁶ <http://secunia.com/advisories/25920/>⁶³²⁷ <http://secunia.com/advisories/26273/>⁶³²⁸ <http://secunia.com/advisories/26443/>⁶³²⁹ <http://secunia.com/advisories/26508/>⁶³³⁰ <http://secunia.com/advisories/26822/>⁶³³¹ <http://secunia.com/advisories/26842/>⁶³³² <http://secunia.com/advisories/26993/>

			SECUNIA 27037 ⁶³³³ SECUNIA 27563 ⁶³³⁴ SECUNIA 27732 ⁶³³⁵ SECUNIA 28606 ⁶³³⁶ SECUNIA 30430 ⁶³³⁷ SUSE SUSE- SA:2007:061 ⁶³³⁸ URL1 ⁶³³⁹		
17.	Apache HTTPD: mod_proxy_ftp DoS (CVE-2009-3094) (apache-httpd-cve-2009-3094)	172.23.202.126:80 172.23.202.225:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ftp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust NULL pointer dereference (pointer sa NULL vrednošću upotrebljen kao da ukazuje na validnu memorijsku oblast) otkriven je u modulu mod_proxy_ftp. Zlonamerni FTP server, kojem su zahtevi proksirani, mogao bi da iskoristi ovaj propust u smislu obaranja http child procesa uz pomoć namerno izmenjenog odgovora EPSV ili PASV komandi, što bi dovelo do delimičnog odbijanja servisa.	CVE CVE-2009-3094 ⁶³⁴⁰ DEBIAN DSA-1934 ⁶³⁴¹ OVAL OVAL10981 ⁶³⁴² OVAL OVAL8087 ⁶³⁴³ SECUNIA 36549 ⁶³⁴⁴ SECUNIA 37152 ⁶³⁴⁵ SUSE SUSE- SA:2009:050 ⁶³⁴⁶ URL1 ⁶³⁴⁷	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.14 Ažurirati na Apache HTTPD version 2.2.14 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.gz
18.	Apache HTTPD: mod_proxy_http DoS (CVE-2008-2364) (apache-httpd-cve-2008-2364))	172.23.202.126:80 172.23.202.225:80 Otkriven je propust prilikom obrade prekomernih privremenih odgovora sa glavnog servera kada se koristi mod_proxy_http. Udaljeni napadač bi mogao da izazove odbijanje servisa ili preopterećenje memorije.	BID 29653 ⁶³⁴⁸ BID 31681 ⁶³⁴⁹ CVE CVE-2008-2364 ⁶³⁵⁰ OVAL OVAL11713 ⁶³⁵¹ OVAL OVAL6084 ⁶³⁵² OVAL OVAL9577 ⁶³⁵³ REDHAT RHSA- 2008:0966 ⁶³⁵⁴ REDHAT RHSA- 2008:0967 ⁶³⁵⁵ SECUNIA 30621 ⁶³⁵⁶ SECUNIA 31026 ⁶³⁵⁷ SECUNIA 31404 ⁶³⁵⁸ SECUNIA 31416 ⁶³⁵⁹ SECUNIA 31651 ⁶³⁶⁰	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.9 Ažurirati na Apache HTTPD version 2.2.9 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.9.tar.gz

⁶³³³ <http://secunia.com/advisories/27037/>⁶³³⁴ <http://secunia.com/advisories/27563/>⁶³³⁵ <http://secunia.com/advisories/27732/>⁶³³⁶ <http://secunia.com/advisories/28606/>⁶³³⁷ <http://secunia.com/advisories/30430/>⁶³³⁸ <https://www.suse.com/support/security/advisories/>⁶³³⁹ http://httpd.apache.org/security/vulnerabilities_20.html⁶³⁴⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3094>⁶³⁴¹ <http://www.debian.org/security/DSA-/DSA-1934> pristupljeno dana 18.12.2011⁶³⁴² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10981>⁶³⁴³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8087>⁶³⁴⁴ <http://secunia.com/advisories/36549/>⁶³⁴⁵ <http://secunia.com/advisories/37152/>⁶³⁴⁶ <https://www.suse.com/support/security/advisories/>⁶³⁴⁷ http://httpd.apache.org/security/vulnerabilities_20.html⁶³⁴⁸ <http://www.securityfocus.com/bid/29653>⁶³⁴⁹ <http://www.securityfocus.com/bid/31681>⁶³⁵⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-2364>⁶³⁵¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11713>⁶³⁵² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6084>⁶³⁵³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9577>⁶³⁵⁴ <http://rhn.redhat.com/errata/RHSA-2008-0966.html>⁶³⁵⁵ <http://rhn.redhat.com/errata/RHSA-2008-0967.html>⁶³⁵⁶ <http://secunia.com/advisories/30621/>⁶³⁵⁷ <http://secunia.com/advisories/31026/>⁶³⁵⁸ <http://secunia.com/advisories/31404/>⁶³⁵⁹ <http://secunia.com/advisories/31416/>⁶³⁶⁰ <http://secunia.com/advisories/31651/>

			SECUNIA 31904 ⁶³⁶¹ SECUNIA 32222 ⁶³⁶² SECUNIA 32685 ⁶³⁶³ SECUNIA 32838 ⁶³⁶⁴ SECUNIA 33156 ⁶³⁶⁵ SECUNIA 33797 ⁶³⁶⁶ SECUNIA 34219 ⁶³⁶⁷ SECUNIA 34259 ⁶³⁶⁸ SECUNIA 34418 ⁶³⁶⁹ XF apache-modproxy- module-dos(42987) ⁶³⁷⁰ URL1 ⁶³⁷¹		
19.	Apache httpd mod_ssl access control DoS (CVE-2005-3357) (apache-httpd-2_0_x- mod_ssl-access- controldos- cve-2005-3357)	172.23.202.126:80 172.23.202.225:80 Propust NULL pointer dereference (pointer sa NULL vrednošću upotrebljen kao da ukazuje na validnu memorijsku oblast) otkriven je u modulu mod_ssl, utičući na konfiguraciju servera kada je SSL virtuelan host konfigurisan sa kontrolisanim pristupom pogrešnim dokumentom 400. Zlonamerni napadač bi mogao da pošalje posebno kreiran zahtev i pokrene ovaj problem i mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	BID 16152 ⁶³⁷² CERT TA08-150A ⁶³⁷³ CVE CVE-2005-3357 ⁶³⁷⁴ OVAL OVAL11467 ⁶³⁷⁵ REDHAT RHSA- 2006:0159 ⁶³⁷⁶ SECUNIA 18307 ⁶³⁷⁷ SECUNIA 18333 ⁶³⁷⁸ SECUNIA 18339 ⁶³⁷⁹ SECUNIA 18340 ⁶³⁸⁰ SECUNIA 18429 ⁶³⁸¹ SECUNIA 18517 ⁶³⁸² SECUNIA 18585 ⁶³⁸³ SECUNIA 18743 ⁶³⁸⁴ SECUNIA 19012 ⁶³⁸⁵ SECUNIA 21848 ⁶³⁸⁶ SECUNIA 22233 ⁶³⁸⁷ SECUNIA 22368 ⁶³⁸⁸ SECUNIA 22523 ⁶³⁸⁹ SECUNIA 22669 ⁶³⁹⁰ SECUNIA 22992 ⁶³⁹¹ SECUNIA 23260 ⁶³⁹² SECUNIA 29849 ⁶³⁹³ SECUNIA 30430 ⁶³⁹⁴	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dis t/httpd/httpd-2.0.58.tar.gz Apache HTTPD >= 2.2 and < 2.2.2 Ažurirati na Apache HTTPD version 2.2.2 Uraditi download a zatim instalirati: http://archive.apache.org/dis t/httpd/httpd-2.2.2.tar.gz

⁶³⁶¹ <http://secunia.com/advisories/31904/>⁶³⁶² <http://secunia.com/advisories/32222/>⁶³⁶³ <http://secunia.com/advisories/32685/>⁶³⁶⁴ <http://secunia.com/advisories/32838/>⁶³⁶⁵ <http://secunia.com/advisories/33156/>⁶³⁶⁶ <http://secunia.com/advisories/33797/>⁶³⁶⁷ <http://secunia.com/advisories/34219/>⁶³⁶⁸ <http://secunia.com/advisories/34259/>⁶³⁶⁹ <http://secunia.com/advisories/34418/>⁶³⁷⁰ <http://xforce.iss.net/xforce/xfdb/42987>⁶³⁷¹ http://httpd.apache.org/security/vulnerabilities_20.html⁶³⁷² <http://www.securityfocus.com/bid/16152>⁶³⁷³ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>⁶³⁷⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-3357>⁶³⁷⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11467>⁶³⁷⁶ <http://rhn.redhat.com/errata/RHSA-2006-0159.html>⁶³⁷⁷ <http://secunia.com/advisories/18307/>⁶³⁷⁸ <http://secunia.com/advisories/18333/>⁶³⁷⁹ <http://secunia.com/advisories/18339/>⁶³⁸⁰ <http://secunia.com/advisories/18340/>⁶³⁸¹ <http://secunia.com/advisories/18429/>⁶³⁸² <http://secunia.com/advisories/18517/>⁶³⁸³ <http://secunia.com/advisories/18585/>⁶³⁸⁴ <http://secunia.com/advisories/18743/>⁶³⁸⁵ <http://secunia.com/advisories/19012/>⁶³⁸⁶ <http://secunia.com/advisories/21848/>⁶³⁸⁷ <http://secunia.com/advisories/22233/>⁶³⁸⁸ <http://secunia.com/advisories/22368/>⁶³⁸⁹ <http://secunia.com/advisories/22523/>⁶³⁹⁰ <http://secunia.com/advisories/22669/>⁶³⁹¹ <http://secunia.com/advisories/22992/>⁶³⁹² <http://secunia.com/advisories/23260/>⁶³⁹³ <http://secunia.com/advisories/29849/>⁶³⁹⁴ <http://secunia.com/advisories/30430/>

			SGI 20060101-01-U ⁶³⁹⁵ SUSE SUSE- SA:2006:051 ⁶³⁹⁶ SUSE SuSE- SA:2006:051 ⁶³⁹⁷ URL1 ⁶³⁹⁸		
20.	Apache HTTPD: Signals to arbitrary processes (CVE-2007-3304) (apache-httpd-cve-2007-3304)	172.23.202.126:80 172.23.202.225:80 Skenirani servis je osetljiv na ovu ranjivost samo ako lokalni napadač može da pokreće skripte na HTTP serveru. Pregledajte konfiguraciju vašeg web servera radi validacije. Pre nego što mu je poslao signale, Apache HTTP server nije overio da li proces potiče od Apache-ovog child procesa. Lokalni napadač koji ima mogućnost da pokreće skripte na HTTP serveru, mogao bi da manipuliše semaforom za signale i da prouzrokuje okončanje proizvoljnog procesa, što bi moglo da dovede do odbijanja servisa.	BID 24215 ⁶³⁹⁹ CVE CVE-2007-3304 ⁶⁴⁰⁰ OSVDB 38939 ⁶⁴⁰¹ OVAL OVAL11589 ⁶⁴⁰² REDHAT RHSA-2007:0532 ⁶⁴⁰³ REDHAT RHSA-2007:0556 ⁶⁴⁰⁴ REDHAT RHSA-2007:0557 ⁶⁴⁰⁵ REDHAT RHSA-2007:0662 ⁶⁴⁰⁶ REDHAT RHSA-2008:0261 ⁶⁴⁰⁷ SECUNIA 25827 ⁶⁴⁰⁸ SECUNIA 25830 ⁶⁴⁰⁹ SECUNIA 25920 ⁶⁴¹⁰ SECUNIA 26211 ⁶⁴¹¹ SECUNIA 26273 ⁶⁴¹² SECUNIA 26443 ⁶⁴¹³ SECUNIA 26508 ⁶⁴¹⁴ SECUNIA 26611 ⁶⁴¹⁵ SECUNIA 26759 ⁶⁴¹⁶ SECUNIA 26790 ⁶⁴¹⁷ SECUNIA 26822 ⁶⁴¹⁸ SECUNIA 26842 ⁶⁴¹⁹ SECUNIA 26993 ⁶⁴²⁰ SECUNIA 27121 ⁶⁴²¹ SECUNIA 27209 ⁶⁴²² SECUNIA 27563 ⁶⁴²³ SECUNIA 27732 ⁶⁴²⁴ SECUNIA 28212 ⁶⁴²⁵ SECUNIA 28224 ⁶⁴²⁶	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.61.tar.gz Apache HTTPD >= 1.3 and < 1.3.39 Ažurirati na Apache HTTPD version 1.3.39 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/apache-1.3.39.tar.gz Apache HTTPD >= 2.2 and < 2.2.6 Ažurirati na Apache HTTPD version 2.2.6 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz

⁶³⁹⁵ <ftp://patches.sgi.com/support/free/security/advisories/20060101-01-U> pristupljeno 18.12.2011⁶³⁹⁶ <https://www.suse.com/support/security/advisories/>⁶³⁹⁷ <https://www.suse.com/support/security/advisories/>⁶³⁹⁸ http://httpd.apache.org/security/vulnerabilities_20.html⁶³⁹⁹ <http://www.securityfocus.com/bid/24215>⁶⁴⁰⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3304>⁶⁴⁰¹ <http://www.osvdb.org/38939>⁶⁴⁰² <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval:def:11589>⁶⁴⁰³ <http://rhn.redhat.com/errata/RHSA-2007-0532.html>⁶⁴⁰⁴ <http://rhn.redhat.com/errata/RHSA-2007-0556.html>⁶⁴⁰⁵ <http://rhn.redhat.com/errata/RHSA-2007-0557.html>⁶⁴⁰⁶ <http://rhn.redhat.com/errata/RHSA-2007-0662.html>⁶⁴⁰⁷ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>⁶⁴⁰⁸ <http://secunia.com/advisories/25827/>⁶⁴⁰⁹ <http://secunia.com/advisories/25830/>⁶⁴¹⁰ <http://secunia.com/advisories/25920/>⁶⁴¹¹ <http://secunia.com/advisories/26211/>⁶⁴¹² <http://secunia.com/advisories/26273/>⁶⁴¹³ <http://secunia.com/advisories/26443/>⁶⁴¹⁴ <http://secunia.com/advisories/26508/>⁶⁴¹⁵ <http://secunia.com/advisories/26611/>⁶⁴¹⁶ <http://secunia.com/advisories/26759/>⁶⁴¹⁷ <http://secunia.com/advisories/26790/>⁶⁴¹⁸ <http://secunia.com/advisories/26822/>⁶⁴¹⁹ <http://secunia.com/advisories/26842/>⁶⁴²⁰ <http://secunia.com/advisories/26993/>⁶⁴²¹ <http://secunia.com/advisories/27121/>⁶⁴²² <http://secunia.com/advisories/27209/>⁶⁴²³ <http://secunia.com/advisories/27563/>⁶⁴²⁴ <http://secunia.com/advisories/27732/>⁶⁴²⁵ <http://secunia.com/advisories/28212/>

			SECUNIA 28606 ⁶⁴²⁷ SGI 20070701-01-P ⁶⁴²⁸ SUSE SUSE-SA:2007:061 ⁶⁴²⁹ XF apache-child-process-dos(35095) ⁶⁴³⁰ URL1 ⁶⁴³¹		
21.	FTP access with ftp account (ftp-generic-0001)	172.23.202.126:21 172.23.202.225:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisnikovim ID-jem (identifikacijom) "ftp" i šifrom "ftp". Dosadašnja praksa je pokazala da je najbolje ukloniti difoltnu naloge, ukoliko je to moguće. Za naloge koje sistem zahteva treba izmeniti difoltnu šifru.	CVE CVE-1999-0497 ⁶⁴³²	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko nije kritičan za dalje funkcionisanje sistema. U suprotnom, treba promeniti šifru u nedifoltnu vrednost.
22.	FTP access with anonymous account (ftp-generic-0002)	172.23.202.126:21 172.23.202.225:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisnikovim ID-jem (identifikacijom) "anonymous" i šifrom "ftp@". Dosadašnja praksa je pokazala da je najbolje ukloniti difoltnu naloge, ukoliko je to moguće. Za naloge koje sistem zahteva treba izmeniti difoltnu šifru.	CVE CVE-1999-0497 ⁶⁴³³	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko nije kritičan za dalje funkcionisanje sistema. U suprotnom, treba promeniti šifru u nedifoltnu vrednost.
23.	FTP server does not support AUTH command (ftp-generic-0007)	172.23.202.126:21 172.23.202.225:21 FTP klijenti po difoltu šalju FTP server-u poverljive podatke (korisnički ID i šifru) u vidu čitkog teksta. Ova okolnost dozvoljava zlonamernim korisnicima da presreću poverljive podatke ukoliko prisluškuju vezu. Noviji FTP serveri podržavaju AUTH komandu, koja omogućava dodatne opcije autentifikacije, kao što su TLS, Kerberos, GSSAPI itd. Ona se može koristiti za sprečavanje prisluškivanja na FTP vezama.		Ozbiljan	Ažurirati/preći na FTP server koji podržava AUTH komandu.
24.	Apache HTTPD: mod_proxy crash (CVE-2007-3847) (apache-httpd-cve-2007-3847)	172.23.202.126:80 172.23.202.225:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja prisustva mod_proxy modula. Propust je otkriven u modulu mod_proxy Apache HTTP servera. Na sajtovima na kojima je	APPLE APPLE-SA-2008-03-18 ⁶⁴³⁴ APPLE APPLE-SA-2008-05-28 ⁶⁴³⁵ BID 25489 ⁶⁴³⁶ CERT TA08-150A ⁶⁴³⁷ CVE CVE-2007-3847 ⁶⁴³⁸ OVAL OVAL10525 ⁶⁴³⁹ REDHAT RHSA-2007:0746 ⁶⁴⁴⁰	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.61.tar.gz Apache HTTPD >= 2.2 and < 2.2.6 Ažurirati na Apache HTTPD version 2.2.6 Uraditi download a zatim

⁶⁴²⁶ <http://secunia.com/advisories/28224/>⁶⁴²⁷ <http://secunia.com/advisories/28606/>⁶⁴²⁸ <ftp://patches.sgi.com/support/free/security/advisories/20070701-01-P> pristupljeno 18.12.2011⁶⁴²⁹ <https://www.suse.com/support/security/advisories/>⁶⁴³⁰ <http://xforce.iss.net/xforce/xfdb/35095>⁶⁴³¹ http://httpd.apache.org/security/vulnerabilities_20.html⁶⁴³² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>⁶⁴³³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>⁶⁴³⁴ <http://lists.apple.com/archives/security-announce/2008/Mar/msg00000.html>⁶⁴³⁵ <http://lists.apple.com/archives/security-announce/2008/May/msg00001.html>⁶⁴³⁶ <http://www.securityfocus.com/bid/25489> pristupljeno 18.12.2011⁶⁴³⁷ <http://www.cert.org/advisories/TA08-150A.html> pristupljeno 18.12.2011⁶⁴³⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3847>⁶⁴³⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10525>

		konfigurisan reverzni proxy, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do toga da Apache child proces, koji obrađuje taj zahtev krahira. Na sajtovima na kojima je konfigurisan "forward proxy", napadač bi mogao da izazove sličan krah ukoliko bi korisnik bio primoran da poseti zlonameran sajt koristeći proxy. To može dovesti samo do odbijanja servisa ako se koristi threaded MPM.	REDHAT 2007:0747 ⁶⁴⁴¹ RHSA- REDHAT 2007:0911 ⁶⁴⁴² RHSA- REDHAT 2008:0005 ⁶⁴⁴³ RHSA- SECUNIA 26636 ⁶⁴⁴⁴ SECUNIA 26722 ⁶⁴⁴⁵ SECUNIA 26790 ⁶⁴⁴⁶ SECUNIA 26842 ⁶⁴⁴⁷ SECUNIA 26952 ⁶⁴⁴⁸ SECUNIA 26993 ⁶⁴⁴⁹ SECUNIA 27209 ⁶⁴⁵⁰ SECUNIA 27563 ⁶⁴⁵¹ SECUNIA 27593 ⁶⁴⁵² SECUNIA 27732 ⁶⁴⁵³ SECUNIA 27882 ⁶⁴⁵⁴ SECUNIA 27971 ⁶⁴⁵⁵ SECUNIA 28467 ⁶⁴⁵⁶ SECUNIA 28606 ⁶⁴⁵⁷ SECUNIA 28749 ⁶⁴⁵⁸ SECUNIA 28922 ⁶⁴⁵⁹ SECUNIA 29420 ⁶⁴⁶⁰ SECUNIA 30430 ⁶⁴⁶¹ SUSE SA:2007:061 ⁶⁴⁶² SUSE- URL1 6463		instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz
25.	Apache httpd Worker MPM memory leak (CVE-2005-2970) (http://apache-worker-mpm-memleak)	172.23.202.126:80 172.23.202.225:80 Gubitak memorije u Worker MPM-u bi udaljenim napadačima omogućio da prouzrokuju odbijanje servisa (zauzimanje memorije) preko prekinutih veza, što onemogućava da se memorija iz transakcionih pool-ova ponovo koristi za druge veze.	BID 15762 ⁶⁴⁶⁴ CVE CVE-2005-2970 ⁶⁴⁶⁵ OVAL OVAL10043 ⁶⁴⁶⁶ REDHAT 2006:0159 ⁶⁴⁶⁷ RHSA- SECUNIA 16559 ⁶⁴⁶⁸ SECUNIA 17923 ⁶⁴⁶⁹ SECUNIA 18161 ⁶⁴⁷⁰ SECUNIA 18333 ⁶⁴⁷¹ SECUNIA 18585 ⁶⁴⁷²	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.55.tar.gz

⁶⁴⁴⁰ <http://rhn.redhat.com/errata/RHSA-2007-0746.html>⁶⁴⁴¹ <http://rhn.redhat.com/errata/RHSA-2007-0747.html>⁶⁴⁴² <http://rhn.redhat.com/errata/RHSA-2007-0911.html>⁶⁴⁴³ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>⁶⁴⁴⁴ <http://secunia.com/advisories/26636/>⁶⁴⁴⁵ <http://secunia.com/advisories/26722/>⁶⁴⁴⁶ <http://secunia.com/advisories/26790/>⁶⁴⁴⁷ <http://secunia.com/advisories/26842/>⁶⁴⁴⁸ <http://secunia.com/advisories/26952/>⁶⁴⁴⁹ <http://secunia.com/advisories/26993/>⁶⁴⁵⁰ <http://secunia.com/advisories/27209/>⁶⁴⁵¹ <http://secunia.com/advisories/27563/>⁶⁴⁵² <http://secunia.com/advisories/27593/>⁶⁴⁵³ <http://secunia.com/advisories/27732/>⁶⁴⁵⁴ <http://secunia.com/advisories/27882/>⁶⁴⁵⁵ <http://secunia.com/advisories/27971/>⁶⁴⁵⁶ <http://secunia.com/advisories/28467/>⁶⁴⁵⁷ <http://secunia.com/advisories/28606/>⁶⁴⁵⁸ <http://secunia.com/advisories/28749/>⁶⁴⁵⁹ <http://secunia.com/advisories/28922/>⁶⁴⁶⁰ <http://secunia.com/advisories/29420/>⁶⁴⁶¹ <http://secunia.com/advisories/30430/>⁶⁴⁶² <https://www.suse.com/support/security/advisories/>⁶⁴⁶³ http://httpd.apache.org/security/vulnerabilities_20.html⁶⁴⁶⁴ <http://www.securityfocus.com/bid/15762>⁶⁴⁶⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2970>⁶⁴⁶⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10043>⁶⁴⁶⁷ <http://rhn.redhat.com/errata/RHSA-2006-0159.html>⁶⁴⁶⁸ <http://secunia.com/advisories/16559/>⁶⁴⁶⁹ <http://secunia.com/advisories/17923/>⁶⁴⁷⁰ <http://secunia.com/advisories/18161/>⁶⁴⁷¹ <http://secunia.com/advisories/18333/>⁶⁴⁷² <http://secunia.com/advisories/18585/>

26.	Apache httpd Memory consumption DoS (CVE-2004-0942) (http://apache2-long-header-dos)	172.23.202.126:80 172.23.202.225:80 Problem je otkriven tamo gde ograničenje dužine rubrike nije bilo primenjeno za određene zlonamerne zahteve. To bi udaljenom napadaču, koji je u mogućnosti da šalje velike količine podataka serveru, omogućilo child procesi Apache-a zauzmu srazmerno velike količine memorije, što bi dovelo do odbijanja servisa.	URL1 ⁶⁴⁷³ CVE CVE-2004-0942 ⁶⁴⁷⁴ MANDRAKE MDKSA-2004:135 ⁶⁴⁷⁵ OVAL OVAL10962 ⁶⁴⁷⁶ REDHAT RHSA-2004:562 ⁶⁴⁷⁷ SECUNIA 19072 ⁶⁴⁷⁸ XF apache-http-get-dos(17930) ⁶⁴⁷⁹ URL1 ⁶⁴⁸⁰	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.53.tar.gz
27.	Apache httpd ByteRange filter DoS (CVE-2005-2728) (http://apache2-reverse-proxy-memory-leak)	172.23.202.126:80 172.23.202.225:80 Propust u Apache-ovom filteru opsega bajtova može da dovede do toga da se određeni odgovori baferuju u memoriju. Ako server poseduje dinamički izvor, kao što je CGI skripte ili PHP skripte, koje obrađuju velike količine podataka, napadač bi mogao da pošalje pažljivo izrađen zahtev sa ciljem iskorišćavanja resursa, što može da dovede do odbijanja servisa.	BID 14660 ⁶⁴⁸¹ CVE CVE-2005-2728 ⁶⁴⁸² DEBIAN DSA-805 ⁶⁴⁸³ OVAL OVAL10017 ⁶⁴⁸⁴ OVAL OVAL1246 ⁶⁴⁸⁵ OVAL OVAL1727 ⁶⁴⁸⁶ OVAL OVAL760 ⁶⁴⁸⁷ REDHAT RHSA-2005:608 ⁶⁴⁸⁸ SECUNIA 16559 ⁶⁴⁸⁹ SECUNIA 16705 ⁶⁴⁹⁰ SECUNIA 16714 ⁶⁴⁹¹ SECUNIA 16743 ⁶⁴⁹² SECUNIA 16746 ⁶⁴⁹³ SECUNIA 16753 ⁶⁴⁹⁴ SECUNIA 16754 ⁶⁴⁹⁵ SECUNIA 16769 ⁶⁴⁹⁶ SECUNIA 16789 ⁶⁴⁹⁷ SECUNIA 16956 ⁶⁴⁹⁸ SECUNIA 17036 ⁶⁴⁹⁹ SECUNIA 17288 ⁶⁵⁰⁰ SECUNIA 17600 ⁶⁵⁰¹ SECUNIA 17831 ⁶⁵⁰² SECUNIA 17923 ⁶⁵⁰³ SECUNIA 18161 ⁶⁵⁰⁴	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.55.tar.gz

⁶⁴⁷³ http://httpd.apache.org/security/vulnerabilities_20.html⁶⁴⁷⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0942>⁶⁴⁷⁵ <http://www.mandriva.com/en/support/security/advisories/advisory/MDKSA-2004:135/?name=MDKSA-2004:135>⁶⁴⁷⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10962>⁶⁴⁷⁷ <http://rhn.redhat.com/errata/RHSA-2004-562.html>⁶⁴⁷⁸ <http://secunia.com/advisories/19072/>⁶⁴⁷⁹ <http://xforce.iss.net/xforce/xfdb/17930>⁶⁴⁸⁰ http://httpd.apache.org/security/vulnerabilities_20.html⁶⁴⁸¹ <http://www.securityfocus.com/bid/14660>⁶⁴⁸² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2728>⁶⁴⁸³ <https://security-tracker.debian.org/tracker/DSA-805-1>⁶⁴⁸⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10017>⁶⁴⁸⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1246>⁶⁴⁸⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1727>⁶⁴⁸⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:760>⁶⁴⁸⁸ <http://rhn.redhat.com/errata/RHSA-2005-608.html>⁶⁴⁸⁹ <http://secunia.com/advisories/16559/>⁶⁴⁹⁰ <http://secunia.com/advisories/16705/>⁶⁴⁹¹ <http://secunia.com/advisories/16714/>⁶⁴⁹² <http://secunia.com/advisories/16743/>⁶⁴⁹³ <http://secunia.com/advisories/16746/>⁶⁴⁹⁴ <http://secunia.com/advisories/16753/>⁶⁴⁹⁵ <http://secunia.com/advisories/16754/>⁶⁴⁹⁶ <http://secunia.com/advisories/16769/>⁶⁴⁹⁷ <http://secunia.com/advisories/16789/>⁶⁴⁹⁸ <http://secunia.com/advisories/16956/>⁶⁴⁹⁹ <http://secunia.com/advisories/17036/>⁶⁵⁰⁰ <http://secunia.com/advisories/17288/>⁶⁵⁰¹ <http://secunia.com/advisories/17600/>⁶⁵⁰² <http://secunia.com/advisories/17831/>⁶⁵⁰³ <http://secunia.com/advisories/17923/>⁶⁵⁰⁴ <http://secunia.com/advisories/18161/>

			SECUNIA 18333 ⁶⁵⁰⁵ SECUNIA 18517 ⁶⁵⁰⁶ SECUNIA 19072 ⁶⁵⁰⁷ SGI 20060101-01-U ⁶⁵⁰⁸ SUSE SUSE- SA:2005:051 ⁶⁵⁰⁹ SUSE SUSE- SA:2005:052 ⁶⁵¹⁰ XF apache-byterange- dos(22006) URL1 ⁶⁵¹¹		
28.	Apache httpd Malicious CRL off-by-one (CVE-2005-1268) (http://apache2-ssl-crl-verify-bof)	172.23.202.126:80 172.23.202.225:80 Ranjivost tipa "off-by-one stack overflow" je otkrivena u mod_ssl CRL pri overi povratnog poziva. Da bi sprečio ovaj problem, Apache server treba da bude konfigurisan tako da koristi listu opozvanih sertifikata (CRL).	BID 14366 ⁶⁵¹² CVE CVE-2005-1268 ⁶⁵¹³ DEBIAN DSA-805 ⁶⁵¹⁴ MANDRAKE MDKSA-2005:129 ⁶⁵¹⁵ OVAL OVAL1346 ⁶⁵¹⁶ OVAL OVAL1714 ⁶⁵¹⁷ OVAL OVAL1747 ⁶⁵¹⁸ OVAL OVAL9589 ⁶⁵¹⁹ REDHAT RHSA-2005:582 ⁶⁵²⁰ SECUNIA 19072 ⁶⁵²¹ SECUNIA 19185 ⁶⁵²² SUSE SUSE- SA:2005:046 ⁶⁵²³ URL1 ⁶⁵²⁴	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.55.tar.gz
29.	Browsable web directory (http-generic-browsable-dir)	172.23.202.126:8080 172.23.202.225:8080 Otkriven je direktorijum na web serveru koji može biti pretraživan, što znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice - spajdering (prateći hiperlinkove), ili -kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute force napadom na liste uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skrivena“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice. Primer:		Ozbiljan	Za Apache: onemogućiti pretraživanje direktorijuma mreže za sve direktorijume i poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati

⁶⁵⁰⁵ <http://secunia.com/advisories/18333/>⁶⁵⁰⁶ <http://secunia.com/advisories/18517/>⁶⁵⁰⁷ <http://secunia.com/advisories/19072/>⁶⁵⁰⁸ <ftp://patches.sgi.com/support/free/security/advisories/20060101-01-U> pristupljeno 18.12.2011⁶⁵⁰⁹ <https://www.suse.com/support/security/advisories/>⁶⁵¹⁰ <https://www.suse.com/support/security/advisories/>⁶⁵¹¹ http://httpd.apache.org/security/vulnerabilities_20.html⁶⁵¹² <http://www.securityfocus.com/bid/14366>⁶⁵¹³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-1268>⁶⁵¹⁴ <https://security-tracker.debian.org/tracker/DSA-805-1>⁶⁵¹⁵ <http://www.mandriva.com/en/support/security/advisories/advisory/MDKSA-2005:129/?name=MDKSA-2005:129>⁶⁵¹⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1346>⁶⁵¹⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1714>⁶⁵¹⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1747>⁶⁵¹⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9589>⁶⁵²⁰ <http://rhn.redhat.com/errata/RHSA-2005-582.html>⁶⁵²¹ <http://secunia.com/advisories/19072/>⁶⁵²² <http://secunia.com/advisories/19185/>⁶⁵²³ <https://www.suse.com/support/security/advisories/>⁶⁵²⁴ http://httpd.apache.org/security/vulnerabilities_20.html

		http://172.23.202.126:8080/webdav/ 1: <html> 2: <head> 3: <title>Directory Listing For /</title>			svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume. Za Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote: Onemogućiti pretraživanje direktorijuma za sve direktorijume i poddirektorijume. Uključiti Tomcat-ov web.xml file. U odeljku „default“, promeniti parametar „listings“ iz „true“ u „false“. Restartovati server. Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripta i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume.
30.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	TCP reset with incorrect sequence number triggered this fault on 172.23.202.126:3306 172.23.202.225:3306: Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	OSVDB 4030 ⁶⁵²⁵ BID: 10183 ⁶⁵²⁶ CERT-VN: 415294 ⁶⁵²⁷ CVE CVE-2004-0230 ⁶⁵²⁸ MS: MS05-019 ⁶⁵²⁹ MS: MS06-064 ⁶⁵³⁰ NETBSD: NetBSD-SA2004-006 ⁶⁵³¹ OVAL: OVAL2689 ⁶⁵³² OVAL: OVAL270 ⁶⁵³³ OVAL OVAL3508 ⁶⁵³⁴ OVAL OVAL4791 ⁶⁵³⁵ OVAL OVAL5711 ⁶⁵³⁶ SECUNIA: 11440 ⁶⁵³⁷ SECUNIA 11458 ⁶⁵³⁸ SECUNIA: 22341 ⁶⁵³⁹ SGI 20040403-01-A ⁶⁵⁴⁰ XF tcp-rst-dos(15886) ⁶⁵⁴¹	Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC 2385 ⁶⁵⁴⁴ . Ono je napravljeno da smanji opasnost od određenih napada na BGP, kao što su TCP reseti.

⁶⁵²⁵ <http://www.osvdb.org/4030>⁶⁵²⁶ <http://www.securityfocus.com/bid/10183>⁶⁵²⁷ <http://www.kb.cert.org/vuls/id/415294>⁶⁵²⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁶⁵²⁹ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁶⁵³⁰ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁶⁵³¹ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁶⁵³² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>⁶⁵³³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>⁶⁵³⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>⁶⁵³⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>⁶⁵³⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>⁶⁵³⁷ <http://secunia.com/advisories/11440/>⁶⁵³⁸ <http://secunia.com/advisories/11458/>⁶⁵³⁹ <http://secunia.com/advisories/22341/>⁶⁵⁴⁰ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>⁶⁵⁴¹ <http://xforce.iss.net/xforce/xfdb/15886>

			URL1 ⁶⁵⁴² URL2 ⁶⁵⁴³		
31.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podesi na jedinstvenu vrednost i da se koristi u rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da fingerprint-uje operativni sistem.	BID 4314 ⁶⁵⁴⁵ CVE CVE-2002-0510 ⁶⁵⁴⁶ XF linux-udp-fingerprint(8588) ⁶⁵⁴⁷	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili pak ranjivost koju treba popravljati, tako da ne postoje rešenja koja se mogu kupiti. Jedino se može postaviti fajervol ili neka druga sprava za filtriranje između napadnutog i neprijateljskog napada koji je u mogućnosti da randomizuje IP ID-jeve.
32.	Apache HTTPD: mod_imap XSS (CVE-2007-5000) (apache-httpd-cve-2007-5000)	172.23.202.126:80 172.23.202.225:80 Skenirani servis je ranjiv na ovu ranjivost samo ako je pokrenuo sledeće module: mod_imagemap, mod_imap i imagemap fajl je javno dostupan. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u modulu mod_imap. Na sajtovim na kojima je omogućen mod_imap i fajl imagemap je javno dostupan, moguće je izvesti napad tipa "crossite scripting attack".	BID 26838 ⁶⁵⁴⁸ CERT TA08-150A ⁶⁵⁴⁹ CVE CVE-2007-5000 ⁶⁵⁵⁰ OSVDB 39134 ⁶⁵⁵¹ OVAL OVAL9539 ⁶⁵⁵² REDHAT RHSA-2008:0004 ⁶⁵⁵³ REDHAT RHSA-2008:0005 ⁶⁵⁵⁴ REDHAT RHSA-2008:0006 ⁶⁵⁵⁵ REDHAT RHSA-2008:0007 ⁶⁵⁵⁶ REDHAT RHSA-2008:0008 ⁶⁵⁵⁷ REDHAT RHSA-2008:0009 ⁶⁵⁵⁸ REDHAT RHSA-2008:0261 ⁶⁵⁵⁹ SECUNIA 28046 ⁶⁵⁶⁰ SECUNIA 28073 ⁶⁵⁶¹ SECUNIA 28081 ⁶⁵⁶² SECUNIA 28196 ⁶⁵⁶³ SECUNIA 28375 ⁶⁵⁶⁴ SECUNIA 28467 ⁶⁵⁶⁵ SECUNIA 28471 ⁶⁵⁶⁶ SECUNIA 28525 ⁶⁵⁶⁷ SECUNIA 28526 ⁶⁵⁶⁸	Ozbiljan	Apache >= 2.0 and < 2.1 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.63.tar.gz Apache HTTPD >= 1.3 and < 1.3.41 Ažurirati na Apache HTTPD version 1.3.41 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/apache-1.3.41.tar.gz Apache HTTPD >= 2.2 and < 2.2.8 Ažurirati na Apache HTTPD version 2.2.8 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.8.tar.gz

⁶⁵⁴⁴ <http://www.ietf.org/rfc/rfc2385.txt>⁶⁵⁴² <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁶⁵⁴³ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>⁶⁵⁴⁵ <http://www.securityfocus.com/bid/4314>⁶⁵⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>⁶⁵⁴⁷ <http://xforce.iss.net/xforce/xfdb/8588>⁶⁵⁴⁸ <http://www.securityfocus.com/bid/26838>⁶⁵⁴⁹ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>⁶⁵⁵⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-5000>⁶⁵⁵¹ <http://www.osvdb.org/39134>⁶⁵⁵² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9539>⁶⁵⁵³ <http://rhn.redhat.com/errata/RHSA-2008-0004.html>⁶⁵⁵⁴ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>⁶⁵⁵⁵ <http://rhn.redhat.com/errata/RHSA-2008-0006.html>⁶⁵⁵⁶ <http://rhn.redhat.com/errata/RHSA-2008-0007.html>⁶⁵⁵⁷ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>⁶⁵⁵⁸ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>⁶⁵⁵⁹ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>⁶⁵⁶⁰ <http://secunia.com/advisories/28046/>⁶⁵⁶¹ <http://secunia.com/advisories/28073/>⁶⁵⁶² <http://secunia.com/advisories/28081/>⁶⁵⁶³ <http://secunia.com/advisories/28196/>⁶⁵⁶⁴ <http://secunia.com/advisories/28375/>⁶⁵⁶⁵ <http://secunia.com/advisories/28467/>⁶⁵⁶⁶ <http://secunia.com/advisories/28471/>⁶⁵⁶⁷ <http://secunia.com/advisories/28525/>⁶⁵⁶⁸ <http://secunia.com/advisories/28526/>

			SECUNIA 28607 ⁶⁵⁶⁹ SECUNIA 28749 ⁶⁵⁷⁰ SECUNIA 28750 ⁶⁵⁷¹ SECUNIA 28922 ⁶⁵⁷² SECUNIA 28977 ⁶⁵⁷³ SECUNIA 29420 ⁶⁵⁷⁴ SECUNIA 29640 ⁶⁵⁷⁵ SECUNIA 29806 ⁶⁵⁷⁶ SECUNIA 29988 ⁶⁵⁷⁷ SECUNIA 30356 ⁶⁵⁷⁸ SECUNIA 30430 ⁶⁵⁷⁹ SECUNIA 30732 ⁶⁵⁸⁰ SECUNIA 31142 ⁶⁵⁸¹ SECUNIA 32800 ⁶⁵⁸² SUSE SA:2008:021 ⁶⁵⁸³ SUSE- URL1 ⁶⁵⁸⁴		
33.	Apache httpd mod_imap XSS (CVE- 2007-5000) (apache- httpd-2_0_x- mod_imap-xss-cve- 2007-5000)	172.23.202.126:80 172.23.202.225:80 Propust je otkriven u modulu mod_imap. Na sajtovima na kojima je omogućen mod_imap i fajl imagemap je javno dostupan, moguće je izvesti napad tipa "cros-site scripting attack".	BID 26838 ⁶⁵⁸⁵ CERT TA08-150A ⁶⁵⁸⁶ CVE CVE-2007-5000 ⁶⁵⁸⁷ OSVDB 39134 ⁶⁵⁸⁸ OVAL OVAL9539 ⁶⁵⁸⁹ REDHAT RHSA- 2008:0004 ⁶⁵⁹⁰ REDHAT RHSA- 2008:0005 ⁶⁵⁹¹ REDHAT RHSA- 2008:0006 ⁶⁵⁹² REDHAT RHSA- 2008:0007 ⁶⁵⁹³ REDHAT RHSA- 2008:0008 ⁶⁵⁹⁴ REDHAT RHSA- 2008:0009 ⁶⁵⁹⁵ REDHAT RHSA- 2008:0261 ⁶⁵⁹⁶ SECUNIA 28046 ⁶⁵⁹⁷ SECUNIA 28073 ⁶⁵⁹⁸ SECUNIA 28081 ⁶⁵⁹⁹	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dis t/httpd/httpd-2.0.63.tar.gz

⁶⁵⁶⁹ <http://secunia.com/advisories/28607/>
⁶⁵⁷⁰ <http://secunia.com/advisories/28749/>
⁶⁵⁷¹ <http://secunia.com/advisories/28750/>
⁶⁵⁷² <http://secunia.com/advisories/28922/>
⁶⁵⁷³ <http://secunia.com/advisories/28977/>
⁶⁵⁷⁴ <http://secunia.com/advisories/29420/>
⁶⁵⁷⁵ <http://secunia.com/advisories/29640/>
⁶⁵⁷⁶ <http://secunia.com/advisories/29806/>
⁶⁵⁷⁷ <http://secunia.com/advisories/29988/>
⁶⁵⁷⁸ <http://secunia.com/advisories/30356/>
⁶⁵⁷⁹ <http://secunia.com/advisories/30430/>
⁶⁵⁸⁰ <http://secunia.com/advisories/30732/>
⁶⁵⁸¹ <http://secunia.com/advisories/31142/>
⁶⁵⁸² <http://secunia.com/advisories/32800/>
⁶⁵⁸³ <https://www.suse.com/support/security/advisories/>
⁶⁵⁸⁴ http://httpd.apache.org/security/vulnerabilities_20.html
⁶⁵⁸⁵ <http://www.securityfocus.com/bid/26838>
⁶⁵⁸⁶ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>
⁶⁵⁸⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-5000>
⁶⁵⁸⁸ <http://www.osvdb.org/39134>
⁶⁵⁸⁹ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:9539>
⁶⁵⁹⁰ <http://rhn.redhat.com/errata/RHSA-2008-0004.html>
⁶⁵⁹¹ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>
⁶⁵⁹² <http://rhn.redhat.com/errata/RHSA-2008-0006.html>
⁶⁵⁹³ <http://rhn.redhat.com/errata/RHSA-2008-0007.html>
⁶⁵⁹⁴ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>
⁶⁵⁹⁵ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>
⁶⁵⁹⁶ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>
⁶⁵⁹⁷ <http://secunia.com/advisories/28046/>
⁶⁵⁹⁸ <http://secunia.com/advisories/28073/>
⁶⁵⁹⁹ <http://secunia.com/advisories/28081/>

			SECUNIA 28196 ⁶⁶⁰⁰ SECUNIA 28375 ⁶⁶⁰¹ SECUNIA 28467 ⁶⁶⁰² SECUNIA 28471 ⁶⁶⁰³ SECUNIA 28525 ⁶⁶⁰⁴ SECUNIA 28526 ⁶⁶⁰⁵ SECUNIA 28607 ⁶⁶⁰⁶ SECUNIA 28749 ⁶⁶⁰⁷ SECUNIA 28750 ⁶⁶⁰⁸ SECUNIA 28922 ⁶⁶⁰⁹ SECUNIA 28977 ⁶⁶¹⁰ SECUNIA 29420 ⁶⁶¹¹ SECUNIA 29640 ⁶⁶¹² SECUNIA 29806 ⁶⁶¹³ SECUNIA 29988 ⁶⁶¹⁴ SECUNIA 30356 ⁶⁶¹⁵ SECUNIA 30430 ⁶⁶¹⁶ SECUNIA 30732 ⁶⁶¹⁷ SECUNIA 31142 ⁶⁶¹⁸ XF apache-modimagemap-xss(39002) ⁶⁶¹⁹ XF apache-modimagemap-xss(39001) ⁶⁶²⁰ URL1 ⁶⁶²¹		
34.	Apache HTTPD: mod_status cross-site scripting (CVE-2006-5752) (apache-httpd-cve-2006-5752)	172.23.202.126:80 172.23.202.225:80 Skenirani servis je osjetljiv na ovu ranjivost samo ako je pokrenut modul mod_status i ukoliko su stranice statusa javno dostupne. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u modulu mod_status. Na sajtovima na kojima je status servera javno dostupan i omogućen je ExtendedStatus, postoji mogućnost XSS napada. Stranica sa statusom servera nije po defaultu	OSVDB 37052 ⁶⁶²² BID 24645 ⁶⁶²³ CVE CVE-2006-5752 ⁶⁶²⁴ OVAL OVAL10154 ⁶⁶²⁵ REDHAT RHSA-2007:0532 ⁶⁶²⁶ REDHAT RHSA-2007:0533 ⁶⁶²⁷ REDHAT RHSA-2007:0534 ⁶⁶²⁸ REDHAT RHSA-2007:0556 ⁶⁶²⁹ REDHAT RHSA-2007:0557 ⁶⁶³⁰	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.61.tar.gz Apache HTTPD >= 1.3 and < 1.3.39 Ažurirati na Apache HTTPD version 1.3.39 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/apache-1.3.39.tar.gz Apache HTTPD >= 2.2 and

⁶⁶⁰⁰ <http://secunia.com/advisories/28196/>⁶⁶⁰¹ <http://secunia.com/advisories/28375/>⁶⁶⁰² <http://secunia.com/advisories/28467/>⁶⁶⁰³ <http://secunia.com/advisories/28471/>⁶⁶⁰⁴ <http://secunia.com/advisories/28525/>⁶⁶⁰⁵ <http://secunia.com/advisories/28526/>⁶⁶⁰⁶ <http://secunia.com/advisories/28607/>⁶⁶⁰⁷ <http://secunia.com/advisories/28749/>⁶⁶⁰⁸ <http://secunia.com/advisories/28750/>⁶⁶⁰⁹ <http://secunia.com/advisories/28922/>⁶⁶¹⁰ <http://secunia.com/advisories/28977/>⁶⁶¹¹ <http://secunia.com/advisories/29420/>⁶⁶¹² <http://secunia.com/advisories/29640/>⁶⁶¹³ <http://secunia.com/advisories/29806/>⁶⁶¹⁴ <http://secunia.com/advisories/29988/>⁶⁶¹⁵ <http://secunia.com/advisories/30356/>⁶⁶¹⁶ <http://secunia.com/advisories/30430/>⁶⁶¹⁷ <http://secunia.com/advisories/30732/>⁶⁶¹⁸ <http://secunia.com/advisories/31142/>⁶⁶¹⁹ <http://xforce.iss.net/xforce/xfdb/39002>⁶⁶²⁰ <http://xforce.iss.net/xforce/xfdb/39001>⁶⁶²¹ http://httpd.apache.org/security/vulnerabilities_20.html⁶⁶²² <http://www.osvdb.org/37052>⁶⁶²³ <http://www.securityfocus.com/bid/24645>⁶⁶²⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-5752>⁶⁶²⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10154>⁶⁶²⁶ <http://rhn.redhat.com/errata/RHSA-2007-0532.html>⁶⁶²⁷ <http://rhn.redhat.com/errata/RHSA-2007-0533.html>⁶⁶²⁸ <http://rhn.redhat.com/errata/RHSA-2007-0534.html>⁶⁶²⁹ <http://rhn.redhat.com/errata/RHSA-2007-0556.html>⁶⁶³⁰ <http://rhn.redhat.com/errata/RHSA-2007-0557.html>

		omogućena, a dosadašnja praksa je pokazala da je najbolje da ona ne bude javno dostupna.	REDHAT RHSA-2008:0261 ⁶⁶³¹ SECUNIA 25827 ⁶⁶³² SECUNIA 25830 ⁶⁶³³ SECUNIA 25873 ⁶⁶³⁴ SECUNIA 25920 ⁶⁶³⁵ SECUNIA 26273 ⁶⁶³⁶ SECUNIA 26443 ⁶⁶³⁷ SECUNIA 26458 ⁶⁶³⁸ SECUNIA 26508 ⁶⁶³⁹ SECUNIA 26822 ⁶⁶⁴⁰ SECUNIA 26842 ⁶⁶⁴¹ SECUNIA 26993 ⁶⁶⁴² SECUNIA 27037 ⁶⁶⁴³ SECUNIA 27563 ⁶⁶⁴⁴ SECUNIA 27732 ⁶⁶⁴⁵ SECUNIA 28212 ⁶⁶⁴⁶ SECUNIA 28224 ⁶⁶⁴⁷ SECUNIA 28606 ⁶⁶⁴⁸ SUSE SUSE-SA:2007:061 ⁶⁶⁴⁹ XF apache-modstatus-xss(35097) ⁶⁶⁵⁰ URL1 ⁶⁶⁵⁰		< 2.2.6 Ažurirati na Apache HTTPD version 2.2.6 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz
35.	Apache HTTPD: Subrequest handling of request headers (mod_headers) (CVE-2010-0434) (apache-httpdcve-2010-0434)	172.23.202.126:80 172.23.202.225:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_headers. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust u jezgru "subrequest process code" može dovesti do greške tipa segmentation fault-a ili do otkrivanja podataka iz nekog drugog zahteva na thread-ovima servera, kao što su worker ili winnt MPM-ovi. Zahvaljujući Philip Pickett-u iz Vmware, ovaj propust je prijavljen i	APPLE APPLE-SA-2010-11-10 ⁶⁶⁵¹ BID 38494 ⁶⁶⁵² CVE CVE-2010-0434 ⁶⁶⁵³ DEBIAN DSA-2035 ⁶⁶⁵⁴ OVAL OVAL10358 ⁶⁶⁵⁵ OVAL OVAL8695 ⁶⁶⁵⁶ REDHAT RHSA-2010:0168 ⁶⁶⁵⁷ REDHAT RHSA-2010:0175 ⁶⁶⁵⁸ SECUNIA 39100 ⁶⁶⁵⁹ SECUNIA 39115 ⁶⁶⁶⁰ SECUNIA 39501 ⁶⁶⁶¹ SECUNIA 39628 ⁶⁶⁶²	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.15 Ažurirati na Apache HTTPD version 2.2.15 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz

⁶⁶³¹ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>⁶⁶³² <http://secunia.com/advisories/25827/>⁶⁶³³ <http://secunia.com/advisories/25830/>⁶⁶³⁴ <http://secunia.com/advisories/25873/>⁶⁶³⁵ <http://secunia.com/advisories/25920/>⁶⁶³⁶ <http://secunia.com/advisories/26273/>⁶⁶³⁷ <http://secunia.com/advisories/26443/>⁶⁶³⁸ <http://secunia.com/advisories/26458/>⁶⁶³⁹ <http://secunia.com/advisories/26508/>⁶⁶⁴⁰ <http://secunia.com/advisories/26822/>⁶⁶⁴¹ <http://secunia.com/advisories/26842/>⁶⁶⁴² <http://secunia.com/advisories/26993/>⁶⁶⁴³ <http://secunia.com/advisories/27037/>⁶⁶⁴⁴ <http://secunia.com/advisories/27563/>⁶⁶⁴⁵ <http://secunia.com/advisories/27732/>⁶⁶⁴⁶ <http://secunia.com/advisories/28212/>⁶⁶⁴⁷ <http://secunia.com/advisories/28224/>⁶⁶⁴⁸ <http://secunia.com/advisories/28606/>⁶⁶⁴⁹ <https://www.suse.com/support/security/advisories/>⁶⁶⁵⁰ http://httpd.apache.org/security/vulnerabilities_20.html⁶⁶⁵¹ <http://support.apple.com/kb/ht4435>⁶⁶⁵² <http://www.securityfocus.com/bid/38494>⁶⁶⁵³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0434>⁶⁶⁵⁴ <http://www.debian.org/security/2010/dsa-2035>⁶⁶⁵⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10358>⁶⁶⁵⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8695>⁶⁶⁵⁷ <http://rhn.redhat.com/errata/RHSA-2010-0168.html>⁶⁶⁵⁸ <http://rhn.redhat.com/errata/RHSA-2010-0175.html>⁶⁶⁵⁹ <http://secunia.com/advisories/39100/>⁶⁶⁶⁰ <http://secunia.com/advisories/39115/>⁶⁶⁶¹ <http://secunia.com/advisories/39501/>

		predložen je način ispravke.	SECUNIA 39632 ⁶⁶⁶³ SECUNIA 39656 ⁶⁶⁶⁴ SECUNIA 40096 ⁶⁶⁶⁵ XF apache-http-rh-info-disclosure(56625) ⁶⁶⁶⁶ URL1 ⁶⁶⁶⁷		
36.	Apache HTTPD: mod_proxy_ftp globbing XSS (CVE-2008-2939) (apache-httpd-cve-2008-2939)	172.23.202.126:80 172.23.202.225:80 Skenirani servis je osjetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ftp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u modulu mod_proxy_ftp prilikom obrade "wildcard-a" ukoliko se on nađe u putanji FTP URL. Ukoliko je mod_proxy_ftp omogućen da podržava FTP-over-HTTP, zahtevi koji sadrže specijalne karaktere mogu da dovedu do cross-site scripting napada (XSS).	APPLE APPLE-SA-2009-05-12 ⁶⁶⁶⁸ BID 30560 ⁶⁶⁶⁹ CERT TA09-133A ⁶⁶⁷⁰ CERT-VN 663763 ⁶⁶⁷¹ CVE CVE-2008-2939 ⁶⁶⁷² OVAL OVAL11316 ⁶⁶⁷³ OVAL OVAL7716 ⁶⁶⁷⁴ REDHAT RHSA-2008:0966 ⁶⁶⁷⁵ REDHAT RHSA-2008:0967 ⁶⁶⁷⁶ SECUNIA 31384 ⁶⁶⁷⁷ SECUNIA 31673 ⁶⁶⁷⁸ SECUNIA 32685 ⁶⁶⁷⁹ SECUNIA 32838 ⁶⁶⁸⁰ SECUNIA 33156 ⁶⁶⁸¹ SECUNIA 33797 ⁶⁶⁸² SECUNIA 34219 ⁶⁶⁸³ SECUNIA 35074 ⁶⁶⁸⁴ XF apache-modproxyftp-xss(44223) ⁶⁶⁸⁵ URL1 ⁶⁶⁸⁶	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.10 Ažurirati na Apache HTTPD version 2.2.10 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.10.tar.gz
37.	Apache httpd mod_imap Referer Cross-Site Scripting (CVE-2005-3352) (http-apache-mod_imap-xss)	172.23.202.126:80 172.23.202.225:80 Propust u modulu mod_imap prilikom upotrebe direktiva Referer sa mapama slika (eng. imagemaps). U određenim konfiguracijama sajtova, udaljeni napadač bi mogao da izvrši napad unakrsnog skriptovanja, ako bi	BID 15834 ⁶⁶⁸⁷ CERT TA08-150A ⁶⁶⁸⁸ CVE CVE-2005-3352 ⁶⁶⁸⁹ DEBIAN DSA-1167 ⁶⁶⁹⁰ OVAL OVAL10480 ⁶⁶⁹¹ REDHAT RHSA-2006:0158 ⁶⁶⁹² REDHAT RHSA-2006:0159 ⁶⁶⁹³	Ozbiljan	Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.58.tar.gz Apache HTTPD >= 1.3 and < 1.3.35 Ažurirati na Apache HTTPD version 1.3.35 Uraditi download a zatim

⁶⁶⁶² <http://secunia.com/advisories/39628/>⁶⁶⁶³ <http://secunia.com/advisories/39632/>⁶⁶⁶⁴ <http://secunia.com/advisories/39656/>⁶⁶⁶⁵ <http://secunia.com/advisories/40096/>⁶⁶⁶⁶ <http://xforce.iss.net/xforce/xfdb/56625>⁶⁶⁶⁷ http://httpd.apache.org/security/vulnerabilities_20.html⁶⁶⁶⁸ <http://lists.apple.com/archives/security-announce/2009/May/msg00001.html>⁶⁶⁶⁹ <http://www.securityfocus.com/bid/30560>⁶⁶⁷⁰ <http://www.us-cert.gov/ncas/alerts/TA09-133A>⁶⁶⁷¹ <http://www.kb.cert.org/vuls/id/663763>⁶⁶⁷² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-2939>⁶⁶⁷³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11316>⁶⁶⁷⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7716>⁶⁶⁷⁵ <http://rhn.redhat.com/errata/RHSA-2008-0966.html>⁶⁶⁷⁶ <http://rhn.redhat.com/errata/RHSA-2008-0967.html>⁶⁶⁷⁷ <http://secunia.com/advisories/31384/>⁶⁶⁷⁸ <http://secunia.com/advisories/31673/>⁶⁶⁷⁹ <http://secunia.com/advisories/32685/>⁶⁶⁸⁰ <http://secunia.com/advisories/32838/>⁶⁶⁸¹ <http://secunia.com/advisories/33156/>⁶⁶⁸² <http://secunia.com/advisories/33797/>⁶⁶⁸³ <http://secunia.com/advisories/34219/>⁶⁶⁸⁴ <http://secunia.com/advisories/35074/>⁶⁶⁸⁵ <http://xforce.iss.net/xforce/xfdb/44223>⁶⁶⁸⁶ http://httpd.apache.org/security/vulnerabilities_20.html⁶⁶⁸⁷ <http://www.securityfocus.com/bid/15834>⁶⁶⁸⁸ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>⁶⁶⁸⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-3352>⁶⁶⁹⁰ <http://lists.debian.org/debian-security-announce/2006/msg00257.html>⁶⁶⁹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10480>⁶⁶⁹² <http://rhn.redhat.com/errata/RHSA-2006-0158.html>⁶⁶⁹³ <http://rhn.redhat.com/errata/RHSA-2006-0159.html>

		korisnik bio naveden da poseti zlonamerni URL koristeći određene web pretraživače.	REDHAT RHSA-2006:0692 ⁶⁶⁹⁴ SECUNIA 17319 ⁶⁶⁹⁵ SECUNIA 18008 ⁶⁶⁹⁶ SECUNIA 18333 ⁶⁶⁹⁷ SECUNIA 18339 ⁶⁶⁹⁸ SECUNIA 18340 ⁶⁶⁹⁹ SECUNIA 18429 ⁶⁷⁰⁰ SECUNIA 18517 ⁶⁷⁰¹ SECUNIA 18526 ⁶⁷⁰² SECUNIA 18585 ⁶⁷⁰³ SECUNIA 18743 ⁶⁷⁰⁴ SECUNIA 19012 ⁶⁷⁰⁵ SECUNIA 20046 ⁶⁷⁰⁶ SECUNIA 20670 ⁶⁷⁰⁷ SECUNIA 21744 ⁶⁷⁰⁸ SECUNIA 22140 ⁶⁷⁰⁹ SECUNIA 22368 ⁶⁷¹⁰ SECUNIA 22388 ⁶⁷¹¹ SECUNIA 22669 ⁶⁷¹² SECUNIA 23260 ⁶⁷¹³ SECUNIA 25239 ⁶⁷¹⁴ SECUNIA 29420 ⁶⁷¹⁵ SECUNIA 29849 ⁶⁷¹⁶ SECUNIA 30430 ⁶⁷¹⁷ SGI 20060101-01-U ⁶⁷¹⁸ SUSE SA:2006:043 ⁶⁷¹⁹ URL1 ⁶⁷²⁰		instalirati: http://archive.apache.org/dist/httpd/apache-1.3.35.tar.gz Apache HTTPD >= 2.2 and < 2.2.2 Ažurirati na Apache HTTPD version 2.2.2 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.2.tar.gz
38.	Apache HTTPD: mod_proxy_ftp UTF-7 XSS (CVE-2008-0005) (apache-httpd-cve-2008-0005)	172.23.202.126:80 172.23.202.225:80 Skenirani servis je osjetljiv na ovu ranjivost samo ako je pokrenut modul mod_proxy_ftp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. U modul mod_proxy_ftp je dodata zaobilaznica. Na sajtovima na kojima	BID 27234 ⁶⁷²¹ CVE CVE-2008-0005 ⁶⁷²² OVAL OVAL10812 ⁶⁷²³ REDHAT RHSA-2008:0004 ⁶⁷²⁴ REDHAT RHSA-2008:0005 ⁶⁷²⁵ REDHAT RHSA-2008:0006 ⁶⁷²⁶	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.63.tar.gz Apache HTTPD >= 2.2 and < 2.2.8 Ažurirati na Apache HTTPD version 2.2.8

⁶⁶⁹⁴ <http://rhn.redhat.com/errata/RHSA-2006-0692.html>⁶⁶⁹⁵ <http://secunia.com/advisories/17319/>⁶⁶⁹⁶ <http://secunia.com/advisories/18008/>⁶⁶⁹⁷ <http://secunia.com/advisories/18333/>⁶⁶⁹⁸ <http://secunia.com/advisories/18339/>⁶⁶⁹⁹ <http://secunia.com/advisories/18340/>⁶⁷⁰⁰ <http://secunia.com/advisories/18429/>⁶⁷⁰¹ <http://secunia.com/advisories/18517/>⁶⁷⁰² <http://secunia.com/advisories/18526/>⁶⁷⁰³ <http://secunia.com/advisories/18585/>⁶⁷⁰⁴ <http://secunia.com/advisories/18743/>⁶⁷⁰⁵ <http://secunia.com/advisories/19012/>⁶⁷⁰⁶ <http://secunia.com/advisories/20046/>⁶⁷⁰⁷ <http://secunia.com/advisories/20670/>⁶⁷⁰⁸ <http://secunia.com/advisories/21744/>⁶⁷⁰⁹ <http://secunia.com/advisories/22140/>⁶⁷¹⁰ <http://secunia.com/advisories/22368/>⁶⁷¹¹ <http://secunia.com/advisories/22388/>⁶⁷¹² <http://secunia.com/advisories/22669/>⁶⁷¹³ <http://secunia.com/advisories/23260/>⁶⁷¹⁴ <http://secunia.com/advisories/25239/>⁶⁷¹⁵ <http://secunia.com/advisories/29420/>⁶⁷¹⁶ <http://secunia.com/advisories/29849/>⁶⁷¹⁷ <http://secunia.com/advisories/30430/>⁶⁷¹⁸ <ftp://patches.sgi.com/support/free/security/advisories/20060101-01-U> pristupljeno 18.12.2011⁶⁷¹⁹ <https://www.suse.com/support/security/advisories/>⁶⁷²⁰ http://httpd.apache.org/security/vulnerabilities_20.html⁶⁷²¹ <http://www.securityfocus.com/bid/27234>⁶⁷²² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0005>⁶⁷²³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10812>⁶⁷²⁴ <http://rhn.redhat.com/errata/RHSA-2008-0004.html>⁶⁷²⁵ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>

		je omogućen mod_proxy_ftp i konfigurisan je forward tipa proxy-ja, moguće je izvesti napad XSS na Web pretraživače koji neprepoznaju određeni character set prema pravilima iz dokumenta RFC 2616.	REDHAT 2008:0007 ⁶⁷²⁷ RHSA- REDHAT 2008:0008 ⁶⁷²⁸ RHSA- REDHAT 2008:0009 ⁶⁷²⁹ RHSA- SECUNIA 28467 ⁶⁷³⁰ SECUNIA 28471 ⁶⁷³¹ SECUNIA 28526 ⁶⁷³² SECUNIA 28607 ⁶⁷³³ SECUNIA 28749 ⁶⁷³⁴ SECUNIA 28977 ⁶⁷³⁵ SECUNIA 29348 ⁶⁷³⁶ SECUNIA 29420 ⁶⁷³⁷ SECUNIA 29640 ⁶⁷³⁸ SECUNIA 30732 ⁶⁷³⁹ SECUNIA 35650 ⁶⁷⁴⁰ SUSE SA:2008:021 ⁶⁷⁴¹ SUSE- XF apache-modproxyftp-utf7-xss(39615) URL1 ⁶⁷⁴²		Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.8.tar.gz
39.	Apache HTTPD: mod_status XSS (CVE-2007-6388) (apache-httpd-cve-2007-6388)	172.23.202.126:80 172.23.202.225:80 Skenirani servis je osjetljiv na ovu ranjivost samo ako je pokrenut modul mod_status i ukoliko su stranice statusa javno dostupne. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u modulu mod_status. Na sajtovima na kojima je status servera javno dostupan, postoji mogućnost XSS napada. Stranica sa statusom servera nije po difoltu omogućena, a dosadašnja praksa je pokazala da je najbolje da ona ne bude javno dostupna.	BID 27237 ⁶⁷⁴³ CERT TA08-150A ⁶⁷⁴⁴ CVE CVE-2007-6388 ⁶⁷⁴⁵ OVAL OVAL10272 ⁶⁷⁴⁶ REDHAT 2008:0004 ⁶⁷⁴⁷ RHSA- REDHAT 2008:0005 ⁶⁷⁴⁸ RHSA- REDHAT 2008:0006 ⁶⁷⁴⁹ RHSA- REDHAT 2008:0007 ⁶⁷⁵⁰ RHSA- REDHAT 2008:0008 ⁶⁷⁵¹ RHSA- REDHAT 2008:0009 ⁶⁷⁵² RHSA- REDHAT 2008:0261 ⁶⁷⁵³ RHSA- SECUNIA 28467 ⁶⁷⁵⁴	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.63.tar.gz Apache HTTPD >= 1.3 and < 1.3.41 Ažurirati na Apache HTTPD version 1.3.41 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/apache-1.3.41.tar.gz Apache HTTPD >= 2.2 and < 2.2.8 Ažurirati na Apache HTTPD version 2.2.8 Uraditi download a zatim instalirati:

⁶⁷²⁶ <http://rhn.redhat.com/errata/RHSA-2008-0006.html>⁶⁷²⁷ <http://rhn.redhat.com/errata/RHSA-2008-0007.html>⁶⁷²⁸ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>⁶⁷²⁹ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>⁶⁷³⁰ <http://secunia.com/advisories/28467/>⁶⁷³¹ <http://secunia.com/advisories/28471/>⁶⁷³² <http://secunia.com/advisories/28526/>⁶⁷³³ <http://secunia.com/advisories/28607/>⁶⁷³⁴ <http://secunia.com/advisories/28749/>⁶⁷³⁵ <http://secunia.com/advisories/28977/>⁶⁷³⁶ <http://secunia.com/advisories/29348/>⁶⁷³⁷ <http://secunia.com/advisories/29420/>⁶⁷³⁸ <http://secunia.com/advisories/29640/>⁶⁷³⁹ <http://secunia.com/advisories/30732/>⁶⁷⁴⁰ <http://secunia.com/advisories/35650/>⁶⁷⁴¹ <https://www.suse.com/support/security/advisories/>⁶⁷⁴² http://httpd.apache.org/security/vulnerabilities_20.html⁶⁷⁴³ <http://www.securityfocus.com/bid/27237>⁶⁷⁴⁴ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>⁶⁷⁴⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6388>⁶⁷⁴⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10272>⁶⁷⁴⁷ <http://rhn.redhat.com/errata/RHSA-2008-0004.html>⁶⁷⁴⁸ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>⁶⁷⁴⁹ <http://rhn.redhat.com/errata/RHSA-2008-0006.html>⁶⁷⁵⁰ <http://rhn.redhat.com/errata/RHSA-2008-0007.html>⁶⁷⁵¹ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>⁶⁷⁵² <http://rhn.redhat.com/errata/RHSA-2008-0009.html>⁶⁷⁵³ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>⁶⁷⁵⁴ <http://secunia.com/advisories/28467/>

			SECUNIA 28471 ⁶⁷⁵⁵ SECUNIA 28526 ⁶⁷⁵⁶ SECUNIA 28607 ⁶⁷⁵⁷ SECUNIA 28749 ⁶⁷⁵⁸ SECUNIA 28922 ⁶⁷⁵⁹ SECUNIA 28965 ⁶⁷⁶⁰ SECUNIA 28977 ⁶⁷⁶¹ SECUNIA 29420 ⁶⁷⁶² SECUNIA 29504 ⁶⁷⁶³ SECUNIA 29640 ⁶⁷⁶⁴ SECUNIA 29806 ⁶⁷⁶⁵ SECUNIA 29988 ⁶⁷⁶⁶ SECUNIA 30356 ⁶⁷⁶⁷ SECUNIA 30430 ⁶⁷⁶⁸ SECUNIA 30732 ⁶⁷⁶⁹ SECUNIA 31142 ⁶⁷⁷⁰ SECUNIA 33200 ⁶⁷⁷¹ SUSE SUSE-SA:2008:021 ⁶⁷⁷² XF apache-status-page-xss(39472) ⁶⁷⁷³		http://archive.apache.org/dist/httpd/httpd-2.2.8.tar.gz
40.	Apache httpd HTTP Request Spoofing (CVE-2005-2088) (http://apache-request-smuggling-vuln)	172.23.202.126:80 172.23.202.225:80 Propust je otkriven kada je Apache server korišćen kao HTTP proksi. Udaljeni napadač bi mogao da pošalje HTTP zahtev sa "Transfer- Encoding: chunked" hederom i Content-Length hederom i da dovede do toga da Apache nepropisno obradi i prosledi zahtev tako da ga server koji ga prima obradi kao poseban HTTP zahtev. Ovo bi moglo da dovede do zaobilaženja fajervola i do XSS napada.	BID 14106 ⁶⁷⁷⁴ BID 15647 ⁶⁷⁷⁵ CVE CVE-2005-2088 ⁶⁷⁷⁶ DEBIAN DSA-803 ⁶⁷⁷⁷ DEBIAN DSA-805 ⁶⁷⁷⁸ OVAL OVAL11452 ⁶⁷⁷⁹ OVAL OVAL1237 ⁶⁷⁸⁰ OVAL OVAL1526 ⁶⁷⁸¹ OVAL OVAL1629 ⁶⁷⁸² OVAL OVAL840 ⁶⁷⁸³ REDHAT RHSA-2005:582 ⁶⁷⁸⁴ SECUNIA 14530 ⁶⁷⁸⁵ SECUNIA 17319 ⁶⁷⁸⁶ SECUNIA 17487 ⁶⁷⁸⁷ SECUNIA 17813 ⁶⁷⁸⁸	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.55.tar.gz

⁶⁷⁵⁵ <http://secunia.com/advisories/28471/>
⁶⁷⁵⁶ <http://secunia.com/advisories/28526/>
⁶⁷⁵⁷ <http://secunia.com/advisories/28607/>
⁶⁷⁵⁸ <http://secunia.com/advisories/28749/>
⁶⁷⁵⁹ <http://secunia.com/advisories/28922/>
⁶⁷⁶⁰ <http://secunia.com/advisories/28965/>
⁶⁷⁶¹ <http://secunia.com/advisories/28977/>
⁶⁷⁶² <http://secunia.com/advisories/29420/>
⁶⁷⁶³ <http://secunia.com/advisories/29504/>
⁶⁷⁶⁴ <http://secunia.com/advisories/29640/>
⁶⁷⁶⁵ <http://secunia.com/advisories/29806/>
⁶⁷⁶⁶ <http://secunia.com/advisories/29988/>
⁶⁷⁶⁷ <http://secunia.com/advisories/30356/>
⁶⁷⁶⁸ <http://secunia.com/advisories/30430/>
⁶⁷⁶⁹ <http://secunia.com/advisories/30732/>
⁶⁷⁷⁰ <http://secunia.com/advisories/31142/>
⁶⁷⁷¹ <http://secunia.com/advisories/33200/>
⁶⁷⁷² <https://www.suse.com/support/security/advisories/>
⁶⁷⁷³ <http://xforce.iss.net/xforce/xfdb/39472> pristupljeno 11.12.2011
⁶⁷⁷⁴ <http://www.securityfocus.com/bid/14106>
⁶⁷⁷⁵ <http://www.securityfocus.com/bid/15647>
⁶⁷⁷⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2088>
⁶⁷⁷⁷ <http://lists.debian.org/debian-security-announce/2005/msg00193.html>
⁶⁷⁷⁸ <https://security-tracker.debian.org/tracker/DSA-805-1>
⁶⁷⁷⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11452>
⁶⁷⁸⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1237>
⁶⁷⁸¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1526>
⁶⁷⁸² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:1629>
⁶⁷⁸³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:840>
⁶⁷⁸⁴ <http://rhn.redhat.com/errata/RHSA-2005-582.html>
⁶⁷⁸⁵ <http://secunia.com/advisories/14530/>
⁶⁷⁸⁶ <http://secunia.com/advisories/17319/>
⁶⁷⁸⁷ <http://secunia.com/advisories/17487/>

			SECUNIA 19072 ⁶⁷⁸⁹ SECUNIA 19073 ⁶⁷⁹⁰ SECUNIA 19185 ⁶⁷⁹¹ SECUNIA 19317 ⁶⁷⁹² SECUNIA 23074 ⁶⁷⁹³ SUSE SA:2005:046 ⁶⁷⁹⁴ SUSE-		
41.	OpenSSH CBC Mode Information Disclosure Vulnerability (ssh-openssh-cbc-mode-info-disclosure)	172.23.202.126:22 172.23.202.225:22 Određene verzije OpenSSH-a poseduju ranjivu implementaciju bloka šifarskog algoritma u CBC modu (Cipher Block Chaining). Ovo bi udaljenom napadaču moglo omogućiti da preko nepoznatih vektora pridobije određene podatke u vidu običnog teksta iz proizvoljnog bloka šifrovanog teksta u SSH sesiji.	BID 32319 ⁶⁷⁹⁵ CVE CVE-2008-5161 ⁶⁷⁹⁶ SECUNIA 32760 ⁶⁷⁹⁷ URL ⁶⁷⁹⁸	Ozbiljan	Uraditi download a zatim instalirati: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-5.2p1.tar.gz Verzija 5.2 OpenSSH-a je puštena u promet 22. februara 2009.
42.	OpenSSH "known_hosts" File Information Disclosure (ssh-openssh-known_hosts-file-info-leak)	172.23.202.126:22 172.23.202.225:22 Verzije OpenSSH pre 4.0 čuvale su imena hostova, IP adrese i oznake u običnom tekstu, u fajlu „known_hosts“. To može omogućiti napadaču koji poseduje kompromitovan nalog SSH korisnika da generiše listu dodatnih meta za koje postoji mogućnost da poseduju istu šifru ili ključ.	CVE CVE-2005-2666 ⁶⁷⁹⁹	Ozbiljan	Uraditi download a zatim instalirati: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-4.0p1.tar.gz Verzija 4.0 OpenSSH-a je puštena u promet 22. februara 2009. Izvorni kôd za ovaj program se može preuzeti sa ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-4.0p1.tar.gz .
43.	OpenSSH "X11UseLocalhost" X11 Forwarding Session Hijacking Vulnerability (ssh-opensshx11uselocalhost-x11-forwarding-session-hijack)	172.23.202.126:22 172.23.202.225:22 Određene verzije OpenSSH-a podešavaju SO_REUSEADDR socket opciju kada je onemogućeno podešavanje X11UseLocalhost konfiguracije. Ovo bi lokalnom napadaču moglo da omogući da preuzme X11 forwarding port preko veze ka pojedinačnoj IP adresi.	BID 30339 ⁶⁸⁰⁰ CVE CVE-2008-3259 ⁶⁸⁰¹ SECUNIA 31179 ⁶⁸⁰²	Ozbiljan	Uraditi download a zatim instalirati: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-5.1p1.tar.gz Verzija 5.1 OpenSSH-a je puštena u promet 21. jula 2008.
44.	SSH server supports SSH protocol v1 clients (ssh-v1-supported)	172.23.202.126:22 172.23.202.225:22 SSH server podržava klijente SSH verzije 1. Verzija 1 SSH protokola sadrži osnovne slabosti koje dovode do toga da su sesije ranjive na napade	CERT-VN 13877 ⁶⁸⁰³ CERT-VN 315308 ⁶⁸⁰⁴ CVE CVE-2001-1473 ⁶⁸⁰⁵ CERT-VN 684820 ⁶⁸⁰⁶	Kritičan	Potrebno je konfigurisati SSH server tako da podržava samo protokol verziju 2. Za servere bazirane na OpenSSH, izmenite liniju „Protocol“ u

⁶⁷⁸⁸ <http://secunia.com/advisories/17813/>⁶⁷⁸⁹ <http://secunia.com/advisories/19072/>⁶⁷⁹⁰ <http://secunia.com/advisories/19073/>⁶⁷⁹¹ <http://secunia.com/advisories/19185/>⁶⁷⁹² <http://secunia.com/advisories/19317/>⁶⁷⁹³ <http://secunia.com/advisories/23074/>⁶⁷⁹⁴ <https://www.suse.com/support/security/advisories/>⁶⁷⁹⁵ <http://www.securityfocus.com/bid/32319>⁶⁷⁹⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-5161>⁶⁷⁹⁷ <http://secunia.com/advisories/32760/>⁶⁷⁹⁸ <http://www.openssh.com/txt/cbc.adv>⁶⁷⁹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2666>⁶⁸⁰⁰ <http://www.securityfocus.com/bid/30339>⁶⁸⁰¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-3259>⁶⁸⁰² <http://secunia.com/advisories/31179/>⁶⁸⁰³ <http://www.kb.cert.org/vuls/id/13877>⁶⁸⁰⁴ <http://www.kb.cert.org/vuls/id/315308>⁶⁸⁰⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2001-1473>⁶⁸⁰⁶ <http://www.kb.cert.org/vuls/id/684820>

		preko posrednika. S obzirom da su svi savremeni SSH klijenti podržavali SSH v2 tokom najmanje 5 godina, ne postoji potreba da se podržava SSHv1.			fajlu sshd_config tako da piše: Protocol 2 Za sisteme koji nisu bazirani na OpenSSH, trebalo bi nadograditi verziju operativnog sistema tako da omogući SSHv2 podršku.
45.	Apache httpd mod_disk_cache stores sensitive headers (CVE-2004-1834) (apache-httpd-2_0_xmod_disk_cache-stores-sensitive-headers-cve-2004-1834)	172.23.202.126:80 172.23.202.225:80 Eksperimentalan modul mod_disk_cache je sačuvao poverljive podatke klijenta za keširane objekte, kao što su poverljivi podaci proxy autentifikacija i šifre osnovne autentifikacije na disku.	BID 9933 ⁶⁸⁰⁷ CVE CVE-2004-1834 ⁶⁸⁰⁸ OSVDB 4446 ⁶⁸⁰⁹ OVAL OVAL11133 ⁶⁸¹⁰ REDHAT RHTSA-2004:562 ⁶⁸¹¹ SECUNIA 11176 ⁶⁸¹² SECUNIA 19072 ⁶⁸¹³ URL1 ⁶⁸¹⁴	Umeren	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.53.tar.gz
46.	HTTP TRACE Method Enabled (http-trace-method-enabled)	172.23.202.126:80 172.23.202.225:80 HTTP TRACE metoda se obično koristi da uzvratu potpuni HTTP zahtev klijentu koji ga zahteva, u cilju debagovanja proxy servera. Napadač bi mogao da kreira web stranicu koristeći XMLHTTP, ActiveX ili XMLHttpRequest da natera klijenta da pošalje TRACE zahtev i da sačuva klijenove kolačiće. Kao posledica može da se javi XSS napad. Primer : 172.23.202.126:80 Running vulnerable HTTP service. http://172.23.202.126/ 1: TRACE / HTTP/1.1 2: Host: 172.23.202.126 3: Cookie: vulnerable=yes	CERT-VN 867593 ⁶⁸¹⁵ OSVDB 35511 ⁶⁸¹⁶ OSVDB 3726 ⁶⁸¹⁷ SECUNIA 10726 ⁶⁸¹⁸ SECUNIA 17334 ⁶⁸¹⁹ SECUNIA 21802 ⁶⁸²⁰ SECUNIA 25636 ⁶⁸²¹ CVE CVE-2004-2320 ⁶⁸²² CVE CVE-2004-2763 ⁶⁸²³ CVE CVE-2005-3398 ⁶⁸²⁴ CVE CVE-2006-4683 ⁶⁸²⁵ CVE CVE-2007-3008 ⁶⁸²⁶ CVE CVE-2008-7253 ⁶⁸²⁷ CVE CVE-2009-2823 ⁶⁸²⁸ CVE CVE-2010-0386 ⁶⁸²⁹ OSVDB 877 ⁶⁸³⁰ SUN 50603 ⁶⁸³¹ BID 9561 ⁶⁸³² URL1 ⁶⁸³³ URL2 ⁶⁸³⁴	Ozbiljan	Apache Onemogućiti HTTP TRACE metodu za Apache. Novije verzije Apache-a (1.3.34 i 2.0.55 i novije) omogućuju konfiguracionu direktivu koja se zove TraceEnable. Da bi se odbili TRACE zahtevi, dodaje se sledeći red u konfiguraciju servera: TraceEnable off Za starije verzije Apache web servera, koristiti modul mod_rewrite da bi se odbili TRACE zahteve: RewriteEngine On RewriteCond %{REQUEST_METHOD} ^TRACE RewriteRule .* - [F]

⁶⁸⁰⁷ <http://www.securityfocus.com/bid/9933>⁶⁸⁰⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-1834>⁶⁸⁰⁹ <http://www.osvdb.org/4446>⁶⁸¹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11133>⁶⁸¹¹ <http://rhn.redhat.com/errata/RHTSA-2004-562.html>⁶⁸¹² <http://secunia.com/advisories/11176/>⁶⁸¹³ <http://secunia.com/advisories/19072/>⁶⁸¹⁴ http://httpd.apache.org/security/vulnerabilities_20.html⁶⁸¹⁵ <http://www.kb.cert.org/vuls/id/867593>⁶⁸¹⁶ <http://www.osvdb.org/35511>⁶⁸¹⁷ <http://www.osvdb.org/3726>⁶⁸¹⁸ <http://secunia.com/advisories/10726/>⁶⁸¹⁹ <http://secunia.com/advisories/17334/>⁶⁸²⁰ <http://secunia.com/advisories/21802/>⁶⁸²¹ <http://secunia.com/advisories/25636/>⁶⁸²² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2320>⁶⁸²³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2763>⁶⁸²⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-3398>⁶⁸²⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-4683>⁶⁸²⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3008>⁶⁸²⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-7253>⁶⁸²⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2823>⁶⁸²⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0386>⁶⁸³⁰ <http://osvdb.org/887>⁶⁸³¹ <https://sunsolve.sun.com/search/document.do?assetkey=1-22-50603-1> pristupljeno 18.12.2011⁶⁸³² <http://www.securityfocus.com/bid/9561>⁶⁸³³ <http://www.apacheweek.com/issues/03-01-24#news>⁶⁸³⁴ <http://www.kb.cert.org/vuls/id/867593>

47.	Database Open Access (database-open-access)	172.23.202.126:3306 172.23.202.225:3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7.	URL ⁶⁸³⁵	Umeren	Konfigurisati server baze podataka tako da dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.
48.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatišu slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	CVE CVE-1999-0524 ⁶⁸³⁶ OSVDB 95 ⁶⁸³⁷ XF netmask(306) ⁶⁸³⁸ icmp- XF timestamp(322) ⁶⁸³⁹ icmp-	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
49.	WebDAV Extensions are Enabled (http-generic-webdav-enabled)	172.23.202.126:8080 172.23.202.225:8080 WebDAV je skup ekstenzija za HTTP protokol koji omogućava korisnicima da zajednički edituju i obrađuju fajlove na udaljenim web serverima. Mnogi web serveri po defaultu omogućavaju WebDAV ekstenzije, čak i kada nisu potrebne. S obzirom na dodatnu složenost, dosadašnja praksa je pokazala da treba onemogućiti WebDAV ukoliko se trenutno ne koristi.		Umeren	Apache: Potrebno je onemogućiti WebDAV (eng. Web-based Distributed Authoring and Versioning) za Apache. Proveriti da li je mod_dav modul isključen ili utvrditi da li postoji zahtevana autentifikacija na direktorijumima nad kojima se zahteva DAV. Apache Tomcat, Tomcat, Tomcat Web Server Onemogućiti WebDAV za Apache Tomcat. Isključiti WebDAV Servlet za sve web aplikacije koje se nalaze na web serveru. To se može uraditi tako što se ukloni definicija servlet-a za WebDAV (kategorija org.apache.catalina.servlets.WebdavServlet) i uklone sve servlet mape koje se pozivaju na WebDAV servlet.
50.	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-	172.23.202.126:80 172.23.202.225:80	APPLE APPLE-SA-2012-09-19-2 ⁶⁸⁴⁰ BID 49957 ⁶⁸⁴¹	Ozbiljan	Apache HTTPD >= 1.3 and < 2 Apply the patch for CVE-

⁶⁸³⁵ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf⁶⁸³⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁶⁸³⁷ <http://www.osvdb.org/95>⁶⁸³⁸ <http://xforce.iss.net/xforce/xfdb/306>⁶⁸³⁹ <http://xforce.iss.net/xforce/xfdb/322>⁶⁸⁴⁰ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁶⁸⁴¹ <http://www.securityfocus.com/bid/49957>

	2011-3368) (apache-httpd-cve-2011-3368)	Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja prisustva mod_proxy modula. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy. Zlonamerni napadač bi mogao da iskoristi ovaj propust na takav način da primora proxy proces da se poveže sa proizvoljnim serverom i potencijalno objavi osetljive informacije sa internih web servera koje inače napadaču nisu direktno dostupne. Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/	CVE CVE-2011-3368 ⁶⁸⁴² IAVM 2012-A-0017 ⁶⁸⁴³ IAVM 2012-A-0152 ⁶⁸⁴⁴ IAVM 2012-B-0056 ⁶⁸⁴⁵ OSVDB 76079 ⁶⁸⁴⁶ REDHAT RHSA-2011:1391 ⁶⁸⁴⁷ REDHAT RHSA-2011:1392 ⁶⁸⁴⁸ SECUNIA 46288 ⁶⁸⁴⁹ SECUNIA 46414 ⁶⁸⁵⁰ SECUNIA 48551 ⁶⁸⁵¹ XF 70336 ⁶⁸⁵² URL1 ⁶⁸⁵³ URL2 ⁶⁸⁵⁴ URL3 ⁶⁸⁵⁵		2011-3368 to 1.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ No update of 1.3 will be released. Patches will be published to http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ Apache HTTPD >= 2.0 and < 2.0.65 Upgrade to Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Upgrade to Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
51.	Apache HTTPD: scoreboard parent DoS (CVE-2012-0031) (apache-httpd-cve-2012-0031)	172.23.202.126:80 172.23.202.225:80 Propust je otkriven u obradi scoreboard-a. Neprivilegovani child proces bi mogao da dovede do toga da parent proces krahira prilikom gašenja.	APPLE APPLE-SA-2012-09-19-2 ⁶⁸⁵⁶ BID 51407 ⁶⁸⁵⁷ CVE CVE-2012-0031 ⁶⁸⁵⁸ IAVM 2012-A-0017 ⁶⁸⁵⁹ REDHAT RHSA-2012:0128 ⁶⁸⁶⁰ SECUNIA 47410 ⁶⁸⁶¹ SECUNIA 48551 ⁶⁸⁶² URL1 ⁶⁸⁶³ URL2 ⁶⁸⁶⁴	Ozbiljan	Apache HTTPD >= 1.3 and < 2 Apply the patch for CVE-2011-3368 to 1.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache

⁶⁸⁴² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3368>
⁶⁸⁴³ <http://iase.disa.mil/stigs/iavm-cve.html>
⁶⁸⁴⁴ <http://iase.disa.mil/stigs/iavm-cve.html>
⁶⁸⁴⁵ <http://iase.disa.mil/stigs/iavm-cve.html>
⁶⁸⁴⁶ <http://www.osvdb.org/76079>
⁶⁸⁴⁷ <http://rhn.redhat.com/errata/RHSA-2011-1391.html>
⁶⁸⁴⁸ <http://rhn.redhat.com/errata/RHSA-2011-1392.html>
⁶⁸⁴⁹ <http://secunia.com/advisories/46288/>
⁶⁸⁵⁰ <http://secunia.com/advisories/46414/>
⁶⁸⁵¹ <http://secunia.com/advisories/48551/>
⁶⁸⁵² <http://xforce.iss.net/xforce/xfdb/70336>
⁶⁸⁵³ http://httpd.apache.org/security/vulnerabilities_13.html
⁶⁸⁵⁴ http://httpd.apache.org/security/vulnerabilities_20.html
⁶⁸⁵⁵ http://httpd.apache.org/security/vulnerabilities_22.html
⁶⁸⁵⁶ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>
⁶⁸⁵⁷ <http://www.securityfocus.com/bid/51407>
⁶⁸⁵⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0031>
⁶⁸⁵⁹ <http://iase.disa.mil/stigs/iavm-cve.html>
⁶⁸⁶⁰ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>
⁶⁸⁶¹ <http://secunia.com/advisories/47410/>
⁶⁸⁶² <http://secunia.com/advisories/48551/>
⁶⁸⁶³ http://httpd.apache.org/security/vulnerabilities_20.html
⁶⁸⁶⁴ http://httpd.apache.org/security/vulnerabilities_22.html

					HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
52.	Apache HTTPD: mod_rewrite log escape filtering (CVE-2013-1862) (apache-httpd-cve-2013-1862)	172.23.202.126:80 172.23.202.225:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_rewrite. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Modul mod_rewrite ne filtrira završne izlazne sekvence iz logova, što zlonamenom napadaču olakšava da ubace takve sekvence u završne emulatore koji sadrže ranjivosti koje se odnose na izlazne sekvence.	CVE CVE-2013-1862⁶⁸⁶⁵ OVAL OVAL18790⁶⁸⁶⁶ REDHAT RHSA-2013:0815⁶⁸⁶⁷ REDHAT RHSA-2013:1207⁶⁸⁶⁸ REDHAT RHSA-2013:1208⁶⁸⁶⁹ REDHAT RHSA-2013:1209⁶⁸⁷⁰ SECUNIA 55032⁶⁸⁷¹ URL1⁶⁸⁷² URL2⁶⁸⁷³	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.25 Ažurirati na Apache HTTPD version 2.2.25 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.25.tar.gz
53.	Apache HTTPD: apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpdcve-2011-0419)	172.23.202.126:80 172.23.202.225:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_autoindex. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_fnmatch() u sklopu APR biblioteke. Ako je omogućen mod_autoindex, a indeksi direktorijuma mod_autoindex su sadržavali fajlove sa dovoljno dugim nazivima, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do preterane upotrebe CPU-a. Ovo bi moglo da bude iskorišćeno u napadu odbijanja servisa. Zahvaljujući Maksymilian	CVE CVE-2011-0419⁶⁸⁷⁴ DEBIAN DSA-2237⁶⁸⁷⁵ IAVM 2012-B-0056⁶⁸⁷⁶ OVAL OVAL14638⁶⁸⁷⁷ OVAL OVAL14804⁶⁸⁷⁸ REDHAT RHSA-2011:0896⁶⁸⁷⁹ REDHAT RHSA-2011:0897⁶⁸⁸⁰ REDHAT RHSA-2011:0507⁶⁸⁸¹ SECUNIA 44490⁶⁸⁸² SECUNIA 44564⁶⁸⁸³ SECUNIA 44574⁶⁸⁸⁴ URL1⁶⁸⁸⁵	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.19 Ažurirati na Apache HTTPD version 2.2.19 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.19.tar.gz

⁶⁸⁶⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1862>

⁶⁸⁶⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18790>

⁶⁸⁶⁷ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>

⁶⁸⁶⁸ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>

⁶⁸⁶⁹ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>

⁶⁸⁷⁰ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>

⁶⁸⁷¹ <http://secunia.com/advisories/55032/>

⁶⁸⁷² http://httpd.apache.org/security/vulnerabilities_20.html

⁶⁸⁷³ http://httpd.apache.org/security/vulnerabilities_22.html

⁶⁸⁷⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419>

⁶⁸⁷⁵ <http://www.debian.org/security/2011/dsa-2237>

⁶⁸⁷⁶ <http://iase.disa.mil/stigs/iavm-cve.html>

⁶⁸⁷⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14638>

⁶⁸⁷⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14804>

⁶⁸⁷⁹ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>

⁶⁸⁸⁰ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>

⁶⁸⁸¹ <http://rhn.redhat.com/errata/RHSA-2011-0507.html>

⁶⁸⁸² <http://secunia.com/advisories/44490/>

⁶⁸⁸³ <http://secunia.com/advisories/44564/>

⁶⁸⁸⁴ <http://secunia.com/advisories/44574/>

⁶⁸⁸⁵ http://httpd.apache.org/security/vulnerabilities_22.html

		Arciemowicz prijavljen je ovaj propust.			
54.	Apache HTTPD: mod_setenvif .htaccess privilege escalation (CVE-2011-3607) (apache-httpd-cve-2011-3607)	172.23.202.126:80 172.23.202.225:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_setenvif. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust preopterećenja je otkriven kada je omogućen modul mod_setenvif, što lokalnim korisnicima omogućava da dobiju privilegije preko fajla .htaccess.	APPLE APPLE-SA-2012-09-19-2 ⁶⁸⁸⁶ BID 50494 ⁶⁸⁸⁷ CVE CVE-2011-3607 ⁶⁸⁸⁸ IAVM 2012-A-0017 ⁶⁸⁸⁹ IAVM 2012-A-0152 ⁶⁸⁹⁰ OSVDB 76744 REDHAT RHSA-2012:0128 ⁶⁸⁹¹ SECUNIA 45793 ⁶⁸⁹² SECUNIA 48551 ⁶⁸⁹³ XF 71093 ⁶⁸⁹⁴ URL1 ⁶⁸⁹⁵ URL2 ⁶⁸⁹⁶	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
55.	Apache HTTPD: error responses can expose cookies (CVE-2012-0053) (apache-httpd-cve-2012-0053)	172.23.202.126:80 172.23.202.225:80 Propust je otkriven u difoltnom pogrešnom odgovoru za statusni kôd 400. Zlonamerni napadač bi mogao da iskoristi ovaj propust da objavi "httpOnly" kolačiće ako nije određen dokument custom ErrorDocument.	APPLE APPLE-SA-2012-09-19-2 ⁶⁸⁹⁷ BID 51706 ⁶⁸⁹⁸ CVE CVE-2012-0053 ⁶⁸⁹⁹ IAVM 2012-A-0017 ⁶⁹⁰⁰ REDHAT RHSA-2012:0128 ⁶⁹⁰¹ SECUNIA 48551 ⁶⁹⁰² URL1 ⁶⁹⁰³ URL2 ⁶⁹⁰⁴	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Upgrade to Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Upgrade to Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
56.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1 ⁶⁹⁰⁵ URL2 ⁶⁹⁰⁶ URL3 ⁶⁹⁰⁷	Umeren	Onemogućavanje TCP timestamp odgovora na Linux OS. Podesiti net.ipv4.tcp_timestamps vrednost na sledećem ključu na 0 pokretanjem sledeće komande: sysctl -w net.ipv4.tcp_timestamps=0 Dodatno, sledeću vrednost u difoltnom sysctl konfiguracionom fajlu, generally sysctl.conf:

⁶⁸⁸⁶ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁶⁸⁸⁷ <http://www.securityfocus.com/bid/50494>⁶⁸⁸⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3607>⁶⁸⁸⁹ <http://iase.disa.mil/stigs/iavm-cve.html>⁶⁸⁹⁰ <http://iase.disa.mil/stigs/iavm-cve.html>⁶⁸⁹¹ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁶⁸⁹² <http://secunia.com/advisories/45793/>⁶⁸⁹³ <http://secunia.com/advisories/48551/>⁶⁸⁹⁴ <http://xforce.iss.net/xforce/xfdb/71093>⁶⁸⁹⁵ http://httpd.apache.org/security/vulnerabilities_20.html⁶⁸⁹⁶ http://httpd.apache.org/security/vulnerabilities_22.html⁶⁸⁹⁷ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁶⁸⁹⁸ <http://www.securityfocus.com/bid/51706>⁶⁸⁹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0053>⁶⁹⁰⁰ <http://iase.disa.mil/stigs/iavm-cve.html>⁶⁹⁰¹ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁶⁹⁰² <http://secunia.com/advisories/48551/>⁶⁹⁰³ http://httpd.apache.org/security/vulnerabilities_20.html⁶⁹⁰⁴ http://httpd.apache.org/security/vulnerabilities_22.html⁶⁹⁰⁵ http://www.forensicswiki.org/wiki/TCP_timestamps⁶⁹⁰⁶ <http://www.ietf.org/rfc/rfc1323.txt>⁶⁹⁰⁷ <http://uptime.netcraft.com/>

					net.ipv4.tcp_timestamps=0

Tabela 126. Linux OS sa IP adresama 172.23.202.193, 172.23.202.227, 172.23.202.194, 172.23.202.226, (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.193		OS: Red Hat Enterprise Linux 5.1 x86, redhat51entx86			57
IP adresa: 172.23.202.227		OS: Red Hat Enterprise Linux 5.1 x64, redhat51entx64			57
IP adresa: 172.23.202.194		OS: Red Hat Enterprise Linux 5.2 x86, redhat52entx86			57
IP adresa: 172.23.202.226		OS: Red Hat Enterprise Linux 5.2 x64, redhat52entx64			57
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Apache httpd mod_isapi module unload flaw (CVE-2010-0425) (apache-httpd-2_2_x-mod_isapi-moduleunload-flaw-cve-2010-0425)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 U modulu mod_isapi je pronađen propust koji će pokušati da ukloni ISAPI dll kada naide na greške. To može ostaviti povratne pozive u nedefinisanom stanju greške i kao posledica može da se javi segmentation fault. Na Windows platformama koje koriste mod_isapi, udaljeni napadač bi mogao da pošalje zlonameran zahtev da pokrene ovaj problem, a kako win32 MPM pokreće samo jedan proces, to bi kao ishod imalo odbijanje servisa i potencijalno dozvolilo da se pokrene proizvoljan kôd. Napomena: Zahvaljujući Brett Gervasoni-ju iz "Sense of Security" ovaj problem je prijavljen i za njega je predložena zakrpa.	BID 38494 ⁶⁹⁰⁸ CERT-VN 280613 ⁶⁹⁰⁹ CVE CVE-2010-0425 ⁶⁹¹⁰ OVAL OVAL8439 ⁶⁹¹¹ SECUNIA 38978 ⁶⁹¹² SECUNIA 39628 ⁶⁹¹³ URL1 ⁶⁹¹⁴ XF apache-http-modisapi-ocp-unspecified(56624) ⁶⁹¹⁵	Kritičan	Apache >= 2.2 and < 2.3 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz
2.	Apache httpd APR apr_palloc heap overflow (CVE-2009-2412) (http-apache-apr_palloc-heap-overflow)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 U modulu apr_palloc() je pronađen propust u sklopu APR-a, koji može prouzrokovati velika preopterećenja u programima koji pokušaju da kontrolišu apr_palloc() veličinu	APPLE APPLE-SA-2009-11-09 ⁶⁹¹⁶ BID 35949 ⁶⁹¹⁷ CVE CVE-2009-2412 ⁶⁹¹⁸ OSVDB 56765 ⁶⁹¹⁹ OSVDB 56766 ⁶⁹²⁰ OVAL OVAL8394 ⁶⁹²¹ OVAL OVAL9958 ⁶⁹²² SECUNIA 36138 ⁶⁹²³	Kritičan	Apache >= 2.2 and < 2.3 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.13.tar.gz Apache HTTPD >= 2.0 and < 2.0.64 Ažurirati na Apache

⁶⁹⁰⁸ <http://www.securityfocus.com/bid/38494>

⁶⁹⁰⁹ <http://www.kb.cert.org/vuls/id/280613>

⁶⁹¹⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0425>

⁶⁹¹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8439>

⁶⁹¹² <http://secunia.com/advisories/38978/>

⁶⁹¹³ <http://secunia.com/advisories/39628/>

⁶⁹¹⁴ http://httpd.apache.org/security/vulnerabilities_22.html

⁶⁹¹⁵ <http://xforce.iss.net/xforce/xfdb/56624>

⁶⁹¹⁶ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>

⁶⁹¹⁷ <http://www.securityfocus.com/bid/35949>

⁶⁹¹⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2412>

⁶⁹¹⁹ <http://osvdb.org/56765>

⁶⁹²⁰ <http://osvdb.org/56766>

⁶⁹²¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8394>

⁶⁹²² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9958>

		zadate od strane korisnika. Sam Apache HTTP server ne dopušta prolaz ka ovoj funkciji neproverenim veličinama koje zadaje korisnik, tako da se on može pokrenuti samo preko neke druge aplikacije koja koristi apr_palloc() na ranjiv način.	SECUNIA 36140 ⁶⁹²⁴ SECUNIA 36166 ⁶⁹²⁵ SECUNIA 36233 ⁶⁹²⁶ SECUNIA 37152 ⁶⁹²⁷ SECUNIA 37221 ⁶⁹²⁸ SUSE SA:2009:050 ⁶⁹²⁹ URL1 ⁶⁹³⁰		HTTPD version 2.0.64 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
3.	Apache httpd mod_proxy_ftp FTP command injection (CVE-2009-3095) (apache-httpd-2_2_xmod_proxy_ftp-ftp-command-injection-cve-2009-3095)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 U modulu mod_proxy_ftp je pronađen propust. U reverznoj proxy konfiguraciji, udaljeni napadač bi mogao da iskoristi ovaj defekt da zaobiđe uobičajenu zabranu pristupa tako što bi kreirao pažljivo izrađen HTTP Authorization heder, koji omogućava napadaču da šalje proizvoljne komande FTP serveru.	APPLE APPLE-SA-2010-03-29 ⁶⁹³¹ CVE CVE-2009-3095 ⁶⁹³² DEBIAN DSA-1934 ⁶⁹³³ OVAL OVAL8662 ⁶⁹³⁴ OVAL OVAL9363 ⁶⁹³⁵ SECUNIA 37152 ⁶⁹³⁶ SUSE SA:2009:050 ⁶⁹³⁷ URL1 ⁶⁹³⁸ URL2 ⁶⁹³⁹	Kritičan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.gz Apache HTTPD >= 2.0 and < 2.0.64 Ažurirati na Apache HTTPD version 2.0.64 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
4.	Apache HTTPD: APR-util XML DoS (CVE-2009-1955) (apache-httpd-cve-2009-1955)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Ranjivost na DOS napad otkrivena je u sklopu kopije kompleta APR-util library Extensible Markup Language (XML) prevodioca (eng. parser). Udaljeni napadač bi mogao da kreira posebno izrađen XML dokument koji bi prouzrokovao ogromno zauzeće memorije kada ga procesira XML decoding engine.	APPLE APPLE-SA-2009-11-09 ⁶⁹⁴⁰ BID 35253 ⁶⁹⁴¹ CVE CVE-2009-1955 ⁶⁹⁴² DEBIAN DSA-1812 ⁶⁹⁴³ OVAL OVAL10270 ⁶⁹⁴⁴ REDHAT RHSA-2009:1107 ⁶⁹⁴⁵ REDHAT RHSA-2009:1108 ⁶⁹⁴⁶ SECUNIA 34724 ⁶⁹⁴⁷ SECUNIA 35284 ⁶⁹⁴⁸ SECUNIA 35360 ⁶⁹⁴⁹ SECUNIA 35395 ⁶⁹⁵⁰ SECUNIA 35444 ⁶⁹⁵¹ SECUNIA 35487 ⁶⁹⁵² SECUNIA 35565 ⁶⁹⁵³	Kritičan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

⁶⁹²³ <http://secunia.com/advisories/36138/>
⁶⁹²⁴ <http://secunia.com/advisories/36140/>
⁶⁹²⁵ <http://secunia.com/advisories/36166/>
⁶⁹²⁶ <http://secunia.com/advisories/36233/>
⁶⁹²⁷ <http://secunia.com/advisories/37152/>
⁶⁹²⁸ <http://secunia.com/advisories/37221/>
⁶⁹²⁹ <https://www.suse.com/support/security/advisories/>
⁶⁹³⁰ http://httpd.apache.org/security/vulnerabilities_22.html
⁶⁹³¹ <http://lists.apple.com/archives/security-announce/2010/Mar/msg00001.html>
⁶⁹³² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3095>
⁶⁹³³ <http://www.debian.org/security/DSA-/DSA-1934>
⁶⁹³⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8662>
⁶⁹³⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9363>
⁶⁹³⁶ <http://secunia.com/advisories/37152/>
⁶⁹³⁷ <https://www.suse.com/support/security/advisories/>
⁶⁹³⁸ http://httpd.apache.org/security/vulnerabilities_22.html
⁶⁹³⁹ http://httpd.apache.org/security/vulnerabilities_20.html
⁶⁹⁴⁰ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>
⁶⁹⁴¹ <http://www.securityfocus.com/bid/35253>
⁶⁹⁴² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1955>
⁶⁹⁴³ <http://lists.debian.org/debian-security-announce/2009/msg00124.html>
⁶⁹⁴⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10270>
⁶⁹⁴⁵ <http://rhn.redhat.com/errata/RHSA-2009-1107.html>
⁶⁹⁴⁶ <http://rhn.redhat.com/errata/RHSA-2009-1108.html>
⁶⁹⁴⁷ <http://secunia.com/advisories/34724/>
⁶⁹⁴⁸ <http://secunia.com/advisories/35284/>
⁶⁹⁴⁹ <http://secunia.com/advisories/35360/>
⁶⁹⁵⁰ <http://secunia.com/advisories/35395/>
⁶⁹⁵¹ <http://secunia.com/advisories/35444/>
⁶⁹⁵² <http://secunia.com/advisories/35487/>
⁶⁹⁵³ <http://secunia.com/advisories/35565/>

			SECUNIA 35710 ⁶⁹⁵⁴ SECUNIA 35797 ⁶⁹⁵⁵ SECUNIA 35843 ⁶⁹⁵⁶ SECUNIA 36473 ⁶⁹⁵⁷ SECUNIA 37221 ⁶⁹⁵⁸ URL1 ⁶⁹⁵⁹		
5.	OpenSSH X11 Cookie Local Authentication Bypass Vulnerability (openssh-x11-cookie-auth-bypass)	172.23.202.193:22 172.23.202.194:22 172.23.202.226:22 172.23.202.227:22 Pre verzije 4.7, OpenSSH nije adekvatno radio kada nepoverljivi kolačić (cookie) nije mogao biti kreiran. Umesto njega, koristi se poverljivi X11 kolačić. To omogućava napadačima da naruše ciljanu politiku i dobiju privilegije korisnika, što kao posledicu servis tretira klijenta X kao poverljivog.	CVE CVE-2007-4752 ⁶⁹⁶⁰ XFD 25628 ⁶⁹⁶¹ XF openssh-x11cookie-privilege-escalation(36637) ⁶⁹⁶²	Kritičan	Uraditi download a zatim instalirati: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-4.7p1.tar.gz Verzija 4.7 of OpenSSH je puštena u promet 4. septembra 2007.
6.	Apache httpd mod_deflate DoS (CVE-2009-1891) (apache-httpd-cve-2009-1891)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Ranjivost na DOS napad otkrivena je u modulu mod_deflate. Ovaj modul nastavlja da kompresuje velike fajlove sve dok se kompresija ne završi, čak i kada je mrežna konekcija koja je zahtevala taj sadržaj prekinuta pre nego što je kompresija završena. To dovodi do toga da mod_deflate zauzima veliku količinu CPU-a ukoliko je mod_deflate bio omogućen za velike fajlove.	APPLE APPLE-SA-2009-11-09 ⁶⁹⁶³ CVE CVE-2009-1891 ⁶⁹⁶⁴ DEBIAN DSA-1834 ⁶⁹⁶⁵ OSVDB 55782 ⁶⁹⁶⁶ OVAL OVAL8632 ⁶⁹⁶⁷ OVAL OVAL9248 ⁶⁹⁶⁸ OVAL OVAL12361 ⁶⁹⁶⁹ REDHAT RHSA-2009-1148 ⁶⁹⁷⁰ REDHAT RHSA-2009-1156 ⁶⁹⁷¹ SECUNIA 35721 ⁶⁹⁷² SECUNIA 35781 ⁶⁹⁷³ SECUNIA 35793 ⁶⁹⁷⁴ SECUNIA 35865 ⁶⁹⁷⁵ SECUNIA 37152 ⁶⁹⁷⁶ SECUNIA 37221 ⁶⁹⁷⁷ SUSE SUSE-SA:2009:050 ⁶⁹⁷⁸ URL1 ⁶⁹⁷⁹	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.12 Ažurirati na Apache HTTPD version 2.2.12 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

⁶⁹⁵⁴ <http://secunia.com/advisories/35710/>⁶⁹⁵⁵ <http://secunia.com/advisories/35797/>⁶⁹⁵⁶ <http://secunia.com/advisories/35843/>⁶⁹⁵⁷ <http://secunia.com/advisories/36473/>⁶⁹⁵⁸ <http://secunia.com/advisories/37221/>⁶⁹⁵⁹ http://httpd.apache.org/security/vulnerabilities_22.html⁶⁹⁶⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-4752>⁶⁹⁶¹ <http://www.securityfocus.com/bid/25628>⁶⁹⁶² <http://xforce.iss.net/xforce/xfdb/36637>⁶⁹⁶³ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>⁶⁹⁶⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1891>⁶⁹⁶⁵ <http://www.debian.org/security/DSA-/DSA-1834> pristupljeno 18.12.2011⁶⁹⁶⁶ <http://osvdb.org/55782>⁶⁹⁶⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8632>⁶⁹⁶⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9248>⁶⁹⁶⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12361>⁶⁹⁷⁰ <http://rhn.redhat.com/errata/RHSA-2009-1148.html>⁶⁹⁷¹ <http://rhn.redhat.com/errata/RHSA-2009-1156.html>⁶⁹⁷² <http://secunia.com/advisories/35721/>⁶⁹⁷³ <http://secunia.com/advisories/35781/>⁶⁹⁷⁴ <http://secunia.com/advisories/35793/>⁶⁹⁷⁵ <http://secunia.com/advisories/35865/>⁶⁹⁷⁶ <http://secunia.com/advisories/37152/>⁶⁹⁷⁷ <http://secunia.com/advisories/37221/>⁶⁹⁷⁸ <https://www.suse.com/support/security/advisories/>⁶⁹⁷⁹ http://httpd.apache.org/security/vulnerabilities_20.html

7.	Apache httpd mod_proxy reverse proxy DoS (CVE-2009-1890) (http-apache-mod_proxy-reverse-proxy-dos)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja prisustva mod_proxy modula. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy. Zlonamerni napadač bi mogao da iskoristi ovaj propust na takav način da primora proxy proces da zauzme veliku količinu CPU vremena.	APPLE APPLE-SA-2009-11-09 ⁶⁹⁸⁰ CVE CVE-2009-1890 ⁶⁹⁸¹ DEBIAN DSA-1834 ⁶⁹⁸² OSVDB 55553 ⁶⁹⁸³ OVAL OVAL12330 ⁶⁹⁸⁴ OVAL OVAL8616 ⁶⁹⁸⁵ OVAL OVAL9403 ⁶⁹⁸⁶ REDHAT RHSA-2009:1148 ⁶⁹⁸⁷ REDHAT RHSA-2009:1156 ⁶⁹⁸⁸ SECUNIA 35691 ⁶⁹⁸⁹ SECUNIA 35721 ⁶⁹⁹⁰ SECUNIA 35793 ⁶⁹⁹¹ SECUNIA 35865 ⁶⁹⁹² SECUNIA 37152 ⁶⁹⁹³ SECUNIA 37221 ⁶⁹⁹⁴ SUSE SA:2009:050 ⁶⁹⁹⁵ URL1 ⁶⁹⁹⁶	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz
8.	Apache HTTPD: APR-util off-by-one overflow (CVE-2009-1956) (apache-httpd-cve-2009-1956)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Propust prepunjavanja bafera "off-by-one" je otkriven u načinu na koji APR-util library komplet procesira promenljivu listu argumenata. Napadač bi mogao da kreira posebno izrađen string kao input za već formatiranu output rutu konverzije, koja bi, na velikim platformama, potencijalno mogla da dovede do otkrivanja povreljivih informacija ili do odbijanja servisa.	APPLE APPLE-SA-2009-11-09 ⁶⁹⁹⁷ BID 35251 ⁶⁹⁹⁸ CVE CVE-2009-1956 ⁶⁹⁹⁹ OVAL OVAL11567 ⁷⁰⁰⁰ OVAL OVAL12237 ⁷⁰⁰¹ REDHAT RHSA-2009:1107 ⁷⁰⁰² REDHAT RHSA-2009:1108 ⁷⁰⁰³ SECUNIA 34724 ⁷⁰⁰⁴ SECUNIA 35284 ⁷⁰⁰⁵ SECUNIA 35395 ⁷⁰⁰⁶ SECUNIA 35487 ⁷⁰⁰⁷ SECUNIA 35565 ⁷⁰⁰⁸ SECUNIA 35710 ⁷⁰⁰⁹ SECUNIA 35797 ⁷⁰¹⁰	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

⁶⁹⁸⁰ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>⁶⁹⁸¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1890>⁶⁹⁸² <http://www.debian.org/security/2009/dsa-1834>⁶⁹⁸³ <http://osvdb.org/55553>⁶⁹⁸⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12330>⁶⁹⁸⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8616>⁶⁹⁸⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9403>⁶⁹⁸⁷ <http://rhn.redhat.com/errata/RHSA-2009-1148.html>⁶⁹⁸⁸ <http://rhn.redhat.com/errata/RHSA-2009-1156.html>⁶⁹⁸⁹ <http://secunia.com/advisories/35691/>⁶⁹⁹⁰ <http://secunia.com/advisories/35721/>⁶⁹⁹¹ <http://secunia.com/advisories/35793/>⁶⁹⁹² <http://secunia.com/advisories/35865/>⁶⁹⁹³ <http://secunia.com/advisories/37152/>⁶⁹⁹⁴ <http://secunia.com/advisories/37221/>⁶⁹⁹⁵ <https://www.suse.com/support/security/advisories/>⁶⁹⁹⁶ http://httpd.apache.org/security/vulnerabilities_22.html⁶⁹⁹⁷ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>⁶⁹⁹⁸ <http://www.securityfocus.com/bid/35251>⁶⁹⁹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1956>⁷⁰⁰⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11567>⁷⁰⁰¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12237>⁷⁰⁰² <http://rhn.redhat.com/errata/RHSA-2009-1107.html>⁷⁰⁰³ <http://rhn.redhat.com/errata/RHSA-2009-1108.html>⁷⁰⁰⁴ <http://secunia.com/advisories/34724/>⁷⁰⁰⁵ <http://secunia.com/advisories/35284/>⁷⁰⁰⁶ <http://secunia.com/advisories/35395/>⁷⁰⁰⁷ <http://secunia.com/advisories/35487/>⁷⁰⁰⁸ <http://secunia.com/advisories/35565/>⁷⁰⁰⁹ <http://secunia.com/advisories/35710/>⁷⁰¹⁰ <http://secunia.com/advisories/35797/>

			SECUNIA 35843 ⁷⁰¹¹ SECUNIA 37221 ⁷⁰¹² URL1 ⁷⁰¹³		
9.	OpenSSH X11 Forwarding Information Disclosure Vulnerability (ssh-openssh-x11-forwarding-info-disclosure)	172.23.202.193:22 172.23.202.194:22 172.23.202.226:22 172.23.202.227:22 Određene verzije OpenSSH-a ne povezuju ispravno TCP portove na lokalnom IPv6 interfejsu ako se koriste zahtevani IPv4 portovi. Ovo bi loklanom napadaču moglo da omogućiti da preuzme prosledenu X11 sesiju putem otvaranja TCP port-a 6010 (IPv4).	BID 28444 ⁷⁰¹⁴ CVE CVE-2008-1483 ⁷⁰¹⁵ SECUNIA 29522 ⁷⁰¹⁶ URL1 ⁷⁰¹⁷	Ozbiljan	Nadograditi na najnoviju verziju OpenSSH-a. Najnovija verzija OpenSSH-a je 5.2 (OpenBSD izvor) i 5.2p1 (prenosivi izvor).
10.	Apache HTTPD: expat DoS (CVE-2009-3560) (apache-httpd-cve-2009-3560)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u mogućnosti da dovede do toga da Apache parsira nepoverljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	BID 37203 ⁷⁰¹⁸ CVE CVE-2009-3560 ⁷⁰¹⁹ DEBIAN DSA-1953 ⁷⁰²⁰ IAVM 2012-A-0020 ⁷⁰²¹ OVAL OVAL12942 ⁷⁰²² REDHAT RHSA-2011-0896 ⁷⁰²³ OVAL OVAL10613 ⁷⁰²⁴ OVAL OVAL6883 ⁷⁰²⁵ SECUNIA 37537 ⁷⁰²⁶ SECUNIA 38231 ⁷⁰²⁷ SECUNIA 38794 ⁷⁰²⁸ SECUNIA 38832 ⁷⁰²⁹ SECUNIA 38834 ⁷⁰³⁰ SECUNIA 39478 ⁷⁰³¹ SECUNIA 41701 ⁷⁰³² SECUNIA 43300 ⁷⁰³³ URL1 ⁷⁰³⁴	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.17 Ažurirati na Apache HTTPD version 2.2.17 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
11.	Apache HTTPD: expat DoS (CVE-2009-3720) (apache-httpd-cve-2009-3720)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu	AVM 2012-A-0020 ⁷⁰³⁵ OVAL OVAL12719 ⁷⁰³⁶ REDHAT RHSA-2011-0896 ⁷⁰³⁷ CVE CVE-2009-3720 ⁷⁰³⁸	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz

⁷⁰¹¹ <http://secunia.com/advisories/35843/>⁷⁰¹² <http://secunia.com/advisories/37221/>⁷⁰¹³ http://httpd.apache.org/security/vulnerabilities_22.html⁷⁰¹⁴ <http://www.securityfocus.com/bid/28444>⁷⁰¹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-1483>⁷⁰¹⁶ <http://secunia.com/advisories/29522/>⁷⁰¹⁷ <http://www.openssh.org/txt/release-5.0>⁷⁰¹⁸ <http://www.securityfocus.com/bid/37203>⁷⁰¹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3560>⁷⁰²⁰ <http://www.debian.org/security/DSA-/DSA-1953> pristupljeno dana 18.12.2011⁷⁰²¹ <http://iase.disa.mil/stigs/iavm-cve.html>⁷⁰²² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12942>⁷⁰²³ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁷⁰²⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10613>⁷⁰²⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6883>⁷⁰²⁶ <http://secunia.com/advisories/37537/>⁷⁰²⁷ <http://secunia.com/advisories/38231/>⁷⁰²⁸ <http://secunia.com/advisories/38794/>⁷⁰²⁹ <http://secunia.com/advisories/38832/>⁷⁰³⁰ <http://secunia.com/advisories/38834/>⁷⁰³¹ <http://secunia.com/advisories/39478/>⁷⁰³² <http://secunia.com/advisories/41701/>⁷⁰³³ <http://secunia.com/advisories/43300/>⁷⁰³⁴ http://httpd.apache.org/security/vulnerabilities_20.html⁷⁰³⁵ <http://iase.disa.mil/stigs/iavm-cve.html>⁷⁰³⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12719>⁷⁰³⁷ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>

		ranjivost SAMO ako je napadač u mogućnosti da dovede do toga da Apache parsira nepoverljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	OVAL OVAL11019 ⁷⁰³⁹ OVAL OVAL7112 ⁷⁰⁴⁰ REDHAT RHSA-2010:0002 ⁷⁰⁴¹ SECUNIA 37324 ⁷⁰⁴² SECUNIA 37537 ⁷⁰⁴³ SECUNIA 37925 ⁷⁰⁴⁴ SECUNIA 38050 ⁷⁰⁴⁵ SECUNIA 38231 ⁷⁰⁴⁶ SECUNIA 38794 ⁷⁰⁴⁷ SECUNIA 38832 ⁷⁰⁴⁸ SECUNIA 38834 ⁷⁰⁴⁹ SECUNIA 39478 ⁷⁰⁵⁰ SECUNIA 41701 ⁷⁰⁵¹ SECUNIA 43300 ⁷⁰⁵² URL1 7053 		Apache HTTPD >= 2.2 and < 2.2.17 Ažurirati na Apache HTTPD version 2.2.17 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
12.	Apache HTTPD: apr_bridage_split_line DoS (CVE-2010-1623) (apache-httpd-cve-2010-1623)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako Apache procesira ne-SSL zahteve. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_brigade_split_line() u sklopu kompleta APR-util library, koji se koristi za procesiranje ne-SSL zahteva. Udaljeni napadač bi mogao da šalje zahteve, pažljivo izrađujući tajming za pojedinačne bajtove, što bi polako zauzimalo memoriju i potencijalno dovelo do odbijanja servisa.	IAVM 2012-B-0056 ⁷⁰⁵⁴ OVAL OVAL12800 ⁷⁰⁵⁵ REDHAT RHSA-2011:0896 ⁷⁰⁵⁶ REDHAT RHSA-2011:0897 ⁷⁰⁵⁷ BID 43673 ⁷⁰⁵⁸ CVE CVE-2010-1623 ⁷⁰⁵⁹ REDHAT RHSA-2010:0950 ⁷⁰⁶⁰ SECUNIA 41701 ⁷⁰⁶¹ SECUNIA 42015 ⁷⁰⁶² SECUNIA 42361 ⁷⁰⁶³ SECUNIA 42367 ⁷⁰⁶⁴ SECUNIA 42403 ⁷⁰⁶⁵ SECUNIA 42537 ⁷⁰⁶⁶ SECUNIA 43211 ⁷⁰⁶⁷ SECUNIA 43285 ⁷⁰⁶⁸ URL1 7069 	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.17 Ažurirati na Apache HTTPD version 2.2.17 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz

⁷⁰³⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3720>
⁷⁰³⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11019>
⁷⁰⁴⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7112>
⁷⁰⁴¹ <http://rhn.redhat.com/errata/RHSA-2010-0002.html>
⁷⁰⁴² <http://secunia.com/advisories/37324/>
⁷⁰⁴³ <http://secunia.com/advisories/37537/>
⁷⁰⁴⁴ <http://secunia.com/advisories/37925/>
⁷⁰⁴⁵ <http://secunia.com/advisories/38050/>
⁷⁰⁴⁶ <http://secunia.com/advisories/38231/>
⁷⁰⁴⁷ <http://secunia.com/advisories/38794/>
⁷⁰⁴⁸ <http://secunia.com/advisories/38832/>
⁷⁰⁴⁹ <http://secunia.com/advisories/38834/>
⁷⁰⁵⁰ <http://secunia.com/advisories/39478/>
⁷⁰⁵¹ <http://secunia.com/advisories/41701/>
⁷⁰⁵² <http://secunia.com/advisories/43300/>
⁷⁰⁵³ http://httpd.apache.org/security/vulnerabilities_20.html
⁷⁰⁵⁴ <http://iase.disa.mil/stigs/iavm-cve.html>
⁷⁰⁵⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12800>
⁷⁰⁵⁶ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>
⁷⁰⁵⁷ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>
⁷⁰⁵⁸ <http://www.securityfocus.com/bid/43673>
⁷⁰⁵⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1623>
⁷⁰⁶⁰ <http://rhn.redhat.com/errata/RHSA-2010-0950.html>
⁷⁰⁶¹ <http://secunia.com/advisories/41701/>
⁷⁰⁶² <http://secunia.com/advisories/42015/>
⁷⁰⁶³ <http://secunia.com/advisories/42361/>
⁷⁰⁶⁴ <http://secunia.com/advisories/42367/>
⁷⁰⁶⁵ <http://secunia.com/advisories/42403/>
⁷⁰⁶⁶ <http://secunia.com/advisories/42537/>
⁷⁰⁶⁷ <http://secunia.com/advisories/43211/>
⁷⁰⁶⁸ <http://secunia.com/advisories/43285/>
⁷⁰⁶⁹ http://httpd.apache.org/security/vulnerabilities_20.html

13.	Apache HTTPD: mod_dav DoS (CVE-2010-1452) (apache-httpd-cve-2010-1452)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako web server izvršava jedan od sledećih modula: mod_cache, mod_dav. Pregledajte konfiguraciju vašeg web servera radi validacije. Propust je otkriven u obradi zahteva od strane mod_cache i mod_dav. Zlonameran udaljeni napadač bi mogao da pošalje pažljivo izrađen zahtev i prouzrokuje da httpd child proces krahira. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM. Ovaj problem se dalje može ublažiti ako na mod_dav samo utiču zahtevi za koje postoji mogućnost autentifikovanja, a mod_cache je pod uticajem samo ako se koristi neuobičajena „CacheIgnoreURLSessionIdentifiers“ direktiva, uvedena u verziji 2.2.14. Ovaj problem je prijavio Mark Drayton.	IAVM 2012-B-0056 ⁷⁰⁷⁰ OVAL OVAL12341 ⁷⁰⁷¹ REDHAT RHSA-2011:0896 ⁷⁰⁷² REDHAT RHSA-2011:0897 ⁷⁰⁷³ APPLE APPLE-SA-2011-03-21 ⁷⁰⁷⁴ CVE CVE-2010-1452 ⁷⁰⁷⁵ OVAL OVAL11683 ⁷⁰⁷⁶ REDHAT RHSA-2010:0659 ⁷⁰⁷⁷ SECUNIA 42367 ⁷⁰⁷⁸ URL1 ⁷⁰⁷⁹	Ozbiljan	Apache >= 2.0 and < 2.1 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.16 Ažurirati na Apache HTTPD version 2.2.16 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.16.tar.gz
14.	Apache HTTPD: mod_proxy crash (CVE-2007-3847) (apache-httpd-cve-2007-3847)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja prisustva mod_proxy modula. Propust je otkriven u modulu mod_proxy Apache HTTP servera. Na sajtovima na kojima je konfigurisan reverzni proxy, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do toga da Apache child proces, koji obrađuje taj zahtev krahira. Na sajtovima na kojima je konfigurisan "forward proxy", napadač bi mogao da izazove	APPLE APPLE-SA-2008-03-18 ⁷⁰⁸⁰ APPLE APPLE-SA-2008-05-28 ⁷⁰⁸¹ CERT TA08-150A ⁷⁰⁸³ CVE CVE-2007-3847 ⁷⁰⁸⁴ OVAL OVAL10525 ⁷⁰⁸⁵ REDHAT RHSA-2007:0746 ⁷⁰⁸⁶ REDHAT RHSA-2007:0747 ⁷⁰⁸⁷ REDHAT RHSA-2007:0911 ⁷⁰⁸⁸ REDHAT RHSA-2008:0005 ⁷⁰⁸⁹ SECUNIA 26636 ⁷⁰⁹⁰ SECUNIA 26722 ⁷⁰⁹¹ SECUNIA 26790 ⁷⁰⁹²	Ozbiljan	Apache >= 2.0 and < 2.1 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.61.tar.gz Apache HTTPD >= 2.2 and < 2.2.6 Upgrade to Apache HTTPD version 2.2.6 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz

⁷⁰⁷⁰ <http://iase.disa.mil/stigs/iavm-cve.html>⁷⁰⁷¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12341>⁷⁰⁷² <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁷⁰⁷³ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>⁷⁰⁷⁴ <http://lists.apple.com/archives/security-announce/2011/Mar/msg00006.html>⁷⁰⁷⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1452>⁷⁰⁷⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11683>⁷⁰⁷⁷ <http://rhn.redhat.com/errata/RHSA-2010-0659.html>⁷⁰⁷⁸ <http://secunia.com/advisories/42367/>⁷⁰⁷⁹ http://httpd.apache.org/security/vulnerabilities_20.html⁷⁰⁸⁰ <http://lists.apple.com/archives/security-announce/2008/Mar/msg00000.html>⁷⁰⁸¹ <http://lists.apple.com/archives/security-announce/2008/May/msg00001.html>⁷⁰⁸² <http://www.securityfocus.com/bid/25489> pristupljeno 18.12.2011⁷⁰⁸³ <http://www.cert.org/advisories/TA08-150A.html> pristupljeno 18.12.2011⁷⁰⁸⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3847>⁷⁰⁸⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10525>⁷⁰⁸⁶ <http://rhn.redhat.com/errata/RHSA-2007-0746.html>⁷⁰⁸⁷ <http://rhn.redhat.com/errata/RHSA-2007-0747.html>⁷⁰⁸⁸ <http://rhn.redhat.com/errata/RHSA-2007-0911.html>⁷⁰⁸⁹ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>⁷⁰⁹⁰ <http://secunia.com/advisories/26636/>⁷⁰⁹¹ <http://secunia.com/advisories/26722/>

		sličan krah ukoliko bi korisnik bio primoran da poseti zlonameran sajt koristeći proxy. To može dovesti samo do odbijanja servisa ako se koristi threaded MPM.	SECUNIA 26842 ⁷⁰⁹³ SECUNIA 26952 ⁷⁰⁹⁴ SECUNIA 26993 ⁷⁰⁹⁵ SECUNIA 27209 ⁷⁰⁹⁶ SECUNIA 27563 ⁷⁰⁹⁷ SECUNIA 27593 ⁷⁰⁹⁸ SECUNIA 27732 ⁷⁰⁹⁹ SECUNIA 27882 ⁷¹⁰⁰ SECUNIA 27971 ⁷¹⁰¹ SECUNIA 28467 ⁷¹⁰² SECUNIA 28606 ⁷¹⁰³ SECUNIA 28749 ⁷¹⁰⁴ SECUNIA 28922 ⁷¹⁰⁵ SECUNIA 29420 ⁷¹⁰⁶ SECUNIA 30430 ⁷¹⁰⁷ SUSE SA:2007:061 ⁷¹⁰⁸ URL1 ⁷¹⁰⁹		
15.	Apache HTTPD: mod_proxy_http DoS (CVE-2008-2364) (apache-httpd-cve-2008-2364)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Otkriven je propust prilikom obrade prekomernih privremenih odgovora sa glavnog servera kada se koristi mod_proxy_http. Udaljeni napadač bi mogao da izazove odbijanje servisa ili preopterećenje memorije.	BID 29653 ⁷¹¹⁰ BID 31681 ⁷¹¹¹ CVE CVE-2008-2364 ⁷¹¹² OVAL OVAL11713 ⁷¹¹³ OVAL OVAL6084 ⁷¹¹⁴ OVAL OVAL9577 ⁷¹¹⁵ REDHAT RHSA-2008:0966 ⁷¹¹⁶ REDHAT RHSA-2008:0967 ⁷¹¹⁷ SECUNIA 30621 ⁷¹¹⁸ SECUNIA 31026 ⁷¹¹⁹ SECUNIA 31404 ⁷¹²⁰ SECUNIA 31416 ⁷¹²¹ SECUNIA 31651 ⁷¹²² SECUNIA 31904 ⁷¹²³ SECUNIA 32222 ⁷¹²⁴ SECUNIA 32685 ⁷¹²⁵	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.9 Ažurirati na Apache HTTPD version 2.2.9 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.9.tar.gz

⁷⁰⁹² <http://secunia.com/advisories/26790/>⁷⁰⁹³ <http://secunia.com/advisories/26842/>⁷⁰⁹⁴ <http://secunia.com/advisories/26952/>⁷⁰⁹⁵ <http://secunia.com/advisories/26993/>⁷⁰⁹⁶ <http://secunia.com/advisories/27209/>⁷⁰⁹⁷ <http://secunia.com/advisories/27563/>⁷⁰⁹⁸ <http://secunia.com/advisories/27593/>⁷⁰⁹⁹ <http://secunia.com/advisories/27732/>⁷¹⁰⁰ <http://secunia.com/advisories/27882/>⁷¹⁰¹ <http://secunia.com/advisories/27971/>⁷¹⁰² <http://secunia.com/advisories/28467/>⁷¹⁰³ <http://secunia.com/advisories/28606/>⁷¹⁰⁴ <http://secunia.com/advisories/28749/>⁷¹⁰⁵ <http://secunia.com/advisories/28922/>⁷¹⁰⁶ <http://secunia.com/advisories/29420/>⁷¹⁰⁷ <http://secunia.com/advisories/30430/>⁷¹⁰⁸ <https://www.suse.com/support/security/advisories/>⁷¹⁰⁹ http://httpd.apache.org/security/vulnerabilities_20.html⁷¹¹⁰ <http://www.securityfocus.com/bid/29653>⁷¹¹¹ <http://www.securityfocus.com/bid/31681>⁷¹¹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-2364>⁷¹¹³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11713>⁷¹¹⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6084>⁷¹¹⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9577>⁷¹¹⁶ <http://rhn.redhat.com/errata/RHSA-2008-0966.html>⁷¹¹⁷ <http://rhn.redhat.com/errata/RHSA-2008-0967.html>⁷¹¹⁸ <http://secunia.com/advisories/30621/>⁷¹¹⁹ <http://secunia.com/advisories/31026/>⁷¹²⁰ <http://secunia.com/advisories/31404/>⁷¹²¹ <http://secunia.com/advisories/31416/>⁷¹²² <http://secunia.com/advisories/31651/>⁷¹²³ <http://secunia.com/advisories/31904/>⁷¹²⁴ <http://secunia.com/advisories/32222/>⁷¹²⁵ <http://secunia.com/advisories/32685/>

			SECUNIA 32838 ⁷¹²⁶ SECUNIA 33156 ⁷¹²⁷ SECUNIA 33797 ⁷¹²⁸ SECUNIA 34219 ⁷¹²⁹ SECUNIA 34259 ⁷¹³⁰ SECUNIA 34418 ⁷¹³¹ XF apache-modproxy-module-dos(42987) ⁷¹³² URL1 ⁷¹³³		
16.	Apache HTTPD: Signals to arbitrary processes (CVE-2007-3304) (apache-httpd-cve-2007-3304)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Pre nego što mu je poslao signale, Apache HTTP server nije overio da li proces potiče od Apache-ovog child procesa. Lokalni napadač koji ima mogućnost da pokreće skripte na HTTP serveru, mogao bi da manipuliše semaforom za signale i da prouzrokuje okončanje proizvoljnog procesa, što bi moglo da dovede do odbijanja servisa.	BID 24215 ⁷¹³⁴ CVE CVE-2007-3304 ⁷¹³⁵ OSVDB 38939 ⁷¹³⁶ OVAL OVAL11589 ⁷¹³⁷ REDHAT RHSA-2007:0532 ⁷¹³⁸ REDHAT RHSA-2007:0556 ⁷¹³⁹ REDHAT RHSA-2007:0557 ⁷¹⁴⁰ REDHAT RHSA-2007:0662 ⁷¹⁴¹ REDHAT RHSA-2008:0261 ⁷¹⁴² SECUNIA 25827 ⁷¹⁴³ SECUNIA 25830 ⁷¹⁴⁴ SECUNIA 25920 ⁷¹⁴⁵ SECUNIA 26211 ⁷¹⁴⁶ SECUNIA 26273 ⁷¹⁴⁷ SECUNIA 26443 ⁷¹⁴⁸ SECUNIA 26508 ⁷¹⁴⁹ SECUNIA 26611 ⁷¹⁵⁰ SECUNIA 26759 ⁷¹⁵¹ SECUNIA 26790 ⁷¹⁵² SECUNIA 26822 ⁷¹⁵³ SECUNIA 26842 ⁷¹⁵⁴ SECUNIA 26993 ⁷¹⁵⁵ SECUNIA 27121 ⁷¹⁵⁶ SECUNIA 27209 ⁷¹⁵⁷	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.61.tar.gz Apache HTTPD >= 1.3 and < 1.3.39 Ažurirati na Apache HTTPD version 1.3.39 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/apache-1.3.39.tar.gz Apache HTTPD >= 2.2 and < 2.2.6 Ažurirati na Apache HTTPD version 2.2.6 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz

⁷¹²⁶ <http://secunia.com/advisories/32838/>⁷¹²⁷ <http://secunia.com/advisories/33156/>⁷¹²⁸ <http://secunia.com/advisories/33797/>⁷¹²⁹ <http://secunia.com/advisories/34219/>⁷¹³⁰ <http://secunia.com/advisories/34259/>⁷¹³¹ <http://secunia.com/advisories/34418/>⁷¹³² <http://xforce.iss.net/xforce/xfdb/42987>⁷¹³³ http://httpd.apache.org/security/vulnerabilities_20.html⁷¹³⁴ <http://www.securityfocus.com/bid/24215>⁷¹³⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3304>⁷¹³⁶ <http://www.osvdb.org/38939>⁷¹³⁷ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval:def:11589>⁷¹³⁸ <http://rhn.redhat.com/errata/RHSA-2007-0532.html>⁷¹³⁹ <http://rhn.redhat.com/errata/RHSA-2007-0556.html>⁷¹⁴⁰ <http://rhn.redhat.com/errata/RHSA-2007-0557.html>⁷¹⁴¹ <http://rhn.redhat.com/errata/RHSA-2007-0662.html>⁷¹⁴² <http://rhn.redhat.com/errata/RHSA-2008-0261.html>⁷¹⁴³ <http://secunia.com/advisories/25827/>⁷¹⁴⁴ <http://secunia.com/advisories/25830/>⁷¹⁴⁵ <http://secunia.com/advisories/25920/>⁷¹⁴⁶ <http://secunia.com/advisories/26211/>⁷¹⁴⁷ <http://secunia.com/advisories/26273/>⁷¹⁴⁸ <http://secunia.com/advisories/26443/>⁷¹⁴⁹ <http://secunia.com/advisories/26508/>⁷¹⁵⁰ <http://secunia.com/advisories/26611/>⁷¹⁵¹ <http://secunia.com/advisories/26759/>⁷¹⁵² <http://secunia.com/advisories/26790/>⁷¹⁵³ <http://secunia.com/advisories/26822/>⁷¹⁵⁴ <http://secunia.com/advisories/26842/>⁷¹⁵⁵ <http://secunia.com/advisories/26993/>⁷¹⁵⁶ <http://secunia.com/advisories/27121/>⁷¹⁵⁷ <http://secunia.com/advisories/27209/>

			SECUNIA 27563 ⁷¹⁵⁸ SECUNIA 27732 ⁷¹⁵⁹ SECUNIA 28212 ⁷¹⁶⁰ SECUNIA 28224 ⁷¹⁶¹ SECUNIA 28606 ⁷¹⁶² SGI 20070701-01-P ⁷¹⁶³ SUSE SA:2007:061 ⁷¹⁶⁴ XF apache-child-process-dos(35095) ⁷¹⁶⁵ URL1 ⁷¹⁶⁶		
17.	FTP access with ftp account (ftp-generic-0001)	172.23.202.193:21 172.23.202.194:21 172.23.202.226:21 172.23.202.227:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisnikovim ID-jem (identifikacijom) "ftp" i šifrom "ftp". Dosadašnja praksa je pokazala da je najbolje ukloniti difoltnu naloge, ukoliko je to moguće. Za naloge koje sistem zahteva treba izmeniti difoltnu šifru.	CVE CVE-1999-0497 ⁷¹⁶⁷	Ozbiljan	Ukloniti ili onemogućiti nalog, ukoliko to nije kritično za funkcionisanje sistema. U suprotnom, lozinku treba promeniti u onu koja nije po difoltu.
18.	FTP access with anonymous account (ftp-generic-0002)	172.23.202.193:21 172.23.202.194:21 172.23.202.226:21 172.23.202.227:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisnikovim ID-jem (identifikacijom) "anonymous" i lozinkom "ftp@". Dosadašnja praksa je pokazala da je najbolje ukloniti difoltnu naloge, ukoliko je to moguće. Za naloge koje sistem zahteva treba izmeniti difoltnu šifru.	CVE CVE-1999-0497 ⁷¹⁶⁸	Ozbiljan	Ukloniti ili onemogućiti nalog, ukoliko to nije kritično za funkcionisanje sistema. U suprotnom, lozinku treba promeniti u onu koja nije po difoltu.
19.	FTP server does not support AUTH command (ftp-generic-0007)	172.23.202.193:21 172.23.202.194:21 172.23.202.226:21 172.23.202.227:21 FTP klijenti po difoltu šalju FTP server-u poverljive podatke (korisnički ID i šifra) u vidu čitkog teksta. Ova okolnost dozvoljava zlonamernim korisnicima da presreću poverljive podatke ukoliko prisluškuju vezu. Noviji FTP serveri podržavaju AUTH komandu, koja omogućava dodatne opcije autentifikacije, kao što su TLS, Kerberos, GSSAPI itd. Ona se može koristiti za sprečavanje prisluškivanja na FTP vezama.		Ozbiljan	Ažurirati/preći na FTP server koji podržava AUTH komandu.
20.	Apache httpd AllowOverride Options	172.23.202.193:80 172.23.202.194:80	APPLE APPLE-SA-2009-11-09 ⁷¹⁶⁹	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim

⁷¹⁵⁸ <http://secunia.com/advisories/27563/>⁷¹⁵⁹ <http://secunia.com/advisories/27732/>⁷¹⁶⁰ <http://secunia.com/advisories/28212/>⁷¹⁶¹ <http://secunia.com/advisories/28224/>⁷¹⁶² <http://secunia.com/advisories/28606/>⁷¹⁶³ <http://patches.sgi.com/support/free/security/advisories/20070701-01-P> pristupljeno 18.12.2011⁷¹⁶⁴ <https://www.suse.com/support/security/advisories/>⁷¹⁶⁵ <http://xforce.iss.net/xforce/xfdb/35095>⁷¹⁶⁶ http://httpd.apache.org/security/vulnerabilities_20.html⁷¹⁶⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>⁷¹⁶⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>⁷¹⁶⁹ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>

	handling bypass (CVE-2009-1195) (http://apache-allowoverrideoptions-handling-bypass)	172.23.202.226:80 172.23.202.227:80 Skenirani servis je osjetljiv na ovu ranjivost SAMO ako web server izvršava direktivu AllowOverride sa određenim opcijama koje se koriste. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u obradi direktiva „Options“ i „AllowOverride“. U konfiguracijama koje koriste direktivu „AllowOverride“ sa određenim „Options“ argumentima, lokalni korisnici mogu da izvršavaju komande iz web-serverskih skripti.	BID 35115 ⁷¹⁷⁰ CVE CVE-2009-1195 ⁷¹⁷¹ DEBIAN DSA-1816 ⁷¹⁷² OSVDB 54733 ⁷¹⁷³ OVAL OVAL11094 ⁷¹⁷⁴ OVAL OVAL8704 ⁷¹⁷⁵ OVAL OVAL12377 ⁷¹⁷⁶ REDHAT RHSA-2009:1075 ⁷¹⁷⁷ REDHAT RHSA-2009:1156 ⁷¹⁷⁸ SECUNIA 35261 ⁷¹⁷⁹ SECUNIA 35264 ⁷¹⁸⁰ SECUNIA 35395 ⁷¹⁸¹ SECUNIA 35453 ⁷¹⁸² SECUNIA 35721 ⁷¹⁸³ SECUNIA 37152 ⁷¹⁸⁴ SUSE SUSE-SA:2009:050 ⁷¹⁸⁵ XF apache-allowoverrides-security-bypass(50808) ⁷¹⁸⁶ URL1 ⁷¹⁸⁷		instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz
21.	Apache HTTPD: Method 413 Error Response Cross-Site Scripting Vulnerability (CVE-2007-6203) (apache-httpd-cve-2007-6203)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Verzije Apache HTTP web servera 2.0x i 2.2x ne saniraju na odgovarajući način metodu zahteva na 413 stranici sa pogrešnim odgovorom koja je uzvraćena kad je zlonameran zahtev sa velikom vrednošću za dužinu sadržaja (Content-Length) poslat serveru. Nedostatak izlaza uzrokuje ranjivost na XSS napade na serveru. Ova ranjivost se može iskoristiti samo ako napadnuti HTTP klijent bude	APPLE APPLE-SA-2008-03-18 ⁷¹⁸⁸ BID 26663 ⁷¹⁸⁹ OVAL OVAL12166 ⁷¹⁹⁰ CVE CVE-2007-6203 ⁷¹⁹¹ SECUNIA 27906 ⁷¹⁹² SECUNIA 28196 ⁷¹⁹³ SECUNIA 29348 ⁷¹⁹⁴ SECUNIA 29420 ⁷¹⁹⁵ SECUNIA 29640 ⁷¹⁹⁶ SECUNIA 30356 ⁷¹⁹⁷ SECUNIA 30732 ⁷¹⁹⁸ SECUNIA 33105 ⁷¹⁹⁹ SECUNIA 34219 ⁷²⁰⁰ XF apache-413error-xss(38800) ⁷²⁰¹	Ozbiljan	Apache >= 2.0 and < 2.1 Ažurirati na Apache verziju 2.0.62 Apache 2.0.62 nikada nije pušten u opticaj usled problema u kvalitetu koji su otkriveni u tarbolima pre puštanja u promet. Umesto toga, ažurirati na Apache verziju 2.0.63. Apache >= 2.1 and < 2.3 Ažurirajte na Apache verziju 2.2.7 Apache 2.2.7 nikada nije pušten u opticaj usled problema u kvalitetu koji su

⁷¹⁷⁰ <http://www.securityfocus.com/bid/35115>⁷¹⁷¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1195>⁷¹⁷² <http://www.debian.org/security/2009/dsa-1816>⁷¹⁷³ <http://osvdb.org/54733>⁷¹⁷⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11094>⁷¹⁷⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8704>⁷¹⁷⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12377>⁷¹⁷⁷ <http://rhn.redhat.com/errata/RHSA-2009-1075.html>⁷¹⁷⁸ <http://rhn.redhat.com/errata/RHSA-2009-1156.html>⁷¹⁷⁹ <http://secunia.com/advisories/35261/>⁷¹⁸⁰ <http://secunia.com/advisories/35264/>⁷¹⁸¹ <http://secunia.com/advisories/35395/>⁷¹⁸² <http://secunia.com/advisories/35453/>⁷¹⁸³ <http://secunia.com/advisories/35721/>⁷¹⁸⁴ <http://secunia.com/advisories/37152/>⁷¹⁸⁵ <https://www.suse.com/support/security/advisories/>⁷¹⁸⁶ <http://xforce.iss.net/xforce/xfdb/50808>⁷¹⁸⁷ http://httpd.apache.org/security/vulnerabilities_22.html⁷¹⁸⁸ <http://lists.apple.com/archives/security-announce/2008/Mar/msg00000.html>⁷¹⁸⁹ <http://www.securityfocus.com/bid/26663>⁷¹⁹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12166>⁷¹⁹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6203>⁷¹⁹² <http://secunia.com/advisories/27906/>⁷¹⁹³ <http://secunia.com/advisories/28196/>⁷¹⁹⁴ <http://secunia.com/advisories/29348/>⁷¹⁹⁵ <http://secunia.com/advisories/29420/>⁷¹⁹⁶ <http://secunia.com/advisories/29640/>⁷¹⁹⁷ <http://secunia.com/advisories/30356/>⁷¹⁹⁸ <http://secunia.com/advisories/30732/>⁷¹⁹⁹ <http://secunia.com/advisories/33105/>⁷²⁰⁰ <http://secunia.com/advisories/34219/>

		primoran da pošalje HTTP zahtev sa nevalidnim imenom metoda. Pokretanje ranjivog HTTP servisa: Apache 2.2.3. Primer: http://172.23.202.193/ 3: <title>413 Request Entity Too Large</title> 4: </head><body> 5: Request Entity Too Large 6: The requested resource </br /> 7: does not allow request data with <SCRIPT>NXSSTEST</SCRIPT> requests	URL1 ⁷²⁰² URL2 ⁷²⁰³ URL3 ⁷²⁰⁴ URL4 ⁷²⁰⁵		otkriveni u tarbolima pre puštanja u promet. Umesto toga, ažurirati na Apache 2.2.8.
22.	Apache HTTPD: mod_cache proxy DoS (CVE-2007-1863) (apache-httpd-cve-2007-1863)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Propust je otkriven u modulu mod_cache. Na sajtovima na kojima je omogućeno keširanje, udaljeni napadač bi mogao da pošalje pažljivo izrađen zahtev koji bi doveo do toga da child proces Apache-a koji to obrađuje krahira. To može dovesti samo do odbijanja servisa ako se koristi threaded MPM.	BID 24649 ⁷²⁰⁶ CERT TA08-150A ⁷²⁰⁷ CVE CVE-2007-1863 ⁷²⁰⁸ OSVDB 37079 ⁷²⁰⁹ OVAL OVAL.9824 ⁷²¹⁰ REDHAT RHSA-2007:0533 ⁷²¹¹ REDHAT RHSA-2007:0534 ⁷²¹² REDHAT RHSA-2007:0556 ⁷²¹³ REDHAT RHSA-2007:0557 ⁷²¹⁴ SECUNIA 25830 ⁷²¹⁵ SECUNIA 25873 ⁷²¹⁶ SECUNIA 25920 ⁷²¹⁷ SECUNIA 26273 ⁷²¹⁸ SECUNIA 26443 ⁷²¹⁹ SECUNIA 26508 ⁷²²⁰ SECUNIA 26822 ⁷²²¹ SECUNIA 26842 ⁷²²² SECUNIA 26993 ⁷²²³ SECUNIA 27037 ⁷²²⁴ SECUNIA 27563 ⁷²²⁵ SECUNIA 27732 ⁷²²⁶ SECUNIA 28606 ⁷²²⁷ SECUNIA 30430 ⁷²²⁸	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.61.tar.gz

⁷²⁰¹ <http://xforce.iss.net/xforce/xfdb/38800>⁷²⁰² http://procheckup.com/Vulnerability_PR07-37.php⁷²⁰³ <http://svn.apache.org/viewvc?revision=600645&view=revision>⁷²⁰⁴ <http://svn.apache.org/viewvc?revision=602473&view=revision>⁷²⁰⁵ <http://svn.apache.org/viewvc?revision=604425&view=revision>⁷²⁰⁶ <http://www.securityfocus.com/bid/24649>⁷²⁰⁷ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>⁷²⁰⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-1863>⁷²⁰⁹ <http://www.osvdb.org/37079>⁷²¹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9824>⁷²¹¹ <http://rhn.redhat.com/errata/RHSA-2007-0533.html>⁷²¹² <http://rhn.redhat.com/errata/RHSA-2007-0534.html>⁷²¹³ <http://rhn.redhat.com/errata/RHSA-2007-0556.html>⁷²¹⁴ <http://rhn.redhat.com/errata/RHSA-2007-0557.html>⁷²¹⁵ <http://secunia.com/advisories/25830/>⁷²¹⁶ <http://secunia.com/advisories/25873/>⁷²¹⁷ <http://secunia.com/advisories/25920/>⁷²¹⁸ <http://secunia.com/advisories/26273/>⁷²¹⁹ <http://secunia.com/advisories/26443/>⁷²²⁰ <http://secunia.com/advisories/26508/>⁷²²¹ <http://secunia.com/advisories/26822/>⁷²²² <http://secunia.com/advisories/26842/>⁷²²³ <http://secunia.com/advisories/26993/>⁷²²⁴ <http://secunia.com/advisories/27037/>⁷²²⁵ <http://secunia.com/advisories/27563/>⁷²²⁶ <http://secunia.com/advisories/27732/>⁷²²⁷ <http://secunia.com/advisories/28606/>⁷²²⁸ <http://secunia.com/advisories/30430/>

			SUSE SA:2007:061 ⁷²²⁹ URL1 ⁷²³⁰		
23.	Apache httpd mod_proxy_ajp DoS (CVE-2010-0408) (http- apache-mod_proxy_ajp- dos)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ajp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Mod_proxy_ajp će vratiti pogrešan kôd statusa ako naide na grešku, prouzrokujući da backend server bude stavljen u status greške dok ne istekne vreme za ponovni pokušaj. Udaljeni napadač bi mogao da pošalje zlonameran zahtev da bi pokrenuo ovaj problem, što bi dovelo do odbijanja servisa. Zahvaljujući Niku Toivola iz Sulake Corporation, ovaj problem je prijavljen uz predloženu adekvatnu meru zaštite u vidu zakrpe.	BID 38491 ⁷²³¹ CVE CVE-2010-0408 ⁷²³² DEBIAN DSA-2035 ⁷²³³ OVAL OVAL8619 ⁷²³⁴ OVAL OVAL9935 ⁷²³⁵ REDHAT RHSA-2010:0168 ⁷²³⁶ SECUNIA 39100 ⁷²³⁷ SECUNIA 39501 ⁷²³⁸ SECUNIA 39628 ⁷²³⁹ SECUNIA 39632 ⁷²⁴⁰ SECUNIA 39656 ⁷²⁴¹ SECUNIA 40096 ⁷²⁴² URL1 ⁷²⁴³	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz
24.	Apache HTTPD: mod_proxy_ftp DoS (CVE-2009-3094) (apache-httpd-cve- 2009-3094)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ftp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust NULL pointer dereference (pointer sa NULL vrednošću upotrebljen kao da ukazuje na validnu memorijsku oblast) otkriven je u modulu mod_proxy_ftp. Zlonamerni FTP server, kojem su zahtevi proksirani, mogao bi da iskoristi ovaj propust u smislu obaranja http child procesa uz pomoć izmenjenog odgovora EPSV ili PASV komandi, što bi dovelo do delimičnog odbijanja servisa.	CVE CVE-2009-3094 ⁷²⁴⁴ DEBIAN DSA-1934 ⁷²⁴⁵ OVAL OVAL10981 ⁷²⁴⁶ OVAL OVAL8087 ⁷²⁴⁷ SECUNIA 36549 ⁷²⁴⁸ SECUNIA 37152 ⁷²⁴⁹ SUSE SA:2009:050 ⁷²⁵⁰ URL1 ⁷²⁵¹	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.14 Ažurirati na Apache HTTPD version 2.2.14 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.gz

⁷²²⁹ <https://www.suse.com/support/security/advisories/>⁷²³⁰ http://httpd.apache.org/security/vulnerabilities_20.html⁷²³¹ <http://www.securityfocus.com/bid/38491>⁷²³² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0408>⁷²³³ <http://www.debian.org/security/2010/dsa-2035>⁷²³⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8619>⁷²³⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9935>⁷²³⁶ <http://rhn.redhat.com/errata/RHSA-2010-0168.html>⁷²³⁷ <http://secunia.com/advisories/39100/>⁷²³⁸ <http://secunia.com/advisories/39501/>⁷²³⁹ <http://secunia.com/advisories/39628/>⁷²⁴⁰ <http://secunia.com/advisories/39632/>⁷²⁴¹ <http://secunia.com/advisories/39656/>⁷²⁴² <http://secunia.com/advisories/40096/>⁷²⁴³ http://httpd.apache.org/security/vulnerabilities_22.html⁷²⁴⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3094>⁷²⁴⁵ <http://www.debian.org/security/2009/dsa-1934>⁷²⁴⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10981>⁷²⁴⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8087>⁷²⁴⁸ <http://secunia.com/advisories/36549/>⁷²⁴⁹ <http://secunia.com/advisories/37152/>⁷²⁵⁰ <https://www.suse.com/support/security/advisories/>⁷²⁵¹ http://httpd.apache.org/security/vulnerabilities_22.html

25.	Apache httpd Solaris pollset DoS (CVE-2009-2699) (http-apache-solaris-pollset-dos)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Nađen je propust koji utiče na Solaris pollset podršku (Event Port backend), a koji uzrokuje propust u APR-u. azlonamerni napadač bi mogao da pokrene ovaj problem na Solaris serverima koji bi koristio MPM-ove i doveo do odbijanja servisa.	BID 36596 ⁷²⁵² CVE CVE-2009-2699 ⁷²⁵³ XF apache-solaris-pollset-dos(53666) ⁷²⁵⁴ URL ⁷²⁵⁵	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.gz
26.	Browsable web directory (http-generic-browsable-dir)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Otkriven je direktorijum na web serveru koji može biti pretraživan, što znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice - spajdering (prateći hiperlinkove), ili -kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute force napadom na liste uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skrivena“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice. Primer: http://172.23.202.193/icons/small/ 4: <title>Index of /icons/small</title> 5: </head> 6: <body> 7: Index of /icons/small 8: ...CO]“</th><th>Name</th><th><a href=“?C=M;O=A...</th>		Ozbiljan	Za Apache: onemogućiti pretraživanje direktorijuma mreže za sve direktorijume i poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume. Za Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote: Onemogućiti pretraživanje direktorijuma za sve direktorijume i poddirektorijume. Uključiti Tomcat-ov web.xml file. U odeljku „default“, promeniti parametar „listings“ iz „true“ u „false“. Restartovati server. Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripta i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi,

⁷²⁵² <http://www.securityfocus.com/bid/36596>⁷²⁵³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2699>⁷²⁵⁴ <http://xforce.iss.net/xforce/xfdb/53666>⁷²⁵⁵ http://httpd.apache.org/security/vulnerabilities_22.html

					koji je zastsareo, kao i nepoznate fajlove i direktorijume.
27.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	TCP reset with incorrect sequence number triggered this fault on 172.23.202.193:21 172.23.202.227:21 172.23.202.194:80 172.23.202.226:80 Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hедера i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	OSVDB 4030 ⁷²⁵⁶ BID: 10183 ⁷²⁵⁷ CERT-VN: 415294 ⁷²⁵⁸ CVE CVE-2004-0230 ⁷²⁵⁹ MS: MS05-019 ⁷²⁶⁰ MS: MS06-064 ⁷²⁶¹ NETBSD: NetBSD-SA2004-006 ⁷²⁶² OVAL: OVAL2689 ⁷²⁶³ OVAL: OVAL270 ⁷²⁶⁴ OVAL OVAL3508 ⁷²⁶⁵ OVAL OVAL4791 ⁷²⁶⁶ OVAL OVAL5711 ⁷²⁶⁷ SECUNIA: 11440 ⁷²⁶⁸ SECUNIA 11458 ⁷²⁶⁹ SECUNIA: 22341 ⁷²⁷⁰ SGI 20040403-01-A ⁷²⁷¹ XF tcp-rst-dos(15886) ⁷²⁷² URL1 ⁷²⁷³ URL2 ⁷²⁷⁴	Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC 2385 ⁷²⁷⁵ . Ono je napravljeno da smanji opasnost od određenih napada na BGP, kao što su TCP reseti.
28.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podesi na jedinstvenu vrednost i da se koristi u rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da fingerprint-uje operativni sistem.	BID 4314 ⁷²⁷⁶ CVE CVE-2002-0510 ⁷²⁷⁷ XF linux-udp-fingerprint(8588) ⁷²⁷⁸	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili pak ranjivost koju treba popravljati, tako da ne postoje rešenja koja se mogu kupiti. Jedino se može postaviti fajervol ili neka druga sprava za filtriranje između napadnutog i neprijateljskog napada koji je u mogućnosti da randomizuje IP ID-jeve.
29.	Apache HTTPD: mod_imap XSS (CVE-2007-5000) (apache-httpd-cve-2007-5000)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je ranjiv na ovu ranjivost samo ako je pokrenuo	BID 26838 ⁷²⁷⁹ CERT TA08-150A ⁷²⁸⁰ CVE CVE-2007-5000 ⁷²⁸¹ OSVDB 39134 ⁷²⁸² OVAL OVAL9539 ⁷²⁸³ REDHAT RHSA-	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.63.tar.gz Apache HTTPD >= 1.3 and

⁷²⁵⁶ <http://www.osvdb.org/4030>⁷²⁵⁷ <http://www.securityfocus.com/bid/10183>⁷²⁵⁸ <http://www.kb.cert.org/vuls/id/415294>⁷²⁵⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁷²⁶⁰ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁷²⁶¹ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁷²⁶² <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁷²⁶³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>⁷²⁶⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>⁷²⁶⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>⁷²⁶⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>⁷²⁶⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>⁷²⁶⁸ <http://secunia.com/advisories/11440/>⁷²⁶⁹ <http://secunia.com/advisories/11458/>⁷²⁷⁰ <http://secunia.com/advisories/22341/>⁷²⁷¹ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>⁷²⁷² <http://xforce.iss.net/xforce/xfdb/15886>⁷²⁷³ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁷²⁷⁴ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>⁷²⁷⁵ <http://www.ietf.org/rfc/rfc2385.txt>⁷²⁷⁶ <http://www.securityfocus.com/bid/4314>⁷²⁷⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>⁷²⁷⁸ <http://xforce.iss.net/xforce/xfdb/8588>⁷²⁷⁹ <http://www.securityfocus.com/bid/26838>⁷²⁸⁰ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>⁷²⁸¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-5000>⁷²⁸² <http://www.osvdb.org/39134>⁷²⁸³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9539>

	sledeće module: mod_imagemap, mod_imap i imagemap fajl je javno dostupan. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u modulu mod_imap. Na sajtovima na kojima je omogućen mod_imap i fajl imagemap je javno dostupan, moguće je izvesti napad tipa "crossite scripting attack".	2008:0004⁷²⁸⁴ REDHAT RHSA- 2008:0005⁷²⁸⁵ REDHAT RHSA- 2008:0006⁷²⁸⁶ REDHAT RHSA- 2008:0007⁷²⁸⁷ REDHAT RHSA- 2008:0008⁷²⁸⁸ REDHAT RHSA- 2008:0009⁷²⁸⁹ REDHAT RHSA- 2008:0261⁷²⁹⁰ SECUNIA 28046⁷²⁹¹ SECUNIA 28073⁷²⁹² SECUNIA 28081⁷²⁹³ SECUNIA 28196⁷²⁹⁴ SECUNIA 28375⁷²⁹⁵ SECUNIA 28467⁷²⁹⁶ SECUNIA 28471⁷²⁹⁷ SECUNIA 28525⁷²⁹⁸ SECUNIA 28526⁷²⁹⁹ SECUNIA 28607⁷³⁰⁰ SECUNIA 28749⁷³⁰¹ SECUNIA 28750⁷³⁰² SECUNIA 28922⁷³⁰³ SECUNIA 28977⁷³⁰⁴ SECUNIA 29420⁷³⁰⁵ SECUNIA 29640⁷³⁰⁶ SECUNIA 29806⁷³⁰⁷ SECUNIA 29988⁷³⁰⁸ SECUNIA 30356⁷³⁰⁹ SECUNIA 30430⁷³¹⁰ SECUNIA 30732⁷³¹¹ SECUNIA 31142⁷³¹² SUSE SA:2008:021⁷³¹³ URL1⁷³¹⁴	< 1.3.41 Ažurirati na Apache HTTPD version 1.3.41 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/apache-1.3.41.tar.gz Apache HTTPD >= 2.2 and < 2.2.8 Ažurirati na Apache HTTPD version 2.2.8 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.8.tar.gz

⁷²⁸⁴ <http://rhn.redhat.com/errata/RHSA-2008-0004.html>

⁷²⁸⁵ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>

⁷²⁸⁶ <http://rhn.redhat.com/errata/RHSA-2008-0006.html>

⁷²⁸⁷ <http://rhn.redhat.com/errata/RHSA-2008-0007.html>

⁷²⁸⁸ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>

⁷²⁸⁹ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>

⁷²⁹⁰ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>

⁷²⁹¹ <http://secunia.com/advisories/28046/>

⁷²⁹² <http://secunia.com/advisories/28073/>

⁷²⁹³ <http://secunia.com/advisories/28081/>

⁷²⁹⁴ <http://secunia.com/advisories/28196/>

⁷²⁹⁵ <http://secunia.com/advisories/28375/>

⁷²⁹⁶ <http://secunia.com/advisories/28467/>

⁷²⁹⁷ <http://secunia.com/advisories/28471/>

⁷²⁹⁸ <http://secunia.com/advisories/28525/>

⁷²⁹⁹ <http://secunia.com/advisories/28526/>

⁷³⁰⁰ <http://secunia.com/advisories/28607/>

⁷³⁰¹ <http://secunia.com/advisories/28749/>

⁷³⁰² <http://secunia.com/advisories/28750/>

⁷³⁰³ <http://secunia.com/advisories/28922/>

⁷³⁰⁴ <http://secunia.com/advisories/28977/>

⁷³⁰⁵ <http://secunia.com/advisories/29420/>

⁷³⁰⁶ <http://secunia.com/advisories/29640/>

⁷³⁰⁷ <http://secunia.com/advisories/29806/>

⁷³⁰⁸ <http://secunia.com/advisories/29988/>

⁷³⁰⁹ <http://secunia.com/advisories/30356/>

⁷³¹⁰ <http://secunia.com/advisories/30430/>

⁷³¹¹ <http://secunia.com/advisories/30732/>

⁷³¹² <http://secunia.com/advisories/31142/>

⁷³¹³ <https://www.suse.com/support/security/advisories/>

⁷³¹⁴ http://httpd.apache.org/security/vulnerabilities_20.html

30.	Apache HTTPD: mod_proxy_ftp globbing XSS (CVE-2008-2939) (apache-httpd-cve-2008-2939)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ftp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u modulu mod_proxy_ftp prilikom obrade "wildcard-a" ukoliko se on nađe u putanji FTP URL. Ukoliko je mod_proxy_ftp omogućen da podržava FTP-over-HTTP, zahtevi koji sadrže specijalne karaktere mogu da dovedu do cross-site scripting napada (XSS).	APPLE APPLE-SA-2009-05-12 ⁷³¹⁵ BID 30560 ⁷³¹⁶ CERT TA09-133A ⁷³¹⁷ CERT-VN 663763 ⁷³¹⁸ CVE CVE-2008-2939 ⁷³¹⁹ OVAL OVAL11316 ⁷³²⁰ OVAL OVAL7716 ⁷³²¹ REDHAT RHSA-2008:0966 ⁷³²² REDHAT RHSA-2008:0967 ⁷³²³ SECUNIA 31384 ⁷³²⁴ SECUNIA 31673 ⁷³²⁵ SECUNIA 32685 ⁷³²⁶ SECUNIA 32838 ⁷³²⁷ SECUNIA 33156 ⁷³²⁸ SECUNIA 33797 ⁷³²⁹ SECUNIA 34219 ⁷³³⁰ SECUNIA 35074 ⁷³³¹ XF apache-modproxyftp-xss(44223). ⁷³³² URL1 ⁷³³³	Ozbiljan	Apache >= 2.0 and < 2.1 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.10 Ažurirati na Apache HTTPD version 2.2.10 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.10.tar.gz
31.	Apache HTTPD: mod_proxy_ftp UTF-7 XSS (CVE-2008-0005) (apache-httpd-cve-2008-0005)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu ranjivost samo ako je pokrenut modul mod_proxy_ftp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. U modul mod_proxy_ftp je dodata zaobilaznica. Na sajtovima na kojima je omogućen mod_proxy_ftp i konfigurisan je forward tipa proxy-ja, moguće je izvesti napad XSS na Web pretraživače koji neprepoznaju određeni character set prema pravilima iz dokumenta RFC 2616.	BID 27234 ⁷³³⁴ CVE CVE-2008-0005 ⁷³³⁵ OVAL OVAL10812 ⁷³³⁶ REDHAT RHSA-2008:0004 ⁷³³⁷ REDHAT RHSA-2008:0005 ⁷³³⁸ REDHAT RHSA-2008:0006 ⁷³³⁹ REDHAT RHSA-2008:0007 ⁷³⁴⁰ REDHAT RHSA-2008:0008 ⁷³⁴¹ REDHAT RHSA-2008:0009 ⁷³⁴² SECUNIA 28467 ⁷³⁴³ SECUNIA 28471 ⁷³⁴⁴	Ozbiljan	Apache >= 2.0 and < 2.1 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.63.tar.gz Apache HTTPD >= 2.2 and < 2.2.8 Ažurirati na Apache HTTPD version 2.2.8 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.8.tar.gz

⁷³¹⁵ <http://lists.apple.com/archives/security-announce/2009/May/msg00001.html>⁷³¹⁶ <http://www.securityfocus.com/bid/30560>⁷³¹⁷ <http://www.us-cert.gov/ncas/alerts/TA09-133A>⁷³¹⁸ <http://www.kb.cert.org/vuls/id/663763>⁷³¹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-2939>⁷³²⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11316>⁷³²¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7716>⁷³²² <http://rhn.redhat.com/errata/RHSA-2008-0966.html>⁷³²³ <http://rhn.redhat.com/errata/RHSA-2008-0967.html>⁷³²⁴ <http://secunia.com/advisories/31384/>⁷³²⁵ <http://secunia.com/advisories/31673/>⁷³²⁶ <http://secunia.com/advisories/32685/>⁷³²⁷ <http://secunia.com/advisories/32838/>⁷³²⁸ <http://secunia.com/advisories/33156/>⁷³²⁹ <http://secunia.com/advisories/33797/>⁷³³⁰ <http://secunia.com/advisories/34219/>⁷³³¹ <http://secunia.com/advisories/35074/>⁷³³² <http://xforce.iss.net/xforce/xfdb/44223>⁷³³³ http://httpd.apache.org/security/vulnerabilities_20.html⁷³³⁴ <http://www.securityfocus.com/bid/27234>⁷³³⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0005>⁷³³⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10812>⁷³³⁷ <http://rhn.redhat.com/errata/RHSA-2008-0004.html>⁷³³⁸ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>⁷³³⁹ <http://rhn.redhat.com/errata/RHSA-2008-0006.html>⁷³⁴⁰ <http://rhn.redhat.com/errata/RHSA-2008-0007.html>⁷³⁴¹ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>⁷³⁴² <http://rhn.redhat.com/errata/RHSA-2008-0009.html>⁷³⁴³ <http://secunia.com/advisories/28467/>⁷³⁴⁴ <http://secunia.com/advisories/28471/>

			SECUNIA 28526 ⁷³⁴⁵ SECUNIA 28607 ⁷³⁴⁶ SECUNIA 28749 ⁷³⁴⁷ SECUNIA 28977 ⁷³⁴⁸ SECUNIA 29348 ⁷³⁴⁹ SECUNIA 29420 ⁷³⁵⁰ SECUNIA 29640 ⁷³⁵¹ SECUNIA 30732 ⁷³⁵² SECUNIA 35650 ⁷³⁵³ SUSE SA:2008:021 ⁷³⁵⁴ XF apache-modproxyftp- utf7-xss(39615) URL1 ⁷³⁵⁵		
32.	Apache HTTPD: mod_status XSS (CVE- 2007-6388) (apache- httpd-cve-2007-6388)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu ranjivost samo ako je pokrenut modul mod_status i ukoliko su stranice statusa javno dostupne. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u modulu mod_status. Na sajtovima na kojima je status servera javno dostupan i omogućen je ExtendedStatus, postoji mogućnost XSS napada. Stranica sa statusom servera nije po difoltu omogućena, a dosadašnja praksa je pokazala da je najbolje da ona ne bude javno dostupna.	BID 27237 ⁷³⁵⁶ CERT TA08-150A ⁷³⁵⁷ CVE CVE-2007-6388 ⁷³⁵⁸ OVAL OVAL10272 ⁷³⁵⁹ REDHAT RHSA- 2008:0004 ⁷³⁶⁰ REDHAT RHSA- 2008:0005 ⁷³⁶¹ REDHAT RHSA- 2008:0006 ⁷³⁶² REDHAT RHSA- 2008:0007 ⁷³⁶³ REDHAT RHSA- 2008:0008 ⁷³⁶⁴ REDHAT RHSA- 2008:0009 ⁷³⁶⁵ REDHAT RHSA- 2008:0261 ⁷³⁶⁶ SECUNIA 28467 ⁷³⁶⁷ SECUNIA 28471 ⁷³⁶⁸ SECUNIA 28526 ⁷³⁶⁹ SECUNIA 28607 ⁷³⁷⁰ SECUNIA 28749 ⁷³⁷¹ SECUNIA 28922 ⁷³⁷² SECUNIA 28965 ⁷³⁷³ SECUNIA 28977 ⁷³⁷⁴	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dis t/httpd/httpd-2.0.63.tar.gz Apache HTTPD >= 1.3 and < 1.3.41 Ažurirati na Apache HTTPD version 1.3.41 Uraditi download a zatim instalirati: http://archive.apache.org/dis t/httpd/apache-1.3.41.tar.gz Apache HTTPD >= 2.2 and < 2.2.8 Ažurirati na Apache HTTPD version 2.2.8 Uraditi download a zatim instalirati: http://archive.apache.org/dis t/httpd/httpd-2.2.8.tar.gz

⁷³⁴⁵ <http://secunia.com/advisories/28526/>⁷³⁴⁶ <http://secunia.com/advisories/28607/>⁷³⁴⁷ <http://secunia.com/advisories/28749/>⁷³⁴⁸ <http://secunia.com/advisories/28977/>⁷³⁴⁹ <http://secunia.com/advisories/29348/>⁷³⁵⁰ <http://secunia.com/advisories/29420/>⁷³⁵¹ <http://secunia.com/advisories/29640/>⁷³⁵² <http://secunia.com/advisories/30732/>⁷³⁵³ <http://secunia.com/advisories/35650/>⁷³⁵⁴ <https://www.suse.com/support/security/advisories/>⁷³⁵⁵ http://httpd.apache.org/security/vulnerabilities_20.html⁷³⁵⁶ <http://www.securityfocus.com/bid/27237>⁷³⁵⁷ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>⁷³⁵⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6388>⁷³⁵⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10272>⁷³⁶⁰ <http://rhn.redhat.com/errata/RHSA-2008-0004.html>⁷³⁶¹ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>⁷³⁶² <http://rhn.redhat.com/errata/RHSA-2008-0006.html>⁷³⁶³ <http://rhn.redhat.com/errata/RHSA-2008-0007.html>⁷³⁶⁴ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>⁷³⁶⁵ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>⁷³⁶⁶ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>⁷³⁶⁷ <http://secunia.com/advisories/28467/>⁷³⁶⁸ <http://secunia.com/advisories/28471/>⁷³⁶⁹ <http://secunia.com/advisories/28526/>⁷³⁷⁰ <http://secunia.com/advisories/28607/>⁷³⁷¹ <http://secunia.com/advisories/28749/>⁷³⁷² <http://secunia.com/advisories/28922/>⁷³⁷³ <http://secunia.com/advisories/28965/>⁷³⁷⁴ <http://secunia.com/advisories/28977/>

			SECUNIA 29420 ⁷³⁷⁵ SECUNIA 29504 ⁷³⁷⁶ SECUNIA 29640 ⁷³⁷⁷ SECUNIA 29806 ⁷³⁷⁸ SECUNIA 29988 ⁷³⁷⁹ SECUNIA 30356 ⁷³⁸⁰ SECUNIA 30430 ⁷³⁸¹ SECUNIA 30732 ⁷³⁸² SECUNIA 31142 ⁷³⁸³ SECUNIA 33200 ⁷³⁸⁴ SUSE SA:2008:021 ⁷³⁸⁵ XF apache-status-page-xss(39472) ⁷³⁸⁶		
33.	Apache HTTPD: apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpdcve-2011-0419)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_autoindex. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_fnmatch() u sklopu APR biblioteke. Ako je omogućen mod_autoindex, a indksi direktorijuma mod_autoindex su sadržavali fajlove sa dovoljno dugim nazivima, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do preterane upotrebe CPU-a. Ovo bi moglo da bude iskorišćeno u napadu odbijanja servisa. Zahvaljujući Maksymilian Arciemowicz prijavljen je ovaj propust.	CVE CVE-2011-0419 ⁷³⁸⁷ DEBIAN DSA-2237 ⁷³⁸⁸ IAVM 2012-B-0056 ⁷³⁸⁹ OVAL OVAL14638 ⁷³⁹⁰ OVAL OVAL14804 ⁷³⁹¹ REDHAT RHSA-2011:0896 ⁷³⁹² REDHAT RHSA-2011:0897 ⁷³⁹³ REDHAT RHSA-2011:0507 ⁷³⁹⁴ SECUNIA 44490 ⁷³⁹⁵ SECUNIA 44564 ⁷³⁹⁶ SECUNIA 44574 ⁷³⁹⁷ URL1 ⁷³⁹⁸	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.19 Ažurirati na Apache HTTPD version 2.2.19 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.19.tar.gz
34.	Apache HTTPD: APR-util heap underwrite (CVE-2009-0023) (apache-httpd-cve-	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu	BID 35221 ⁷³⁹⁹ CVE CVE-2009-0023 ⁷⁴⁰⁰ DEBIAN DSA-1812 ⁷⁴⁰¹ OVAL OVAL10968 ⁷⁴⁰² OVAL OVAL12321 ⁷⁴⁰³	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

⁷³⁷⁵ <http://secunia.com/advisories/29420/>⁷³⁷⁶ <http://secunia.com/advisories/29504/>⁷³⁷⁷ <http://secunia.com/advisories/29640/>⁷³⁷⁸ <http://secunia.com/advisories/29806/>⁷³⁷⁹ <http://secunia.com/advisories/29988/>⁷³⁸⁰ <http://secunia.com/advisories/30356/>⁷³⁸¹ <http://secunia.com/advisories/30430/>⁷³⁸² <http://secunia.com/advisories/30732/>⁷³⁸³ <http://secunia.com/advisories/31142/>⁷³⁸⁴ <http://secunia.com/advisories/33200/>⁷³⁸⁵ <https://www.suse.com/support/security/advisories/>⁷³⁸⁶ <http://xforce.iss.net/xforce/xfdb/39472> pristupljeno 11.12.2011⁷³⁸⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419>⁷³⁸⁸ <http://www.debian.org/security/2011/dsa-2237>⁷³⁸⁹ <http://iase.disa.mil/stigs/iavm-cve.html>⁷³⁹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14638>⁷³⁹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14804>⁷³⁹² <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁷³⁹³ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>⁷³⁹⁴ <http://rhn.redhat.com/errata/RHSA-2011-0507.html>⁷³⁹⁵ <http://secunia.com/advisories/44490/>⁷³⁹⁶ <http://secunia.com/advisories/44564/>⁷³⁹⁷ <http://secunia.com/advisories/44574/>⁷³⁹⁸ http://httpd.apache.org/security/vulnerabilities_22.html⁷³⁹⁹ <http://www.securityfocus.com/bid/35221>⁷⁴⁰⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-0023>⁷⁴⁰¹ <http://lists.debian.org/debian-security-announce/2009/msg00124.html>⁷⁴⁰² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10968>

	2009-0023)	ranjivost SAMO ako napadač poseduje posebno kreiranu ključnu reč za pretraživanje one funkcije koja upravlja kompajliranjem formi zahtevane pretrage. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u načinu na koji komplet APR-biblioteke kompajlira forme zahtevanih pretraživanja. Napadač bi mogao da formuliše posebno izrađenu ključnu reč pretraživanja koja bi se proizvoljnim prepisivanjem gomilala u memoriji prilikom obrađivanja zahteva za pretragu.	REDHAT RHSA-2009:1107 ⁷⁴⁰⁴ REDHAT RHSA-2009:1108 ⁷⁴⁰⁵ SECUNIA 34724 ⁷⁴⁰⁶ SECUNIA 35284 ⁷⁴⁰⁷ SECUNIA 35360 ⁷⁴⁰⁸ SECUNIA 35395 ⁷⁴⁰⁹ SECUNIA 35444 ⁷⁴¹⁰ SECUNIA 35487 ⁷⁴¹¹ SECUNIA 35565 ⁷⁴¹² SECUNIA 35710 ⁷⁴¹³ SECUNIA 35797 ⁷⁴¹⁴ SECUNIA 35843 ⁷⁴¹⁵ SECUNIA 37221 ⁷⁴¹⁶ XF apache-aprstrmatchprecompile-dos(50964) ⁷⁴¹⁷ URL1 ⁷⁴¹⁸		
35.	Apache HTTPD: mod_proxy_balancer CSRF (CVE-2007-6420) (apache-httpd-cve-2007-6420)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Mod_proxy_balancer je omogućio administrativni interfejs koji bi mogao biti ranjiv na napade lažnih zahteva CSRF (cross-site request forgery).	BID 27236 ⁷⁴¹⁹ BID 31681 ⁷⁴²⁰ CVE CVE-2007-6420 ⁷⁴²¹ OVAL OVAL8371 ⁷⁴²² REDHAT RHSA-2008:0966 ⁷⁴²³ SECUNIA 31026 ⁷⁴²⁴ SECUNIA 32222 ⁷⁴²⁵ SECUNIA 33797 ⁷⁴²⁶ SECUNIA 34219 ⁷⁴²⁷ URL1 ⁷⁴²⁸	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.9.tar.gz
36.	Apache HTTPD: mod_proxy_balancer DoS (CVE-2007-6422) (apache-httpd-cve-2007-6422)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Propust je otkriven u modulu mod_proxy_balancer. Na sajtovmu na kojima je omogućen mod_proxy_balancer, autorizovan	BID 27236 ⁷⁴²⁹ CVE CVE-2007-6422 ⁷⁴³⁰ OVAL OVAL10181 ⁷⁴³¹ OVAL OVAL8690 ⁷⁴³² REDHAT RHSA-2008:0008 ⁷⁴³³ REDHAT RHSA-2008:0009 ⁷⁴³⁴	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.8.tar.gz

⁷⁴⁰³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12321>⁷⁴⁰⁴ <http://rhn.redhat.com/errata/RHSA-2009-1107.html>⁷⁴⁰⁵ <http://rhn.redhat.com/errata/RHSA-2009-1108.html>⁷⁴⁰⁶ <http://secunia.com/advisories/34724/>⁷⁴⁰⁷ <http://secunia.com/advisories/35284/>⁷⁴⁰⁸ <http://secunia.com/advisories/35360/>⁷⁴⁰⁹ <http://secunia.com/advisories/35395/>⁷⁴¹⁰ <http://secunia.com/advisories/35444/>⁷⁴¹¹ <http://secunia.com/advisories/35487/>⁷⁴¹² <http://secunia.com/advisories/35565/>⁷⁴¹³ <http://secunia.com/advisories/35710/>⁷⁴¹⁴ <http://secunia.com/advisories/35797/>⁷⁴¹⁵ <http://secunia.com/advisories/35843/>⁷⁴¹⁶ <http://secunia.com/advisories/37221/>⁷⁴¹⁷ <http://xforce.iss.net/xforce/xfdb/50964>⁷⁴¹⁸ http://httpd.apache.org/security/vulnerabilities_22.html⁷⁴¹⁹ <http://www.securityfocus.com/bid/27236>⁷⁴²⁰ <http://www.securityfocus.com/bid/31681>⁷⁴²¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6420>⁷⁴²² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8371>⁷⁴²³ <http://rhn.redhat.com/errata/RHSA-2008-0966.html>⁷⁴²⁴ <http://secunia.com/advisories/31026/>⁷⁴²⁵ <http://secunia.com/advisories/32222/>⁷⁴²⁶ <http://secunia.com/advisories/33797/>⁷⁴²⁷ <http://secunia.com/advisories/34219/>⁷⁴²⁸ http://httpd.apache.org/security/vulnerabilities_22.html⁷⁴²⁹ <http://www.securityfocus.com/bid/27236>⁷⁴³⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6422>⁷⁴³¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10181>⁷⁴³² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8690>⁷⁴³³ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>

		korisnik bi mogao poslati pažljivo izrađen zahtev koji bi doveo do toga da krahira child proces Apache-a koji taj zahtev obrađuje. To može dovesti samo do odbijanja servisa ako se koristi threaded MPM.	SECUNIA 28526 ⁷⁴³⁵ SECUNIA 28749 ⁷⁴³⁶ SECUNIA 28977 ⁷⁴³⁷ SECUNIA 29348 ⁷⁴³⁸ SECUNIA 29640 ⁷⁴³⁹ SUSE SUSE-SA:2008:021 ⁷⁴⁴⁰ XF apache-modproxybalancer-dos(39476) ⁷⁴⁴¹ URL1 ⁷⁴⁴²		
37.	Apache HTTPD: mod_proxy_balancer XSS (CVE-2007-6421) (apache-httpd-cve-2007-6421)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Propust je otkriven u modulu mod_proxy_balancer. Na sajtovmu na kojima je omogućen mod_proxy_balancer, moguć je XSS napad prema autorizovanom korisniku.	BID 27236 ⁷⁴⁴³ CVE CVE-2007-6421 ⁷⁴⁴⁴ OVAL OVAL10664 ⁷⁴⁴⁵ OVAL OVAL8651 ⁷⁴⁴⁶ REDHAT RHSA-2008:0008 ⁷⁴⁴⁷ REDHAT RHSA-2008:0009 ⁷⁴⁴⁸ SECUNIA 28526 ⁷⁴⁴⁹ SECUNIA 28749 ⁷⁴⁵⁰ SECUNIA 28977 ⁷⁴⁵¹ SECUNIA 29420 ⁷⁴⁵² SECUNIA 29640 ⁷⁴⁵³ SUSE SUSE-SA:2008:021 ⁷⁴⁵⁴ XF apache-modproxybalancer-dos(39476) ⁷⁴⁵⁵ URL1 ⁷⁴⁵⁶	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.8.tar.gz
38.	Apache HTTPD: mod_status cross-site scripting (CVE-2006-5752) (apache-httpd-cve-2006-5752)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osjetljiv na ovu ranjivost samo ako je pokrenut modul mod_status i ukoliko su stranice statusa javno dostupan. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti.	OSVDB 37052 ⁷⁴⁵⁷ BID 24645 ⁷⁴⁵⁸ CVE CVE-2006-5752 ⁷⁴⁵⁹ OVAL OVAL10154 ⁷⁴⁶⁰ REDHAT RHSA-2007:0532 ⁷⁴⁶¹ REDHAT RHSA-2007:0533 ⁷⁴⁶² REDHAT RHSA-2007:0534 ⁷⁴⁶³	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.61.tar.gz Apache HTTPD >= 1.3 and < 1.3.39 Ažurirati na Apache HTTPD version 1.3.39 Uraditi download a zatim

⁷⁴³⁴ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>⁷⁴³⁵ <http://secunia.com/advisories/28526/>⁷⁴³⁶ <http://secunia.com/advisories/28749/>⁷⁴³⁷ <http://secunia.com/advisories/28977/>⁷⁴³⁸ <http://secunia.com/advisories/29348/>⁷⁴³⁹ <http://secunia.com/advisories/29640/>⁷⁴⁴⁰ <https://www.suse.com/support/security/advisories/>⁷⁴⁴¹ <http://xforce.iss.net/xforce/xfdb/39476>⁷⁴⁴² http://httpd.apache.org/security/vulnerabilities_22.html⁷⁴⁴³ <http://www.securityfocus.com/bid/27236>⁷⁴⁴⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6421>⁷⁴⁴⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10664>⁷⁴⁴⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8651>⁷⁴⁴⁷ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>⁷⁴⁴⁸ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>⁷⁴⁴⁹ <http://secunia.com/advisories/28526/>⁷⁴⁵⁰ <http://secunia.com/advisories/28749/>⁷⁴⁵¹ <http://secunia.com/advisories/28977/>⁷⁴⁵² <http://secunia.com/advisories/29420/>⁷⁴⁵³ <http://secunia.com/advisories/29640/>⁷⁴⁵⁴ <https://www.suse.com/support/security/advisories/>⁷⁴⁵⁵ <http://xforce.iss.net/xforce/xfdb/39476>⁷⁴⁵⁶ http://httpd.apache.org/security/vulnerabilities_22.html⁷⁴⁵⁷ <http://www.osvdb.org/37052>⁷⁴⁵⁸ <http://www.securityfocus.com/bid/24645>⁷⁴⁵⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-5752>⁷⁴⁶⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10154>⁷⁴⁶¹ <http://rhn.redhat.com/errata/RHSA-2007-0532.html>⁷⁴⁶² <http://rhn.redhat.com/errata/RHSA-2007-0533.html>⁷⁴⁶³ <http://rhn.redhat.com/errata/RHSA-2007-0534.html>

		Propust je otkriven u modulu mod_status. Na sajtovima na kojima je status servera javno dostupan i omogućen je ExtendedStatus, postoji mogućnost XSS napada. Stranica sa statusom servera nije po defaultu omogućena, a dosadašnja praksa je pokazala da je najbolje da ona ne bude javno dostupna.	REDHAT 2007:0556 ⁷⁴⁶⁴ REDHAT 2007:0557 ⁷⁴⁶⁵ REDHAT 2008:0261 ⁷⁴⁶⁶ SECUNIA 25827 ⁷⁴⁶⁷ SECUNIA 25830 ⁷⁴⁶⁸ SECUNIA 25873 ⁷⁴⁶⁹ SECUNIA 25920 ⁷⁴⁷⁰ SECUNIA 26273 ⁷⁴⁷¹ SECUNIA 26443 ⁷⁴⁷² SECUNIA 26458 ⁷⁴⁷³ SECUNIA 26508 ⁷⁴⁷⁴ SECUNIA 26822 ⁷⁴⁷⁵ SECUNIA 26842 ⁷⁴⁷⁶ SECUNIA 26993 ⁷⁴⁷⁷ SECUNIA 27037 ⁷⁴⁷⁸ SECUNIA 27563 ⁷⁴⁷⁹ SECUNIA 27732 ⁷⁴⁸⁰ SECUNIA 28212 ⁷⁴⁸¹ SECUNIA 28224 ⁷⁴⁸² SECUNIA 28606 ⁷⁴⁸³ SUSE SA:2007:061 ⁷⁴⁸⁴ XF apache-modstatus-xss(35097) URL1 ⁷⁴⁸⁵		instalirati: http://archive.apache.org/dist/httpd/apache-1.3.39.tar.gz Apache HTTPD >= 2.2 and < 2.2.6 Ažurirati na Apache HTTPD version 2.2.6 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz
39.	Apache HTTPD: Subrequest handling of request headers (mod_headers) (CVE-2010-0434) (apache-httpd-cve-2010-0434)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_headers. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust u jezgru "subrequest process code" može dovesti do greške tipa segmentation fault-a ili do otkrivanja	APPLE APPLE-SA-2010-11-10 ⁷⁴⁸⁶ BID 38494 ⁷⁴⁸⁷ CVE CVE-2010-0434 ⁷⁴⁸⁸ DEBIAN DSA-2035 ⁷⁴⁸⁹ OVAL OVAL10358 ⁷⁴⁹⁰ OVAL OVAL8695 ⁷⁴⁹¹ REDHAT 2010:0168 ⁷⁴⁹² REDHAT 2010:0175 ⁷⁴⁹³ SECUNIA 39100 ⁷⁴⁹⁴	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.15 Ažurirati na Apache HTTPD version 2.2.15 Uraditi download a zatim instalirati: http://archive.apache.org/dist

⁷⁴⁶⁴ <http://rhn.redhat.com/errata/RHSA-2007-0556.html>⁷⁴⁶⁵ <http://rhn.redhat.com/errata/RHSA-2007-0557.html>⁷⁴⁶⁶ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>⁷⁴⁶⁷ <http://secunia.com/advisories/25827/>⁷⁴⁶⁸ <http://secunia.com/advisories/25830/>⁷⁴⁶⁹ <http://secunia.com/advisories/25873/>⁷⁴⁷⁰ <http://secunia.com/advisories/25920/>⁷⁴⁷¹ <http://secunia.com/advisories/26273/>⁷⁴⁷² <http://secunia.com/advisories/26443/>⁷⁴⁷³ <http://secunia.com/advisories/26458/>⁷⁴⁷⁴ <http://secunia.com/advisories/26508/>⁷⁴⁷⁵ <http://secunia.com/advisories/26822/>⁷⁴⁷⁶ <http://secunia.com/advisories/26842/>⁷⁴⁷⁷ <http://secunia.com/advisories/26993/>⁷⁴⁷⁸ <http://secunia.com/advisories/27037/>⁷⁴⁷⁹ <http://secunia.com/advisories/27563/>⁷⁴⁸⁰ <http://secunia.com/advisories/27732/>⁷⁴⁸¹ <http://secunia.com/advisories/28212/>⁷⁴⁸² <http://secunia.com/advisories/28224/>⁷⁴⁸³ <http://secunia.com/advisories/28606/>⁷⁴⁸⁴ <https://www.suse.com/support/security/advisories/>⁷⁴⁸⁵ http://httpd.apache.org/security/vulnerabilities_20.html⁷⁴⁸⁶ <http://support.apple.com/kb/ht4435>⁷⁴⁸⁷ <http://www.securityfocus.com/bid/38494>⁷⁴⁸⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0434>⁷⁴⁸⁹ <http://www.debian.org/security/2010/dsa-2035>⁷⁴⁹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10358>⁷⁴⁹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8695>⁷⁴⁹² <http://rhn.redhat.com/errata/RHSA-2010-0168.html>⁷⁴⁹³ <http://rhn.redhat.com/errata/RHSA-2010-0175.html>

		podataka iz nekog drugog zahteva na thread-ovima servera, kao što su worker ili winnt MPM-ovi. Zahvaljujući Philip Pickett-u iz Vmware, ovaj propust je prijavljen i predložen je način ispravke.	SECUNIA 39115 ⁷⁴⁹⁵ SECUNIA 39501 ⁷⁴⁹⁶ SECUNIA 39628 ⁷⁴⁹⁷ SECUNIA 39632 ⁷⁴⁹⁸ SECUNIA 39656 ⁷⁴⁹⁹ SECUNIA 40096 ⁷⁵⁰⁰ XF apache-http-rh-info-disclosure(56625) ⁷⁵⁰¹ URL1 ⁷⁵⁰²		t/httpd/httpd-2.2.15.tar.gz
40.	OpenSSH CBC Mode Information Disclosure Vulnerability (ssh-openssh-cbc-mode-info-disclosure)	172.23.202.193:22 172.23.202.194:22 172.23.202.226:22 172.23.202.227:22 Određene verzije OpenSSH-a poseduju ranjivu implementaciju bloka šifarskog algoritma u CBC modu (Cipher Block Chaining). Ovo bi udaljenom napadaču moglo omogućiti da preko nepoznatih vektora pridobije određene podatke u vidu običnog teksta iz proizvoljnog bloka šifrovanog teksta u SSH sesiji.	BID 32319 ⁷⁵⁰³ CVE CVE-2008-5161 ⁷⁵⁰⁴ SECUNIA 32760 ⁷⁵⁰⁵ URL1 ⁷⁵⁰⁶ URL2 ⁷⁵⁰⁷	Ozbiljan	Uraditi download a zatim instalirati: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-5.2p1.tar.gz Verzija 5.2 OpenSSH-a je puštena u promet 22. februara 2009.
41.	OpenSSH „X11UseLocalhost“ X11 Forwarding Session Hijacking Vulnerability (ssh-opensshx11uselocalhost - x11-forwarding-session-hijack)	172.23.202.193:22 172.23.202.194:22 172.23.202.226:22 172.23.202.227:22 Određene verzije OpenSSH-a podešavaju SO_REUSEADDR soket opciju kada je onemogućeno podešavanje X11UseLocalhost konfiguracije. Ovo bi lokalnom napadaču moglo da omogući da preuzme X11 forwarding port preko veze ka pojedinačnoj IP adresi.	BID 30339 ⁷⁵⁰⁸ CVE CVE-2008-3259 ⁷⁵⁰⁹ SECUNIA 31179 ⁷⁵¹⁰	Ozbiljan	Uraditi download a zatim instalirati: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-5.1p1.tar.gz Verzija 5.1 OpenSSH-a je puštena u promet 21. jula 2008.
42.	HTTP TRACE Method Enabled (http-trace-method-enabled)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 HTTP TRACE metoda se obično koristi da uzvratu potpuni HTTP zahtev klijentu koji ga zahteva, u cilju debugovanja proxy servera. Napadač bi mogao da kreira web	CERT-VN 867593 ⁷⁵¹¹ OSVDB 35511 ⁷⁵¹² OSVDB 3726 ⁷⁵¹³ SECUNIA 10726 ⁷⁵¹⁴ SECUNIA 17334 ⁷⁵¹⁵ SECUNIA 21802 ⁷⁵¹⁶ SECUNIA 25636 ⁷⁵¹⁷ CVE CVE-2004-2320 ⁷⁵¹⁸ CVE CVE-2004-2763 ⁷⁵¹⁹	Ozbiljan	Apache Onemogućiti HTTP TRACE metodu za Apache. Novije verzije Apache-a (1.3.34 i 2.0.55 i novije) omogućuju konfiguracionu direktivu koja se zove TraceEnable. Da bi se odbili TRACE zahtevi,

⁷⁴⁹⁴ <http://secunia.com/advisories/39100/>⁷⁴⁹⁵ <http://secunia.com/advisories/39115/>⁷⁴⁹⁶ <http://secunia.com/advisories/39501/>⁷⁴⁹⁷ <http://secunia.com/advisories/39628/>⁷⁴⁹⁸ <http://secunia.com/advisories/39632/>⁷⁴⁹⁹ <http://secunia.com/advisories/39656/>⁷⁵⁰⁰ <http://secunia.com/advisories/40096/>⁷⁵⁰¹ <http://xforce.iss.net/xforce/xfdb/56625>⁷⁵⁰² http://httpd.apache.org/security/vulnerabilities_20.html⁷⁵⁰³ <http://www.securityfocus.com/bid/32319>⁷⁵⁰⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-5161>⁷⁵⁰⁵ <http://secunia.com/advisories/32760/>⁷⁵⁰⁶ http://www.cpmi.gov.uk/Docs/Vulnerability_Advisory_SSH.txt, pristupljeno 20.12.2011⁷⁵⁰⁷ <http://www.openssh.com/txt/cbc.adv>⁷⁵⁰⁸ <http://www.securityfocus.com/bid/30339>⁷⁵⁰⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-3259>⁷⁵¹⁰ <http://secunia.com/advisories/31179/>⁷⁵¹¹ <http://www.kb.cert.org/vuls/id/867593>⁷⁵¹² <http://www.osvdb.org/35511>⁷⁵¹³ <http://www.osvdb.org/3726>⁷⁵¹⁴ <http://secunia.com/advisories/10726/>⁷⁵¹⁵ <http://secunia.com/advisories/17334/>⁷⁵¹⁶ <http://secunia.com/advisories/21802/>⁷⁵¹⁷ <http://secunia.com/advisories/25636/>⁷⁵¹⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2320>

		stranicu koristeći XMLHTTP, ActiveX ili XMLDOM da natera klijenta da pošalje TRACE zahtev i da sačuva klijenove kolačiće. Kao posledica može da se javi XSS napad. Primer: 172.23.202.193:80 Running vulnerable HTTP service. http://172.23.202.193/ 1: TRACE / HTTP/1.1 2: Host: 172.23.202.193 3: Cookie: vulnerable=yes	CVE CVE-2005-3398 ⁷⁵²⁰ CVE CVE-2006-4683 ⁷⁵²¹ CVE CVE-2007-3008 ⁷⁵²² CVE CVE-2008-7253 ⁷⁵²³ CVE CVE-2009-2823 ⁷⁵²⁴ CVE CVE-2010-0386 ⁷⁵²⁵ OSVDB 877 ⁷⁵²⁶ SUN 50603 ⁷⁵²⁷ BID 9561 ⁷⁵²⁸ URL1 ⁷⁵²⁹ URL2 ⁷⁵³⁰		dodaje se sledeći red u konfiguraciju servera: TraceEnable off Za starije verzije Apache web servera, koristiti modul mod_rewrite da bi se odbili TRACE zahteve: RewriteEngine On RewriteCond %{REQUEST_METHOD} ^TRACE RewriteRule .* - [F]
43.	Database Open Access (database-open-access)	172.23.202.193:3306 172.23.202.194:3306 172.23.202.226:3306 172.23.202.227:3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posjedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7.	URL1 ⁷⁵³¹	Umeren	Konfigurisati server baze podataka tako da dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.
44.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	CVE CVE-1999-0524 ⁷⁵³² OSVDB 95 ⁷⁵³³ XF netmask(306) ⁷⁵³⁴ icmp- XF timestamp(322) ⁷⁵³⁵ icmp-	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
45.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada	URL1 ⁷⁵³⁶ URL2 ⁷⁵³⁷ URL3 ⁷⁵³⁸	Umeren	Onemogućavanje TCP timestamp odgovora na Linux OS. Podesiti net.ipv4.tcp_timestamps

⁷⁵¹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2763>⁷⁵²⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-3398>⁷⁵²¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-4683>⁷⁵²² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3008>⁷⁵²³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-7253>⁷⁵²⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2823>⁷⁵²⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0386>⁷⁵²⁶ <http://osvdb.org/887>⁷⁵²⁷ <https://sunsolve.sun.com/search/document.do?assetkey=1-22-50603-1> pristupljeno 18.12.2011⁷⁵²⁸ <http://www.securityfocus.com/bid/9561>⁷⁵²⁹ <http://www.apacheweek.com/issues/03-01-24#news>⁷⁵³⁰ <http://www.kb.cert.org/vuls/id/867593>⁷⁵³¹ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf⁷⁵³² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁷⁵³³ <http://www.osvdb.org/95>⁷⁵³⁴ <http://xforce.iss.net/xforce/xfdb/306>⁷⁵³⁵ <http://xforce.iss.net/xforce/xfdb/322>⁷⁵³⁶ http://www.forensicswiki.org/wiki/TCP_timestamps⁷⁵³⁷ <http://www.ietf.org/rfc/rfc1323.txt>⁷⁵³⁸ <http://uptime.netcraft.com/>

		udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.			vrednost na sledećem ključu na 0 pokretanjem sledeće komande: sysctl -w net.ipv4.tcp_timestamps=0 Dodatno, sledeću vrednost u difoltnom sysctl konfiguracionom fajlu, generally sysctl.conf: net.ipv4.tcp_timestamps=0
46.	WebDAV Extensions are Enabled (http-generic-webdav-enabled)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 WebDAV je skup ekstenzija za HTTP protokol koji omogućava korisnicima da zajednički edituju i obrađuju fajlove na udaljenim web serverima. Mnogi web serveri po difoltu omogućavaju WebDAV ekstenzije, čak i kada nisu potrebne. S obzirom na dodatnu složenost, dosadašnja praksa je pokazala da treba onemogućiti WebDAV ukoliko se trenutno ne koristi.		Umeren	Apache: Potrebno je onemogućiti WebDAV (eng. Web-based Distributed Authoring and Versioning) za Apache. Proveriti da li je mod_dav modul isključen ili utvrditi da li postoji zahtevana autentifikacija na direktorijumima nad kojima se zahteva DAV.
47.	Apache HTTPD: insecure LD_LIBRARY_PATH handling (CVE-2012-0883) (apache-httpd-cve-2012-0883)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Otkrivena je nebezbedna obrada rute LD_LIBRARY_PATH koja bi mogla da dovede do toga da direktorijum koji trenutno radi traži DSO-ove. Ovo bi lokalnom korisniku omogućilo da izvrši kôd kao root ako je administrator pokrenuo apachectl sa nepoverljivog direktorijuma.	APPLE APPLE-SA-2013-09-12-1 ⁷⁵³⁹ CVE CVE-2012-0883 ⁷⁵⁴⁰ SECUNIA 48849 ⁷⁵⁴¹ URL1 ⁷⁵⁴² URL2 ⁷⁵⁴³	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.23 Ažurirati na to Apache HTTPD version 2.2.23 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz Apache HTTPD >= 2.4 and < 2.4.2 Ažurirati na Apache HTTPD version 2.4.2 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.2.tar.gz
48.	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368) (apache-httpd-cve-2011-3368)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja prisustva mod_proxy modula. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao	APPLE APPLE-SA-2012-09-19-2 ⁷⁵⁴⁴ BID 49957 ⁷⁵⁴⁵ CVE CVE-2011-3368 ⁷⁵⁴⁶ IAVM 2012-A-0017 ⁷⁵⁴⁷ IAVM 2012-A-0152 ⁷⁵⁴⁸ IAVM 2012-B-0056 ⁷⁵⁴⁹ OSVDB 76079 ⁷⁵⁵⁰ REDHAT 2011:1391 ⁷⁵⁵¹ RHSA- REDHAT 2011:1392 ⁷⁵⁵² RHSA-	Ozbiljan	Apache HTTPD >= 1.3 and < 2 Apply the patch for CVE-2011-3368 to 1.3 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na

⁷⁵³⁹ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁷⁵⁴⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0883>⁷⁵⁴¹ <http://secunia.com/advisories/48849/>⁷⁵⁴² http://httpd.apache.org/security/vulnerabilities_22.html⁷⁵⁴³ http://httpd.apache.org/security/vulnerabilities_24.html⁷⁵⁴⁴ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁷⁵⁴⁵ <http://www.securityfocus.com/bid/49957>⁷⁵⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3368>⁷⁵⁴⁷ <http://iase.disa.mil/stigs/iavm-cve.html>⁷⁵⁴⁸ <http://iase.disa.mil/stigs/iavm-cve.html>⁷⁵⁴⁹ <http://iase.disa.mil/stigs/iavm-cve.html>⁷⁵⁵⁰ <http://www.osvdb.org/76079>⁷⁵⁵¹ <http://rhn.redhat.com/errata/RHSA-2011-1391.html>⁷⁵⁵² <http://rhn.redhat.com/errata/RHSA-2011-1392.html>

		reverzni proxy. Zlonamerni napadač bi mogao da iskoristi ovaj propust na takav način da primora proxy proces da se poveže sa proizvoljnim serverom i potencijalno objavi osetljive informacije sa internih web servera koje inače napadaču nisu direktno dostupne. Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/	SECUNIA 46288 ⁷⁵⁵³ SECUNIA 46414 ⁷⁵⁵⁴ SECUNIA 48551 ⁷⁵⁵⁵ XF 70336 ⁷⁵⁵⁶ URL1 ⁷⁵⁵⁷ URL2 ⁷⁵⁵⁸ URL3 ⁷⁵⁵⁹		http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
49.	Apache HTTPD: mod_rewrite log escape filtering (CVE-2013-1862) (apache-httpd-cve-2013-1862)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_rewrite. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Modul mod_rewrite ne filtrira završne izlazne sekvence iz logova, što zlonamenrom napadaču olakšava da ubace takve sekvence u završne emulatore koji sadrže ranjivosti koje se odnose na izlazne sekvence.	CVE CVE-2013-1862 ⁷⁵⁶⁰ OVAL OVAL18790 ⁷⁵⁶¹ REDHAT RHSA-2013:0815 ⁷⁵⁶² REDHAT RHSA-2013:1207 ⁷⁵⁶³ REDHAT RHSA-2013:1208 ⁷⁵⁶⁴ REDHAT RHSA-2013:1209 ⁷⁵⁶⁵ SECUNIA 55032 ⁷⁵⁶⁶ URL1 ⁷⁵⁶⁷ URL2 ⁷⁵⁶⁸	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.25 Ažurirati na Apache HTTPD version 2.2.25 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.25.tar.gz
50.	Apache HTTPD: mod_setenvif.htaccess privilege escalation (CVE-2011-3607) (apache-httpd-cve-2011-3607)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_setenvif. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust preopterećenja je otkriven	APPLE APPLE-SA-2012-09-19-2 ⁷⁵⁶⁹ BID 50494 ⁷⁵⁷⁰ CVE CVE-2011-3607 ⁷⁵⁷¹ IAVM 2012-A-0017 ⁷⁵⁷² IAVM 2012-A-0152 ⁷⁵⁷³ OSVDB 76744 REDHAT RHSA-2012:0128 ⁷⁵⁷⁴ SECUNIA 45793 ⁷⁵⁷⁵ SECUNIA 48551 ⁷⁵⁷⁶	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache

⁷⁵⁵³ <http://secunia.com/advisories/46288/>⁷⁵⁵⁴ <http://secunia.com/advisories/46414/>⁷⁵⁵⁵ <http://secunia.com/advisories/48551/>⁷⁵⁵⁶ <http://xforce.iss.net/xforce/xfdb/70336>⁷⁵⁵⁷ http://httpd.apache.org/security/vulnerabilities_13.html⁷⁵⁵⁸ http://httpd.apache.org/security/vulnerabilities_20.html⁷⁵⁵⁹ http://httpd.apache.org/security/vulnerabilities_22.html⁷⁵⁶⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1862>⁷⁵⁶¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18790>⁷⁵⁶² <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁷⁵⁶³ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁷⁵⁶⁴ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁷⁵⁶⁵ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁷⁵⁶⁶ <http://secunia.com/advisories/55032/>⁷⁵⁶⁷ http://httpd.apache.org/security/vulnerabilities_20.html⁷⁵⁶⁸ http://httpd.apache.org/security/vulnerabilities_22.html⁷⁵⁶⁹ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁷⁵⁷⁰ <http://www.securityfocus.com/bid/50494>⁷⁵⁷¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3607>⁷⁵⁷² <http://iase.disa.mil/stigs/iavm-cve.html>⁷⁵⁷³ <http://iase.disa.mil/stigs/iavm-cve.html>⁷⁵⁷⁴ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁷⁵⁷⁵ <http://secunia.com/advisories/45793/>

		kada je omogućen modul mod_setenvif, što lokalnim korisnicima omogućava da dobiju privilegije preko fajla .htaccess.	XF 71093 ⁷⁵⁷⁷ URL1 ⁷⁵⁷⁸ URL2 ⁷⁵⁷⁹		HTTPD version 2.2.22 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
51.	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-4317) (apache-httpd-cve-2011-4317)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osjetljiv na ovu ranjivost samo ako je pokrenut modul mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy U određenim konfiguracijama koje koriste RewriteRule sa proxy flag-om ili ProxyPassMatch, udaljeni napadač bi mogao da primora reverzni proksi da se poveže sa proizvoljnim serverom i potencijalno objavi osjetljive informacije sa internih web servera koje inače napadaču nisu direktno dostupne.	APPLE APPLE-SA-2012-09-19-2 ⁷⁵⁸⁰ CVE CVE-2011-4317 ⁷⁵⁸¹ IAVM 2012-A-0017 ⁷⁵⁸² IAVM 2012-A-0152 ⁷⁵⁸³ REDHAT RHSA-2012:0128 ⁷⁵⁸⁴ SECUNIA 48551 ⁷⁵⁸⁵ URL1 ⁷⁵⁸⁶	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.22 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
52.	Apache HTTPD: error responses can expose cookies (CVE-2012-0053) (apache-httpd-cve-2012-0053)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Propust je otkriven u difoltnom pogrešnom odgovoru za statusni kôd 400. Zlonamerni napadač bi mogao da iskoristi ovaj propust da objavi "httpOnly" kolačiće ako nije određen dokument custom ErrorDocument.	APPLE APPLE-SA-2012-09-19-2 ⁷⁵⁸⁷ BID 51706 ⁷⁵⁸⁸ CVE CVE-2012-0053 ⁷⁵⁸⁹ IAVM 2012-A-0017 ⁷⁵⁹⁰ REDHAT RHSA-2012:0128 ⁷⁵⁹¹ SECUNIA 48551 ⁷⁵⁹² URL1 ⁷⁵⁹³ URL2 ⁷⁵⁹⁴	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
53.	Apache HTTPD: XSS due to unescaped hostnames (CVE-2012-3499) (apache-httpd-cve-2012-3499)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut jedan od sledećih	APPLE APPLE-SA-2013-09-12-1 ⁷⁵⁹⁵ CVE CVE-2012-3499 ⁷⁵⁹⁶ DEBIAN DSA-2637 ⁷⁵⁹⁷ REDHAT RHSA-2013:0815 ⁷⁵⁹⁸	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.24 Ažurirati na Apache HTTPD version 2.2.24 Uradi download a zatim instalirati:

⁷⁵⁷⁶ <http://secunia.com/advisories/48551/>⁷⁵⁷⁷ <http://xforce.iss.net/xforce/xfdb/71093>⁷⁵⁷⁸ http://httpd.apache.org/security/vulnerabilities_20.html⁷⁵⁷⁹ http://httpd.apache.org/security/vulnerabilities_22.html⁷⁵⁸⁰ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁷⁵⁸¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4317>⁷⁵⁸² <http://iase.disa.mil/stigs/iavm-cve.html>⁷⁵⁸³ <http://iase.disa.mil/stigs/iavm-cve.html>⁷⁵⁸⁴ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁷⁵⁸⁵ <http://secunia.com/advisories/48551/>⁷⁵⁸⁶ http://httpd.apache.org/security/vulnerabilities_22.html⁷⁵⁸⁷ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁷⁵⁸⁸ <http://www.securityfocus.com/bid/51706>⁷⁵⁸⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0053>⁷⁵⁹⁰ <http://iase.disa.mil/stigs/iavm-cve.html>⁷⁵⁹¹ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁷⁵⁹² <http://secunia.com/advisories/48551/>⁷⁵⁹³ http://httpd.apache.org/security/vulnerabilities_20.html⁷⁵⁹⁴ http://httpd.apache.org/security/vulnerabilities_22.html⁷⁵⁹⁵ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁷⁵⁹⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3499>⁷⁵⁹⁷ <http://www.debian.org/security/2013/dsa-2637>

		modula: mod_imagemap, mod_info, mod_ldap, mod_proxy_ftp, mod_status. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Različiti XSS propusti usled nenapuštenih host imena i URI-ja HTML output-a u mod_info, mod_status, mod_imagemap, mod_ldap i mod_proxy_ftp.	REDHAT 2013:1207 ⁷⁵⁹⁹ RHSA- REDHAT 2013:1208 ⁷⁶⁰⁰ RHSA- REDHAT 2013:1209 ⁷⁶⁰¹ RHSA- SECUNIA 55032 ⁷⁶⁰² URL1 ⁷⁶⁰³ URL2 ⁷⁶⁰⁴		http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz Apache HTTPD >= 2.4 and < 2.4.4 Ažurirati na Apache HTTPD version 2.4.4 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz
54.	Apache HTTPD: XSS in mod_proxy_balancer (CVE-2012-4558) (apache-httpd-cve-2012-4558)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu ranjivost samo ako je pokrenut modul mod_proxy_balancer. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust XSS napada je uticao na mod_proxy_balancer manager interface.	APPLE APPLE-SA-2013-09-12-1 ⁷⁶⁰⁵ CVE CVE-2012-4558 ⁷⁶⁰⁶ DEBIAN DSA-2637 ⁷⁶⁰⁷ REDHAT 2013:0815 ⁷⁶⁰⁸ RHSA- REDHAT 2013:1207 ⁷⁶⁰⁹ RHSA- REDHAT 2013:1208 ⁷⁶¹⁰ RHSA- REDHAT 2013:1209 ⁷⁶¹¹ RHSA- URL1 ⁷⁶¹² URL2 ⁷⁶¹³	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.24 Ažurirati na Apache HTTPD version 2.2.24 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz Apache HTTPD >= 2.4 and < 2.4.4 Ažurirati na Apache HTTPD version 2.4.4 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz
55.	Apache HTTPD: mod_dav crash (CVE-2013-1896) (apache-httpd-cve-2013-1896)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_dav_svn. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Slanje MERGE zahteva URI-ju koji obrađuje mod_dav_svn sa izvorom href (poslato kao deo zahteva XML) ciljajući na URI koji nije konfigurisan za DAV prouzrokuje segmentation fault (segfault).	CVE CVE-2013-1896 ⁷⁶¹⁴ OVAL OVAL18835 ⁷⁶¹⁵ REDHAT 2013:1156 ⁷⁶¹⁶ RHSA- REDHAT 2013:1207 ⁷⁶¹⁷ RHSA- REDHAT 2013:1208 ⁷⁶¹⁸ RHSA- REDHAT 2013:1209 ⁷⁶¹⁹ RHSA- SECUNIA 55032 ⁷⁶²⁰ URL1 ⁷⁶²¹ URL2 ⁷⁶²²	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.25 Upgrade to Apache HTTPD version 2.2.25 Apache HTTPD >= 2.4 and < 2.4.6 Upgrade to Apache HTTPD version 2.4.6 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.6.tar.gz
56.	Apache HTTPD: CRLF injection in	172.23.202.193:80 172.23.202.194:80	APPLE APPLE-SA-2009-05-12 ⁷⁶²³	Umeren	Apache HTTPD >= 2.2 and < 2.2.12

⁷⁵⁹⁸ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁷⁵⁹⁹ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁷⁶⁰⁰ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁷⁶⁰¹ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁷⁶⁰² <http://secunia.com/advisories/55032/>⁷⁶⁰³ http://httpd.apache.org/security/vulnerabilities_22.html⁷⁶⁰⁴ http://httpd.apache.org/security/vulnerabilities_24.html⁷⁶⁰⁵ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁷⁶⁰⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4558>⁷⁶⁰⁷ <http://www.debian.org/security/2013/dsa-2637>⁷⁶⁰⁸ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁷⁶⁰⁹ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁷⁶¹⁰ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁷⁶¹¹ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁷⁶¹² http://httpd.apache.org/security/vulnerabilities_22.html⁷⁶¹³ http://httpd.apache.org/security/vulnerabilities_24.html⁷⁶¹⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1896>⁷⁶¹⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18835>⁷⁶¹⁶ <http://rhn.redhat.com/errata/RHSA-2013-1156.html>⁷⁶¹⁷ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁷⁶¹⁸ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁷⁶¹⁹ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁷⁶²⁰ <http://secunia.com/advisories/55032/>⁷⁶²¹ http://httpd.apache.org/security/vulnerabilities_22.html⁷⁶²² http://httpd.apache.org/security/vulnerabilities_24.html⁷⁶²³ <http://lists.apple.com/archives/security-announce/2009/May/msg00001.html>

	mod_negotiation when untrusted uploads are supported (CVE-2008-0456) (apache-httpd-cve-2008-0456)	172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_negotiation. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Moguće je ubaciti CRLF (Carriage Return and Line Feed) koji omogućava CRLF Injection napade (poznatih i kao HTTP Response Splitting) za sajtove koji koriste mod_negotiation, omogućavajući neproverene upload-ove na lokacije na kojima je omogućen MultiViews (višestruko pregledanje).	BID 27409 ⁷⁶²⁴ CERT TA09-133A ⁷⁶²⁵ CVE CVE-2008-0456 ⁷⁶²⁶ REDHAT 2013:0130 ⁷⁶²⁷ RHSA- SECUNIA 29348 ⁷⁶²⁸ SECUNIA 35074 ⁷⁶²⁹ XF 39893 ⁷⁶³⁰ URL1 ⁷⁶³¹		Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz
57.	Apache HTTPD: XSS in mod_negotiation when untrusted uploads are supported (CVE-2012-2687) (apachehttpd-cve-2012-2687)	172.23.202.193:80 172.23.202.194:80 172.23.202.226:80 172.23.202.227:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_negotiation. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Moguće je ubaciti CRLF (Carriage Return and Line Feed) koji omogućava CRLF Injection napade (poznatih i kao HTTP Response Splitting) za sajtove koji koriste mod_negotiation, omogućavajući neproverene upload-ove na lokacije na kojima je omogućen MultiViews (višestruko pregledanje). Ovaj problem je poznat i kao CVE-2008-0455.	APPLE APPLE-SA-2013-09-12-1 ⁷⁶³² BID 55131 ⁷⁶³³ CVE CVE-2012-2687 ⁷⁶³⁴ IAVM 2012-A-0139 ⁷⁶³⁵ REDHAT 2012:1591 ⁷⁶³⁶ RHSA- REDHAT 2012:1592 ⁷⁶³⁷ RHSA- REDHAT 2012:1594 ⁷⁶³⁸ RHSA- REDHAT 2013:0130 ⁷⁶³⁹ RHSA- SECUNIA 50894 ⁷⁶⁴⁰ SECUNIA 51607 ⁷⁶⁴¹ URL1 ⁷⁶⁴² URL2 ⁷⁶⁴³	Umeren	Apache HTTPD >= 2.2 and < 2.2.23 Ažurirati na Apache HTTPD version 2.2.23 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz Apache HTTPD >= 2.4 and < 2.4.3 Ažurirati na Apache HTTPD version 2.4.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.3.tar.gz

Tabela 127. Linux OS sa IP adresama 172.23.202.195, 172.23.202.196, 172.23.202.221, 172.23.202.222, (2013. godina)

Datum: 16.11.2013	Operativni sistem i ime računara	Broj ranjivosti
IP adresa: 172.23.202.195	OS: Red Hat Enterprise Linux 5.6 x64, redhat56entx64	56

⁷⁶²⁴ <http://www.securityfocus.com/bid/27409>⁷⁶²⁵ <http://www.us-cert.gov/ncas/alerts/ta09-133a>⁷⁶²⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0456>⁷⁶²⁷ <http://rhn.redhat.com/errata/RHSA-2013-0130.html>⁷⁶²⁸ <http://secunia.com/advisories/29348/>⁷⁶²⁹ <http://secunia.com/advisories/35074/>⁷⁶³⁰ <http://xforce.iss.net/xforce/xfdb/39893>⁷⁶³¹ http://httpd.apache.org/security/vulnerabilities_22.html⁷⁶³² <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁷⁶³³ <http://www.securityfocus.com/bid/55131>⁷⁶³⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2687>⁷⁶³⁵ <http://iase.disa.mil/stigs/iavm-cve.html>⁷⁶³⁶ <http://rhn.redhat.com/errata/RHSA-2012-1591.html>⁷⁶³⁷ <http://rhn.redhat.com/errata/RHSA-2012-1592.html>⁷⁶³⁸ <http://rhn.redhat.com/errata/RHSA-2012-1594.html>⁷⁶³⁹ <http://rhn.redhat.com/errata/RHSA-2013-0130.html>⁷⁶⁴⁰ <http://secunia.com/advisories/50894/>⁷⁶⁴¹ <http://secunia.com/advisories/51607/>⁷⁶⁴² http://httpd.apache.org/security/vulnerabilities_22.html⁷⁶⁴³ http://httpd.apache.org/security/vulnerabilities_24.html

IP adresa: 172.23.202.196		OS: Centos 5.6 x64, centos56x64			56
IP adresa: 172.23.202.221		OS: Centos 5.6 x86, centos56x86			56
IP adresa: 172.23.202.222		OS: Red Hat Enterprise Linux 5.6 x86, redhat56entx86			56
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Apache httpd mod_isapi module unload flaw (CVE-2010-0425) (apache-httpd-2_2_x-mod_isapi-moduleunload-flaw-cve-2010-0425)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 U modulu mod_isapi je pronađen propust koji će pokušati da ukloni ISAPI dll kada naiđe na greške. To može ostaviti povratne pozive u nedefinisanom stanju greške i kao posledica može da se javi segmentation fault. Na Windows platformama koje koriste mod_isapi, udaljeni napadač bi mogao da pošalje zlonameran zahtev da pokrene ovaj problem, a kako win32 MPM pokreće samo jedan proces, to bi kao ishod imalo odbijanje servisa i potencijalno dozvolilo da se pokrene proizvoljan kôd. Napomena: Zahvaljujući Brett Gervasoni-ju iz "Sense of Security" ovaj problem je prijavljen i za njega je predložena zakrpa.	BID 38494 ⁷⁶⁴⁴ CERT-VN 280613 ⁷⁶⁴⁵ CVE CVE-2010-0425 ⁷⁶⁴⁶ OVAL OVAL8439 ⁷⁶⁴⁷ SECUNIA 38978 ⁷⁶⁴⁸ SECUNIA 39628 ⁷⁶⁴⁹ URL1 ⁷⁶⁵⁰ XF apache-http-modisapi-ocp-unspeccified(56624) ⁷⁶⁵¹	Kritičan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz
2.	Apache httpd APR apr_palloc heap overflow (CVE-2009-2412) (http-apache-apr_palloc-heap-overflow)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 U modulu apr_palloc() je pronađen propust u sklopu APR-a, koji može prouzrokovati velika preopterećenja u programima koji pokušaju da kontrolišu apr_palloc() veličinu zadate od strane korisnika. Sam Apache HTTP server ne dopušta prolaz ka ovoj funkciji neproverenim veličinama koje zadaje korisnik, tako da se on može pokrenuti samo preko neke druge aplikacije koja koristi apr_palloc() na ranjiv način.	APPLE APPLE-SA-2009-11-09 ⁷⁶⁵² BID 35949 ⁷⁶⁵³ CVE CVE-2009-2412 ⁷⁶⁵⁴ OSVDB 56765 ⁷⁶⁵⁵ OSVDB 56766 ⁷⁶⁵⁶ OVAL OVAL8394 ⁷⁶⁵⁷ OVAL OVAL9958 ⁷⁶⁵⁸ SECUNIA 36138 ⁷⁶⁵⁹ SECUNIA 36140 ⁷⁶⁶⁰ SECUNIA 36166 ⁷⁶⁶¹ SECUNIA 36233 ⁷⁶⁶² SECUNIA 37152 ⁷⁶⁶³ SECUNIA 37221 ⁷⁶⁶⁴ SUSE SUSE-SA:2009:050 ⁷⁶⁶⁵	Kritičan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.13.tar.gz Apache HTTPD >= 2.0 and < 2.0.64 Ažurirati na Apache HTTPD version 2.0.64 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz

⁷⁶⁴⁴ <http://www.securityfocus.com/bid/38494>⁷⁶⁴⁵ <http://www.kb.cert.org/vuls/id/280613>⁷⁶⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0425>⁷⁶⁴⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8439>⁷⁶⁴⁸ <http://secunia.com/advisories/38978/>⁷⁶⁴⁹ <http://secunia.com/advisories/39628/>⁷⁶⁵⁰ http://httpd.apache.org/security/vulnerabilities_22.html⁷⁶⁵¹ <http://xforce.iss.net/xforce/xfdb/56624>⁷⁶⁵² <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>⁷⁶⁵³ <http://www.securityfocus.com/bid/35949>⁷⁶⁵⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2412>⁷⁶⁵⁵ <http://osvdb.org/56765>⁷⁶⁵⁶ <http://osvdb.org/56766>⁷⁶⁵⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8394>⁷⁶⁵⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9958>⁷⁶⁵⁹ <http://secunia.com/advisories/36138/>⁷⁶⁶⁰ <http://secunia.com/advisories/36140/>⁷⁶⁶¹ <http://secunia.com/advisories/36166/>⁷⁶⁶² <http://secunia.com/advisories/36233/>⁷⁶⁶³ <http://secunia.com/advisories/37152/>⁷⁶⁶⁴ <http://secunia.com/advisories/37221/>⁷⁶⁶⁵ <https://www.suse.com/support/security/advisories/>

			URL1 ⁷⁶⁶⁶		
3.	Apache HTTPD: mod_proxy_ftp FTP command injection (CVE-2009-3095) (apache-httpd-cve-2009-3095)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 U modulu mod_proxy_ftp je pronađen propust. U reverznoj proxy konfiguraciji, udaljeni napadač bi mogao da iskoristi ovaj defekt da zaobiđe uobičajenu zabranu pristupa tako što bi kreirao pažljivo izrađen HTTP Authorization heder, koji omogućava napadaču da šalje proizvoljne komande FTP serveru.	APPLE APPLE-SA-2010-03-29 ⁷⁶⁶⁷ CVE CVE-2009-3095 ⁷⁶⁶⁸ DEBIAN DSA-1934 ⁷⁶⁶⁹ OVAL OVAL8662 ⁷⁶⁷⁰ OVAL OVAL9363 ⁷⁶⁷¹ SECUNIA 37152 ⁷⁶⁷² SUSE SUSE-SA:2009:050 ⁷⁶⁷³ URL1 ⁷⁶⁷⁴ URL2 ⁷⁶⁷⁵	Kritičan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.gz Apache HTTPD >= 2.0 and < 2.0.64 Ažurirati na Apache HTTPD version 2.0.64 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz
4.	Apache HTTPD: APR-util XML DoS (CVE-2009-1955) (apache-httpd-cve-2009-1955)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Ranjivost na DOS napad otkrivena je u sklopu kopije kompleta APR-util library Extensible Markup Language (XML) prevodioca (eng. parser). Udaljeni napadač bi mogao da kreira posebno izrađen XML dokument koji bi prouzrokovao ogromno zauzeće memorije kada ga procesira XML decoding engine.	APPLE APPLE-SA-2009-11-09 ⁷⁶⁷⁶ BID 35253 ⁷⁶⁷⁷ CVE CVE-2009-1955 ⁷⁶⁷⁸ DEBIAN DSA-1812 ⁷⁶⁷⁹ OVAL OVAL10270 ⁷⁶⁸⁰ REDHAT RHSA-2009:1107 ⁷⁶⁸¹ REDHAT RHSA-2009:1108 ⁷⁶⁸² SECUNIA 34724 ⁷⁶⁸³ SECUNIA 35284 ⁷⁶⁸⁴ SECUNIA 35360 ⁷⁶⁸⁵ SECUNIA 35395 ⁷⁶⁸⁶ SECUNIA 35444 ⁷⁶⁸⁷ SECUNIA 35487 ⁷⁶⁸⁸ SECUNIA 35565 ⁷⁶⁸⁹ SECUNIA 35710 ⁷⁶⁹⁰ SECUNIA 35797 ⁷⁶⁹¹ SECUNIA 35843 ⁷⁶⁹² SECUNIA 36473 ⁷⁶⁹³ SECUNIA 37221 ⁷⁶⁹⁴ URL1 ⁷⁶⁹⁵	Kritičan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

⁷⁶⁶⁶ http://httpd.apache.org/security/vulnerabilities_22.html⁷⁶⁶⁷ <http://lists.apple.com/archives/security-announce/2010/Mar/msg00001.html>⁷⁶⁶⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3095>⁷⁶⁶⁹ <http://www.debian.org/security/DSA-/DSA-1934>⁷⁶⁷⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8662>⁷⁶⁷¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9363>⁷⁶⁷² <http://secunia.com/advisories/37152/>⁷⁶⁷³ <https://www.suse.com/support/security/advisories/>⁷⁶⁷⁴ http://httpd.apache.org/security/vulnerabilities_22.html⁷⁶⁷⁵ http://httpd.apache.org/security/vulnerabilities_20.html⁷⁶⁷⁶ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>⁷⁶⁷⁷ <http://www.securityfocus.com/bid/35253>⁷⁶⁷⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1955>⁷⁶⁷⁹ <http://lists.debian.org/debian-security-announce/2009/msg00124.html>⁷⁶⁸⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10270>⁷⁶⁸¹ <http://rhn.redhat.com/errata/RHSA-2009-1107.html>⁷⁶⁸² <http://rhn.redhat.com/errata/RHSA-2009-1108.html>⁷⁶⁸³ <http://secunia.com/advisories/34724/>⁷⁶⁸⁴ <http://secunia.com/advisories/35284/>⁷⁶⁸⁵ <http://secunia.com/advisories/35360/>⁷⁶⁸⁶ <http://secunia.com/advisories/35395/>⁷⁶⁸⁷ <http://secunia.com/advisories/35444/>⁷⁶⁸⁸ <http://secunia.com/advisories/35487/>⁷⁶⁸⁹ <http://secunia.com/advisories/35565/>⁷⁶⁹⁰ <http://secunia.com/advisories/35710/>⁷⁶⁹¹ <http://secunia.com/advisories/35797/>⁷⁶⁹² <http://secunia.com/advisories/35843/>⁷⁶⁹³ <http://secunia.com/advisories/36473/>⁷⁶⁹⁴ <http://secunia.com/advisories/37221/>⁷⁶⁹⁵ http://httpd.apache.org/security/vulnerabilities_22.html

5.	OpenSSH X11 Cookie Local Authentication Bypass Vulnerability (openssh-x11-cookie-auth-bypass)	172.23.202.195:22 172.23.202.196:22 172.23.202.221:22 172.23.202.222:22 Pre verzije 4.7, OpenSSH nije adekvatno radio kada nepoverljivi kolačić (cookie) nije mogao biti kreiran. Umesto njega, koristi se poverljivi X11 kolačić. To omogućava napadačima da naruše ciljanu polisu i dobiju privilegije korisnika, što kao posledicu servis tretira klijenta X kao poverljivog.	CVE CVE-2007-4752 ⁷⁶⁹⁶ BID 25628 ⁷⁶⁹⁷ XF openssh-x11cookie-privilege-escalation(36637) ⁷⁶⁹⁸	Kritičan	Uraditi download a zatim instalirati: http://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-4.7p1.tar.gz Verzija 4.7 of OpenSSH je puštena u promet 4. septembra 2007.
6	Apache HTTPD: mod_deflate DoS (CVE-2009-1891) (apache-httpd-cve-2009-1891)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Ranjivost na DOS napad otkrivena je u modulu mod_deflate. Ovaj modul nastavlja da kompresuje velike fajlove sve dok se kompresija ne završi, čak i kada je mrežna konekcija koja je zahtevala taj sadržaj prekinuta pre nego što je kompresija završena. To dovodi do toga da mod_deflate zauzima veliku količinu CPU-a ukoliko je mod_deflate bio omogućen za velike fajlove.	APPLE APPLE-SA-2009-11-09 ⁷⁶⁹⁹ CVE CVE-2009-1891 ⁷⁷⁰⁰ DEBIAN DSA-1834 ⁷⁷⁰¹ OSVDB 55782 ⁷⁷⁰² OVAL OVAL8632 ⁷⁷⁰³ OVAL OVAL9248 ⁷⁷⁰⁴ OVAL OVAL12361 ⁷⁷⁰⁵ REDHAT RHSA-2009:1148 ⁷⁷⁰⁶ REDHAT RHSA-2009:1156 ⁷⁷⁰⁷ SECUNIA 35721 ⁷⁷⁰⁸ SECUNIA 35781 ⁷⁷⁰⁹ SECUNIA 35793 ⁷⁷¹⁰ SECUNIA 35865 ⁷⁷¹¹ SECUNIA 37152 ⁷⁷¹² SECUNIA 37221 ⁷⁷¹³ SUSE SA:2009:050 ⁷⁷¹⁴ URL1 ⁷⁷¹⁵	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.12 Ažurirati na Apache HTTPD version 2.2.12 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz
7.	Apache HTTPD: mod_proxy reverse proxy DoS (CVE-2009-1890) (apache-httpd-cve-2009-1890)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy. Proveriti konfiguraciju	APPLE APPLE-SA-2009-11-09 ⁷⁷¹⁶ CVE CVE-2009-1890 ⁷⁷¹⁷ DEBIAN DSA-1834 ⁷⁷¹⁸ OSVDB 55553 ⁷⁷¹⁹ OVAL OVAL12330 ⁷⁷²⁰ OVAL OVAL8616 ⁷⁷²¹	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

⁷⁶⁹⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-4752>⁷⁶⁹⁷ <http://www.securityfocus.com/bid/25628>⁷⁶⁹⁸ <http://xfocus.iss.net/xfocus/xfdb/36637>⁷⁶⁹⁹ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>⁷⁷⁰⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1891>⁷⁷⁰¹ <http://www.debian.org/security/DSA-1834> pristupljeno 18.12.2011⁷⁷⁰² <http://osvdb.org/55782>⁷⁷⁰³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8632>⁷⁷⁰⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9248>⁷⁷⁰⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12361>⁷⁷⁰⁶ <http://rhn.redhat.com/errata/RHSA-2009-1148.html>⁷⁷⁰⁷ <http://rhn.redhat.com/errata/RHSA-2009-1156.html>⁷⁷⁰⁸ <http://secunia.com/advisories/35721/>⁷⁷⁰⁹ <http://secunia.com/advisories/35781/>⁷⁷¹⁰ <http://secunia.com/advisories/35793/>⁷⁷¹¹ <http://secunia.com/advisories/35865/>⁷⁷¹² <http://secunia.com/advisories/37152/>⁷⁷¹³ <http://secunia.com/advisories/37221/>⁷⁷¹⁴ <https://www.suse.com/support/security/advisories/>⁷⁷¹⁵ http://httpd.apache.org/security/vulnerabilities_20.html⁷⁷¹⁶ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>⁷⁷¹⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1890>⁷⁷¹⁸ <http://www.debian.org/security/2009/dsa-1834>⁷⁷¹⁹ <http://osvdb.org/55553>⁷⁷²⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12330>⁷⁷²¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8616>

		web servera radi utvrđivanja prisustva mod_proxy modula. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy. Zlonamerni napadač bi mogao da iskoristi ovaj propust na takav način da primora proxy proces da zauzme veliku količinu CPU vremena.	OVAL OVAL9403 ⁷⁷²² REDHAT RHSA-2009:1148 ⁷⁷²³ REDHAT RHSA-2009:1156 ⁷⁷²⁴ SECUNIA 35691 ⁷⁷²⁵ SECUNIA 35721 ⁷⁷²⁶ SECUNIA 35793 ⁷⁷²⁷ SECUNIA 35865 ⁷⁷²⁸ SECUNIA 37152 ⁷⁷²⁹ SECUNIA 37221 ⁷⁷³⁰ SUSE SUSE-SA:2009:050 ⁷⁷³¹ URL1 7732		
8.	Apache HTTPD: APR-util off-by-one overflow (CVE-2009-1956) (apache-httpd-cve-2009-1956)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Propust prepunjavanja bafera "off-by-one" je otkriven u načinu na koji sklop kopije APR-util library komplet procesira promenljivu listu argumenata. Napadač bi mogao da kreira posebno izrađeni string kao input za već formatiranu output rutu konverzije, koja bi, na velikim platformama, potencijalno mogla da dovede do otkrivanja povreljivih informacija ili do odbijanja servisa.	APPLE APPLE-SA-2009-11-09 ⁷⁷³³ BID 35251 ⁷⁷³⁴ CVE CVE-2009-1956 ⁷⁷³⁵ OVAL OVAL11567 ⁷⁷³⁶ OVAL OVAL12237 ⁷⁷³⁷ REDHAT RHSA-2009:1107 ⁷⁷³⁸ REDHAT RHSA-2009:1108 ⁷⁷³⁹ SECUNIA 34724 ⁷⁷⁴⁰ SECUNIA 35284 ⁷⁷⁴¹ SECUNIA 35395 ⁷⁷⁴² SECUNIA 35487 ⁷⁷⁴³ SECUNIA 35565 ⁷⁷⁴⁴ SECUNIA 35710 ⁷⁷⁴⁵ SECUNIA 35797 ⁷⁷⁴⁶ SECUNIA 35843 ⁷⁷⁴⁷ SECUNIA 37221 ⁷⁷⁴⁸ URL1 7749 	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz
9.	OpenSSH X11 Forwarding Information Disclosure Vulnerability (ssh-)	172.23.202.195:22 172.23.202.196:22 172.23.202.221:22 172.23.202.222:22	BID 28444 ⁷⁷⁵⁰ CVE CVE-2008-1483 ⁷⁷⁵¹ SECUNIA 29522 ⁷⁷⁵² URL1 7753 	Ozbiljan	Nadograditi na najnoviju verziju OpenSSH-a. Najnovija verzija OpenSSH-a je 5.2

⁷⁷²² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9403>

⁷⁷²³ <http://rhn.redhat.com/errata/RHSA-2009-1148.html>

⁷⁷²⁴ <http://rhn.redhat.com/errata/RHSA-2009-1156.html>

⁷⁷²⁵ <http://secunia.com/advisories/35691/>

⁷⁷²⁶ <http://secunia.com/advisories/35721/>

⁷⁷²⁷ <http://secunia.com/advisories/35793/>

⁷⁷²⁸ <http://secunia.com/advisories/35865/>

⁷⁷²⁹ <http://secunia.com/advisories/37152/>

⁷⁷³⁰ <http://secunia.com/advisories/37221/>

⁷⁷³¹ <https://www.suse.com/support/security/advisories/>

⁷⁷³² http://httpd.apache.org/security/vulnerabilities_22.html

⁷⁷³³ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>

⁷⁷³⁴ <http://www.securityfocus.com/bid/35251>

⁷⁷³⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1956>

⁷⁷³⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11567>

⁷⁷³⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12237>

⁷⁷³⁸ <http://rhn.redhat.com/errata/RHSA-2009-1107.html>

⁷⁷³⁹ <http://rhn.redhat.com/errata/RHSA-2009-1108.html>

⁷⁷⁴⁰ <http://secunia.com/advisories/34724/>

⁷⁷⁴¹ <http://secunia.com/advisories/35284/>

⁷⁷⁴² <http://secunia.com/advisories/35395/>

⁷⁷⁴³ <http://secunia.com/advisories/35487/>

⁷⁷⁴⁴ <http://secunia.com/advisories/35565/>

⁷⁷⁴⁵ <http://secunia.com/advisories/35710/>

⁷⁷⁴⁶ <http://secunia.com/advisories/35797/>

⁷⁷⁴⁷ <http://secunia.com/advisories/35843/>

⁷⁷⁴⁸ <http://secunia.com/advisories/37221/>

⁷⁷⁴⁹ http://httpd.apache.org/security/vulnerabilities_22.html

⁷⁷⁵⁰ <http://www.securityfocus.com/bid/28444>

⁷⁷⁵¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-1483>

⁷⁷⁵² <http://secunia.com/advisories/29522/>

	openssh-x11-forwarding-info-disclosure)	Određene verzije OpenSSH-a ne povezuju ispravno TCP portove na lokalnom IPv6 interfejsu ako se koriste zahtevani IPv4 portovi. Ovo bi loklanom napadaču moglo da omogući da preuzme prosleđenu X11 sesiju putem otvaranja TCP port-a 6010 (IPv4).			(OpenBSD izvor) i 5.2p1 (prenosivi izvor).
10.	Apache HTTPD: expat DoS (CVE-2009-3560) (apache-httpd-cve-2009-3560)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepoverljivi XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	BID 37203 ⁷⁷⁵⁴ CVE CVE-2009-3560 ⁷⁷⁵⁵ DEBIAN DSA-1953 ⁷⁷⁵⁶ IAVM 2012-A-0020 ⁷⁷⁵⁷ OVAL OVAL12942 ⁷⁷⁵⁸ REDHAT RHSA-2011:0896 ⁷⁷⁵⁹ OVAL OVAL10613 ⁷⁷⁶⁰ OVAL OVAL6883 ⁷⁷⁶¹ SECUNIA 37537 ⁷⁷⁶² SECUNIA 38231 ⁷⁷⁶³ SECUNIA 38794 ⁷⁷⁶⁴ SECUNIA 38832 ⁷⁷⁶⁵ SECUNIA 38834 ⁷⁷⁶⁶ SECUNIA 39478 ⁷⁷⁶⁷ SECUNIA 41701 ⁷⁷⁶⁸ SECUNIA 43300 ⁷⁷⁶⁹ URL1 ⁷⁷⁷⁰	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.17 Ažurirati na Apache HTTPD version 2.2.17 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
11.	Apache HTTPD: expat DoS (CVE-2009-3720) (apache-httpd-cve-2009-3720)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer	IAVM 2012-A-0020 ⁷⁷⁷¹ OVAL OVAL12719 ⁷⁷⁷² REDHAT RHSA-2011:0896 ⁷⁷⁷³ CVE CVE-2009-3720 ⁷⁷⁷⁴ OVAL OVAL11019 ⁷⁷⁷⁵ OVAL OVAL7112 ⁷⁷⁷⁶ REDHAT RHSA-2010:0002 ⁷⁷⁷⁷ SECUNIA 37324 ⁷⁷⁷⁸ SECUNIA 37537 ⁷⁷⁷⁹	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.17 Ažurirati na Apache HTTPD version 2.2.17 Uraditi download a zatim instalirati: http://archive.apache.org/dist

⁷⁷⁵³ <http://www.openssh.org/txt/release-5.0>⁷⁷⁵⁴ <http://www.securityfocus.com/bid/37203>⁷⁷⁵⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3560>⁷⁷⁵⁶ <http://www.debian.org/security/DSA-/DSA-1953> pristupljeno dana 18.12.2011⁷⁷⁵⁷ <http://iase.disa.mil/stigs/iavm-cve.html>⁷⁷⁵⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12942>⁷⁷⁵⁹ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁷⁷⁶⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10613>⁷⁷⁶¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6883>⁷⁷⁶² <http://secunia.com/advisories/37537/>⁷⁷⁶³ <http://secunia.com/advisories/38231/>⁷⁷⁶⁴ <http://secunia.com/advisories/38794/>⁷⁷⁶⁵ <http://secunia.com/advisories/38832/>⁷⁷⁶⁶ <http://secunia.com/advisories/38834/>⁷⁷⁶⁷ <http://secunia.com/advisories/39478/>⁷⁷⁶⁸ <http://secunia.com/advisories/41701/>⁷⁷⁶⁹ <http://secunia.com/advisories/43300/>⁷⁷⁷⁰ http://httpd.apache.org/security/vulnerabilities_20.html⁷⁷⁷¹ <http://iase.disa.mil/stigs/iavm-cve.html>⁷⁷⁷² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12719>⁷⁷⁷³ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁷⁷⁷⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3720>⁷⁷⁷⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11019>⁷⁷⁷⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7112>⁷⁷⁷⁷ <http://rhn.redhat.com/errata/RHSA-2010-0002.html>⁷⁷⁷⁸ <http://secunia.com/advisories/37324/>⁷⁷⁷⁹ <http://secunia.com/advisories/37537/>

		over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepoverljivi XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	SECUNIA 37925 ⁷⁷⁸⁰ SECUNIA 38050 ⁷⁷⁸¹ SECUNIA 38231 ⁷⁷⁸² SECUNIA 38794 ⁷⁷⁸³ SECUNIA 38832 ⁷⁷⁸⁴ SECUNIA 38834 ⁷⁷⁸⁵ SECUNIA 39478 ⁷⁷⁸⁶ SECUNIA 41701 ⁷⁷⁸⁷ SECUNIA 43300 ⁷⁷⁸⁸ URL1 ⁷⁷⁸⁹		t/httpd/httpd-2.2.17.tar.gz
12.	Apache HTTPD: apr_bridage_split_line DoS (CVE-2010-1623) (apache-httpd-cve-2010-1623)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako Apache procesira ne-SSL zahteve. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_bridage_split_line() u sklopu kompleta APR-util library, koji se koristi za procesiranje ne-SSL zahteva. Udaljeni napadač bi mogao da šalje zahteve, pažljivo izrađujući tajming za pojedinačne bajtove, što bi polako zauzimalo memoriju i potencijalno dovelo do odbijanja servisa.	IAVM 2012-B-0056 ⁷⁷⁹⁰ OVAL OVAL12800 ⁷⁷⁹¹ REDHAT RHSA-2011:0896 ⁷⁷⁹² REDHAT RHSA-2011:0897 ⁷⁷⁹³ BID 43673 ⁷⁷⁹⁴ CVE CVE-2010-1623 ⁷⁷⁹⁵ REDHAT RHSA-2010:0950 ⁷⁷⁹⁶ SECUNIA 41701 ⁷⁷⁹⁷ SECUNIA 42015 ⁷⁷⁹⁸ SECUNIA 42361 ⁷⁷⁹⁹ SECUNIA 42367 ⁷⁸⁰⁰ SECUNIA 42403 ⁷⁸⁰¹ SECUNIA 42537 ⁷⁸⁰² SECUNIA 43211 ⁷⁸⁰³ SECUNIA 43285 ⁷⁸⁰⁴ URL1 ⁷⁸⁰⁵	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.17 Ažurirati na Apache HTTPD version 2.2.17 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
13.	Apache HTTPD: mod_dav DoS (CVE-2010-1452) (apache-httpd-cve-2010-1452)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako web server izvršava jedan od sledećih modula:	IAVM 2012-B-0056 ⁷⁸⁰⁶ OVAL OVAL12341 ⁷⁸⁰⁷ REDHAT RHSA-2011:0896 ⁷⁸⁰⁸ REDHAT RHSA-2011:0897 ⁷⁸⁰⁹ APPLE APPLE-SA-	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.16

⁷⁷⁸⁰ <http://secunia.com/advisories/37925/>⁷⁷⁸¹ <http://secunia.com/advisories/38050/>⁷⁷⁸² <http://secunia.com/advisories/38231/>⁷⁷⁸³ <http://secunia.com/advisories/38794/>⁷⁷⁸⁴ <http://secunia.com/advisories/38832/>⁷⁷⁸⁵ <http://secunia.com/advisories/38834/>⁷⁷⁸⁶ <http://secunia.com/advisories/39478/>⁷⁷⁸⁷ <http://secunia.com/advisories/41701/>⁷⁷⁸⁸ <http://secunia.com/advisories/43300/>⁷⁷⁸⁹ http://httpd.apache.org/security/vulnerabilities_20.html⁷⁷⁹⁰ <http://iase.disa.mil/stigs/iavm-cve.html>⁷⁷⁹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12800>⁷⁷⁹² <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁷⁷⁹³ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>⁷⁷⁹⁴ <http://www.securityfocus.com/bid/43673>⁷⁷⁹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1623>⁷⁷⁹⁶ <http://rhn.redhat.com/errata/RHSA-2010-0950.html>⁷⁷⁹⁷ <http://secunia.com/advisories/41701/>⁷⁷⁹⁸ <http://secunia.com/advisories/42015/>⁷⁷⁹⁹ <http://secunia.com/advisories/42361/>⁷⁸⁰⁰ <http://secunia.com/advisories/42367/>⁷⁸⁰¹ <http://secunia.com/advisories/42403/>⁷⁸⁰² <http://secunia.com/advisories/42537/>⁷⁸⁰³ <http://secunia.com/advisories/43211/>⁷⁸⁰⁴ <http://secunia.com/advisories/43285/>⁷⁸⁰⁵ http://httpd.apache.org/security/vulnerabilities_20.html⁷⁸⁰⁶ <http://iase.disa.mil/stigs/iavm-cve.html>⁷⁸⁰⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12341>⁷⁸⁰⁸ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁷⁸⁰⁹ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>

		mod_cache, mod_dav. Pregledajte konfiguraciju vašeg web servera radi validacije. Propust je otkriven u obradi zahteva od strane mod_cache i mod_dav. Zlonameran udaljeni napadač bi mogao da pošalje pažljivo izrađen zahtev i prouzrokuje da httpd child proces krahira. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM. Ovaj problem se dalje može ublažiti ako na mod_dav samo utiču zahtevi za koje postoji mogućnost autentifikovanja, a mod_cache je pod uticajem samo ako se koristi neuobičajena „CacheIgnoreURLSessionIdentifiers“ direktiva, uvedena u verziji 2.2.14. Ovaj problem je prijavio Mark Drayton.	2011-03-21 ⁷⁸¹⁰ CVE CVE-2010-1452 ⁷⁸¹¹ OVAL OVAL11683 ⁷⁸¹² REDHAT RHSA-2010:0659 ⁷⁸¹³ SECUNIA 42367 ⁷⁸¹⁴ URL1 ⁷⁸¹⁵		Ažurirati na Apache HTTPD version 2.2.16 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.16.tar.gz
14.	Apache HTTPD: mod_proxy crash (CVE-2007-3847) (apache-httpd-cve-2007-3847)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja prisustva mod_proxy modula. Propust je otkriven u modulu mod_proxy Apache HTTP servera. Na sajtovima na kojima je konfigurisan reverzni proxy, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do toga da Apache child proces, koji obrađuje taj zahtev krahira. Na sajtovima na kojima je konfigurisan "forward proxy", napadač bi mogao da izazove sličan krah ukoliko bi korisnik bio primoran da poseti zlonameran sajt koristeći proxy. To može dovesti samo do odbijanja servisa ako se koristi threaded MPM.	APPLE APPLE-SA-2008-03-18 ⁷⁸¹⁶ APPLE APPLE-SA-2008-05-28 ⁷⁸¹⁷ CERT TA08-150A ⁷⁸¹⁹ CVE CVE-2007-3847 ⁷⁸²⁰ OVAL OVAL10525 ⁷⁸²¹ REDHAT RHSA-2007:0746 ⁷⁸²² REDHAT RHSA-2007:0747 ⁷⁸²³ REDHAT RHSA-2007:0911 ⁷⁸²⁴ REDHAT RHSA-2008:0005 ⁷⁸²⁵ SECUNIA 26636 ⁷⁸²⁶ SECUNIA 26722 ⁷⁸²⁷ SECUNIA 26790 ⁷⁸²⁸ SECUNIA 26842 ⁷⁸²⁹ SECUNIA 26952 ⁷⁸³⁰ SECUNIA 26993 ⁷⁸³¹ SECUNIA 27209 ⁷⁸³² SECUNIA 27563 ⁷⁸³³	Ozbiljan	Apache >= 2.0 and < 2.1 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.61.tar.gz Apache HTTPD >= 2.2 and < 2.2.6 Ažurirati na Apache HTTPD version 2.2.6 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz

⁷⁸¹⁰ <http://lists.apple.com/archives/security-announce/2011/Mar/msg00006.html>
⁷⁸¹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1452>
⁷⁸¹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11683>
⁷⁸¹³ <http://rhn.redhat.com/errata/RHSA-2010-0659.html>
⁷⁸¹⁴ <http://secunia.com/advisories/42367/>
⁷⁸¹⁵ http://httpd.apache.org/security/vulnerabilities_20.html
⁷⁸¹⁶ <http://lists.apple.com/archives/security-announce/2008/Mar/msg00000.html>
⁷⁸¹⁷ <http://lists.apple.com/archives/security-announce/2008/May/msg00001.html>
⁷⁸¹⁸ <http://www.securityfocus.com/bid/25489> pristupljeno 18.12.2011
⁷⁸¹⁹ <http://www.cert.org/advisories/TA08-150A.html> pristupljeno 18.12.2011
⁷⁸²⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3847>
⁷⁸²¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10525>
⁷⁸²² <http://rhn.redhat.com/errata/RHSA-2007-0746.html>
⁷⁸²³ <http://rhn.redhat.com/errata/RHSA-2007-0747.html>
⁷⁸²⁴ <http://rhn.redhat.com/errata/RHSA-2007-0911.html>
⁷⁸²⁵ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>
⁷⁸²⁶ <http://secunia.com/advisories/26636/>
⁷⁸²⁷ <http://secunia.com/advisories/26722/>
⁷⁸²⁸ <http://secunia.com/advisories/26790/>
⁷⁸²⁹ <http://secunia.com/advisories/26842/>
⁷⁸³⁰ <http://secunia.com/advisories/26952/>
⁷⁸³¹ <http://secunia.com/advisories/26993/>
⁷⁸³² <http://secunia.com/advisories/27209/>
⁷⁸³³ <http://secunia.com/advisories/27563/>

			SECUNIA 27593 ⁷⁸³⁴ SECUNIA 27732 ⁷⁸³⁵ SECUNIA 27882 ⁷⁸³⁶ SECUNIA 27971 ⁷⁸³⁷ SECUNIA 28467 ⁷⁸³⁸ SECUNIA 28606 ⁷⁸³⁹ SECUNIA 28749 ⁷⁸⁴⁰ SECUNIA 28922 ⁷⁸⁴¹ SECUNIA 29420 ⁷⁸⁴² SECUNIA 30430 ⁷⁸⁴³ SUSE SUSE- SA:2007:061 ⁷⁸⁴⁴ URL1 ⁷⁸⁴⁵		
15.	Apache HTTPD: mod_proxy_http DoS (CVE-2008-2364) (apache-httpd-cve- 2008-2364)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Otkriven je propust prilikom obrade prekomernih privremenih odgovora sa glavnog servera kada se koristi mod_proxy_http. Udaljeni napadač bi mogao da izazove odbijanje servisa ili preopterećenje memorije.	BID 29653 ⁷⁸⁴⁶ BID 31681 ⁷⁸⁴⁷ CVE CVE-2008-2364 ⁷⁸⁴⁸ OVAL OVAL11713 ⁷⁸⁴⁹ OVAL OVAL6084 ⁷⁸⁵⁰ OVAL OVAL9577 ⁷⁸⁵¹ REDHAT RHSA- 2008:0966 ⁷⁸⁵² REDHAT RHSA- 2008:0967 ⁷⁸⁵³ SECUNIA 30621 ⁷⁸⁵⁴ SECUNIA 31026 ⁷⁸⁵⁵ SECUNIA 31404 ⁷⁸⁵⁶ SECUNIA 31416 ⁷⁸⁵⁷ SECUNIA 31651 ⁷⁸⁵⁸ SECUNIA 31904 ⁷⁸⁵⁹ SECUNIA 32222 ⁷⁸⁶⁰ SECUNIA 32685 ⁷⁸⁶¹ SECUNIA 32838 ⁷⁸⁶² SECUNIA 33156 ⁷⁸⁶³ SECUNIA 33797 ⁷⁸⁶⁴ SECUNIA 34219 ⁷⁸⁶⁵ SECUNIA 34259 ⁷⁸⁶⁶ SECUNIA 34418 ⁷⁸⁶⁷	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dis t/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.9 Ažurirati na Apache HTTPD version 2.2.9 Uraditi download a zatim instalirati: http://archive.apache.org/dis t/httpd/httpd-2.2.9.tar.gz

⁷⁸³⁴ <http://secunia.com/advisories/27593/>
⁷⁸³⁵ <http://secunia.com/advisories/27732/>
⁷⁸³⁶ <http://secunia.com/advisories/27882/>
⁷⁸³⁷ <http://secunia.com/advisories/27971/>
⁷⁸³⁸ <http://secunia.com/advisories/28467/>
⁷⁸³⁹ <http://secunia.com/advisories/28606/>
⁷⁸⁴⁰ <http://secunia.com/advisories/28749/>
⁷⁸⁴¹ <http://secunia.com/advisories/28922/>
⁷⁸⁴² <http://secunia.com/advisories/29420/>
⁷⁸⁴³ <http://secunia.com/advisories/30430/>
⁷⁸⁴⁴ <https://www.suse.com/support/security/advisories/>
⁷⁸⁴⁵ http://httpd.apache.org/security/vulnerabilities_20.html
⁷⁸⁴⁶ <http://www.securityfocus.com/bid/29653>
⁷⁸⁴⁷ <http://www.securityfocus.com/bid/31681>
⁷⁸⁴⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-2364>
⁷⁸⁴⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11713>
⁷⁸⁵⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6084>
⁷⁸⁵¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9577>
⁷⁸⁵² <http://rhn.redhat.com/errata/RHSA-2008-0966.html>
⁷⁸⁵³ <http://rhn.redhat.com/errata/RHSA-2008-0967.html>
⁷⁸⁵⁴ <http://secunia.com/advisories/30621/>
⁷⁸⁵⁵ <http://secunia.com/advisories/31026/>
⁷⁸⁵⁶ <http://secunia.com/advisories/31404/>
⁷⁸⁵⁷ <http://secunia.com/advisories/31416/>
⁷⁸⁵⁸ <http://secunia.com/advisories/31651/>
⁷⁸⁵⁹ <http://secunia.com/advisories/31904/>
⁷⁸⁶⁰ <http://secunia.com/advisories/32222/>
⁷⁸⁶¹ <http://secunia.com/advisories/32685/>
⁷⁸⁶² <http://secunia.com/advisories/32838/>
⁷⁸⁶³ <http://secunia.com/advisories/33156/>
⁷⁸⁶⁴ <http://secunia.com/advisories/33797/>
⁷⁸⁶⁵ <http://secunia.com/advisories/34219/>
⁷⁸⁶⁶ <http://secunia.com/advisories/34259/>

			XF apache-modproxy-module-dos(42987) ⁷⁸⁶⁸ URL ⁷⁸⁶⁹		
16.	Apache HTTPD: Signals to arbitrary processes (CVE-2007-3304) (apache-httpd-cve-2007-3304)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Pre nego što mu je poslao signale, Apache HTTP server nije overio da li proces potiče od Apache čajlda. Lokalni napadač koji ima mogućnost da pokreće skripta na HTTP serveru, mogao bi da manipuliše semaforom za signale i da prouzrokuje okončanje proizvoljnog procesa, što bi moglo da dovede do odbijanja servisa.	BID 24215 ⁷⁸⁷⁰ CVE CVE-2007-3304 ⁷⁸⁷¹ OSVDB 38939 ⁷⁸⁷² OVAL OVAL11589 ⁷⁸⁷³ REDHAT RHSA-2007:0532 ⁷⁸⁷⁴ REDHAT RHSA-2007:0556 ⁷⁸⁷⁵ REDHAT RHSA-2007:0557 ⁷⁸⁷⁶ REDHAT RHSA-2007:0662 ⁷⁸⁷⁷ REDHAT RHSA-2008:0261 ⁷⁸⁷⁸ SECUNIA 25827 ⁷⁸⁷⁹ SECUNIA 25830 ⁷⁸⁸⁰ SECUNIA 25920 ⁷⁸⁸¹ SECUNIA 26211 ⁷⁸⁸² SECUNIA 26273 ⁷⁸⁸³ SECUNIA 26443 ⁷⁸⁸⁴ SECUNIA 26508 ⁷⁸⁸⁵ SECUNIA 26611 ⁷⁸⁸⁶ SECUNIA 26759 ⁷⁸⁸⁷ SECUNIA 26790 ⁷⁸⁸⁸ SECUNIA 26822 ⁷⁸⁸⁹ SECUNIA 26842 ⁷⁸⁹⁰ SECUNIA 26993 ⁷⁸⁹¹ SECUNIA 27121 ⁷⁸⁹² SECUNIA 27209 ⁷⁸⁹³ SECUNIA 27563 ⁷⁸⁹⁴ SECUNIA 27732 ⁷⁸⁹⁵ SECUNIA 28212 ⁷⁸⁹⁶ SECUNIA 28224 ⁷⁸⁹⁷ SECUNIA 28606 ⁷⁸⁹⁸ SGI 20070701-01-p ⁷⁸⁹⁹	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.61.tar.gz Apache HTTPD >= 1.3 and < 1.3.39 Ažurirati na Apache HTTPD version 1.3.39 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/apache-1.3.39.tar.gz Apache HTTPD >= 2.2 and < 2.2.6 Ažurirati na Apache HTTPD version 2.2.6 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz

⁷⁸⁶⁷ <http://secunia.com/advisories/34418/>⁷⁸⁶⁸ <http://xforce.iss.net/xforce/xfdb/42987>⁷⁸⁶⁹ http://httpd.apache.org/security/vulnerabilities_20.html⁷⁸⁷⁰ <http://www.securityfocus.com/bid/24215>⁷⁸⁷¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3304>⁷⁸⁷² <http://www.osvdb.org/38939>⁷⁸⁷³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11589>⁷⁸⁷⁴ <http://rhn.redhat.com/errata/RHSA-2007-0532.html>⁷⁸⁷⁵ <http://rhn.redhat.com/errata/RHSA-2007-0556.html>⁷⁸⁷⁶ <http://rhn.redhat.com/errata/RHSA-2007-0557.html>⁷⁸⁷⁷ <http://rhn.redhat.com/errata/RHSA-2007-0662.html>⁷⁸⁷⁸ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>⁷⁸⁷⁹ <http://secunia.com/advisories/25827/>⁷⁸⁸⁰ <http://secunia.com/advisories/25830/>⁷⁸⁸¹ <http://secunia.com/advisories/25920/>⁷⁸⁸² <http://secunia.com/advisories/26211/>⁷⁸⁸³ <http://secunia.com/advisories/26273/>⁷⁸⁸⁴ <http://secunia.com/advisories/26443/>⁷⁸⁸⁵ <http://secunia.com/advisories/26508/>⁷⁸⁸⁶ <http://secunia.com/advisories/26611/>⁷⁸⁸⁷ <http://secunia.com/advisories/26759/>⁷⁸⁸⁸ <http://secunia.com/advisories/26790/>⁷⁸⁸⁹ <http://secunia.com/advisories/26822/>⁷⁸⁹⁰ <http://secunia.com/advisories/26842/>⁷⁸⁹¹ <http://secunia.com/advisories/26993/>⁷⁸⁹² <http://secunia.com/advisories/27121/>⁷⁸⁹³ <http://secunia.com/advisories/27209/>⁷⁸⁹⁴ <http://secunia.com/advisories/27563/>⁷⁸⁹⁵ <http://secunia.com/advisories/27732/>⁷⁸⁹⁶ <http://secunia.com/advisories/28212/>⁷⁸⁹⁷ <http://secunia.com/advisories/28224/>⁷⁸⁹⁸ <http://secunia.com/advisories/28606/>

			SUSE SA:2007:061 ⁷⁹⁰⁰ XF apache-child-process-dos(35095) ⁷⁹⁰¹ URL1 ⁷⁹⁰²		
17.	FTP access with ftp account (ftp-generic-0001)	172.23.202.195:21 172.23.202.196:21 172.23.202.221:21 172.23.202.222:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisničkim ID-jem „ftp“ i šifrom „ftp“. Dosadašnja praksa je pokazala da treba ukloniti difoltnu naloge, ako je to moguće. Za naloge koje zahteva sistem, treba promeniti difoltnu šifru.	CVE CVE-1999-0497 ⁷⁹⁰³	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko to nije kritično za dalje funkcionisanje sistema. U suprotnom, treba promeniti lozinku u nedifoltnu vrednost.
18.	FTP access with anonymous account (ftp-generic-0002)	172.23.202.195:21 172.23.202.196:21 172.23.202.221:21 172.23.202.222:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisničkim ID-jem „anonymous“ i šifrom „ftp@“. Dosadašnja praksa je pokazala da treba ukloniti difoltnu naloge, ako je to moguće. Za naloge koje zahteva sistem, treba promeniti difoltnu šifru.	CVE CVE-1999-0497 ⁷⁹⁰⁴	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko to nije kritično za dalje funkcionisanje sistema. U suprotnom, treba promeniti lozinku u nedifoltnu vrednost.
19.	FTP server does not support AUTH command (ftp-generic-0007)	172.23.202.195:21 172.23.202.196:21 172.23.202.221:21 172.23.202.222:21 FTP klijenti po difoltu šalju FTP server-u poverljive podatke (korisnički ID i šifra) u vidu čitkog teksta. Ova okolnost dozvoljava zlonamernim korisnicima da presreću poverljive podatke ukoliko prisluškuju vezu. Noviji FTP serveri podržavaju AUTH komandu, koja omogućava dodatne opcije autentifikacije, kao što su TLS, Kerberos, GSSAPI itd. Ona se može koristiti za sprečavanje prisluškivanja na FTP vezama.		Ozbiljan	Ažurirati/preći na FTP server koji podržava AUTH komandu.
20.	Apache HTTPD: AllowOverride Options handling bypass (CVE-2009-1195) (apache-httpd-cve-2009-1195)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako web server izvršava direktivu AllowOverride sa određenim opcijama koje se koriste.	APPLE APPLE-SA-2009-11-09 ⁷⁹⁰⁵ BID 35115 ⁷⁹⁰⁶ CVE CVE-2009-1195 ⁷⁹⁰⁷ DEBIAN DSA-1816 ⁷⁹⁰⁸ OSVDB 54733 ⁷⁹⁰⁹ OVAL OVAL11094 ⁷⁹¹⁰ OVAL OVAL8704 ⁷⁹¹¹	Ozbiljan	Apache >= 2.2 and < 2.3 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

⁷⁸⁹⁹ <http://patches.sgi.com/support/free/security/advisories/20070701-01-P> pristupljeno 18.12.2011

⁷⁹⁰⁰ <https://www.suse.com/support/security/advisories/>

⁷⁹⁰¹ <http://xforce.iss.net/xforce/xfdb/35095>

⁷⁹⁰² http://httpd.apache.org/security/vulnerabilities_20.html

⁷⁹⁰³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>

⁷⁹⁰⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>

⁷⁹⁰⁵ <http://lists.apple.com/archives/security-announce/2009/Nov/msg00000.html>

⁷⁹⁰⁶ <http://www.securityfocus.com/bid/35115>

⁷⁹⁰⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1195>

⁷⁹⁰⁸ <http://www.debian.org/security/2009/dsa-1816>

⁷⁹⁰⁹ <http://osvdb.org/54733>

⁷⁹¹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11094>

⁷⁹¹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8704>

		Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u obradi direktiva „Options“ i „AllowOverride“. U konfiguracijama koje koriste direktivu „AllowOverride“ sa određenim „Options“ argumentima, lokalni korisnici mogu da izvršavaju komande iz web-serverskih skripti.	OVAL OVAL12377⁷⁹¹² REDHAT RHSA-2009:1075⁷⁹¹³ REDHAT RHSA-2009:1156⁷⁹¹⁴ SECUNIA 35261⁷⁹¹⁵ SECUNIA 35264⁷⁹¹⁶ SECUNIA 35395⁷⁹¹⁷ SECUNIA 35453⁷⁹¹⁸ SECUNIA 35721⁷⁹¹⁹ SECUNIA 37152⁷⁹²⁰ SUSE SA:2009:050⁷⁹²¹ XF apache-allowoverrides-security-bypass(50808)⁷⁹²² URL1⁷⁹²³		
21.	Apache HTTPD: mod_cache proxy DoS (CVE-2007-1863) (apache-httpd-cve-2007-1863)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Propust je otkriven u modulu mod_cache. Na sajtovima na kojima je omogućeno keširanje, udaljeni napadač bi mogao da pošalje pažljivo izrađen zahtev koji bi doveo do toga da child proces Apache-a koji to obrađuje krahira. To može dovesti samo do odbijanja servisa ako se koristi threaded MPM.	BID 24649⁷⁹²⁴ CERT TA08-150A⁷⁹²⁵ CVE CVE-2007-1863⁷⁹²⁶ OSVDB 37079⁷⁹²⁷ OVAL OVAL9824⁷⁹²⁸ REDHAT RHSA-2007:0533⁷⁹²⁹ REDHAT RHSA-2007:0534⁷⁹³⁰ REDHAT RHSA-2007:0556⁷⁹³¹ REDHAT RHSA-2007:0557⁷⁹³² SECUNIA 25830⁷⁹³³ SECUNIA 25873⁷⁹³⁴ SECUNIA 25920⁷⁹³⁵ SECUNIA 26273⁷⁹³⁶ SECUNIA 26443⁷⁹³⁷ SECUNIA 26508⁷⁹³⁸ SECUNIA 26822⁷⁹³⁹ SECUNIA 26842⁷⁹⁴⁰ SECUNIA 26993⁷⁹⁴¹ SECUNIA 27037⁷⁹⁴²	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.61.tar.gz

⁷⁹¹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12377>⁷⁹¹³ <http://rhn.redhat.com/errata/RHSA-2009-1075.html>⁷⁹¹⁴ <http://rhn.redhat.com/errata/RHSA-2009-1156.html>⁷⁹¹⁵ <http://secunia.com/advisories/35261/>⁷⁹¹⁶ <http://secunia.com/advisories/35264/>⁷⁹¹⁷ <http://secunia.com/advisories/35395/>⁷⁹¹⁸ <http://secunia.com/advisories/35453/>⁷⁹¹⁹ <http://secunia.com/advisories/35721/>⁷⁹²⁰ <http://secunia.com/advisories/37152/>⁷⁹²¹ <https://www.suse.com/support/security/advisories/>⁷⁹²² <http://xforce.iss.net/xforce/xfdb/50808>⁷⁹²³ http://httpd.apache.org/security/vulnerabilities_22.html⁷⁹²⁴ <http://www.securityfocus.com/bid/24649>⁷⁹²⁵ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>⁷⁹²⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-1863>⁷⁹²⁷ <http://www.osvdb.org/37079>⁷⁹²⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9824>⁷⁹²⁹ <http://rhn.redhat.com/errata/RHSA-2007-0533.html>⁷⁹³⁰ <http://rhn.redhat.com/errata/RHSA-2007-0534.html>⁷⁹³¹ <http://rhn.redhat.com/errata/RHSA-2007-0556.html>⁷⁹³² <http://rhn.redhat.com/errata/RHSA-2007-0557.html>⁷⁹³³ <http://secunia.com/advisories/25830/>⁷⁹³⁴ <http://secunia.com/advisories/25873/>⁷⁹³⁵ <http://secunia.com/advisories/25920/>⁷⁹³⁶ <http://secunia.com/advisories/26273/>⁷⁹³⁷ <http://secunia.com/advisories/26443/>⁷⁹³⁸ <http://secunia.com/advisories/26508/>⁷⁹³⁹ <http://secunia.com/advisories/26822/>⁷⁹⁴⁰ <http://secunia.com/advisories/26842/>⁷⁹⁴¹ <http://secunia.com/advisories/26993/>

			SECUNIA 27563 ⁷⁹⁴³ SECUNIA 27732 ⁷⁹⁴⁴ SECUNIA 28606 ⁷⁹⁴⁵ SECUNIA 30430 ⁷⁹⁴⁶ SUSE SUSE-SA:2007:061 ⁷⁹⁴⁷ URL1 ⁷⁹⁴⁸		
22.	Apache HTTPD: mod_proxy_ajp DoS (CVE-2010-0408) (apache-httpd-cve-2010-0408)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ajp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Mod_proxy_ajp će vratiti pogrešan kôd statusa ako naiđe na grešku, prouzrokujući da backend server bude stavljen u status greške dok ne istekne vreme za ponovni pokušaj. Udaljeni napadač bi mogao da pošalje zlonameran zahtev da bi pokrenuo ovaj problem, što bi dovelo do odbijanja servisa. Zahvaljujući Niku Toivola iz Sulake Corporation, ovaj problem je prijavljen uz predloženu adekvatnu meru zaštite u vidu zakrpe.	BID 38491 ⁷⁹⁴⁹ CVE CVE-2010-0408 ⁷⁹⁵⁰ DEBIAN DSA-2035 ⁷⁹⁵¹ OVAL OVAL8619 ⁷⁹⁵² OVAL OVAL9935 ⁷⁹⁵³ REDHAT RHSA-2010:0168 ⁷⁹⁵⁴ SECUNIA 39100 ⁷⁹⁵⁵ SECUNIA 39501 ⁷⁹⁵⁶ SECUNIA 39628 ⁷⁹⁵⁷ SECUNIA 39632 ⁷⁹⁵⁸ SECUNIA 39656 ⁷⁹⁵⁹ SECUNIA 40096 ⁷⁹⁶⁰ URL1 ⁷⁹⁶¹	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz
23.	Apache HTTPD: mod_proxy_ftp DoS (CVE-2009-3094) (apache-httpd-cve-2009-3094)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ftp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust NULL pointer dereference (pointer sa NULL vrednošću upotrebljen kao da ukazuje na validnu memorijsku oblast) otkriven je u modulu mod_proxy_ftp. Zlonamerni	CVE CVE-2009-3094 ⁷⁹⁶² DEBIAN DSA-1934 ⁷⁹⁶³ OVAL OVAL10981 ⁷⁹⁶⁴ OVAL OVAL8087 ⁷⁹⁶⁵ SECUNIA 36549 ⁷⁹⁶⁶ SECUNIA 37152 ⁷⁹⁶⁷ SUSE SUSE-SA:2009:050 ⁷⁹⁶⁸ URL1 ⁷⁹⁶⁹	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.14 Ažurirati na Apache HTTPD version 2.2.14 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.14.tar.gz

⁷⁹⁴² <http://secunia.com/advisories/27037/>⁷⁹⁴³ <http://secunia.com/advisories/27563/>⁷⁹⁴⁴ <http://secunia.com/advisories/27732/>⁷⁹⁴⁵ <http://secunia.com/advisories/28606/>⁷⁹⁴⁶ <http://secunia.com/advisories/30430/>⁷⁹⁴⁷ <https://www.suse.com/support/security/advisories/>⁷⁹⁴⁸ http://httpd.apache.org/security/vulnerabilities_20.html⁷⁹⁴⁹ <http://www.securityfocus.com/bid/38491>⁷⁹⁵⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0408>⁷⁹⁵¹ <http://www.debian.org/security/2010/dsa-2035>⁷⁹⁵² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8619>⁷⁹⁵³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9935>⁷⁹⁵⁴ <http://rhn.redhat.com/errata/RHSA-2010-0168.html>⁷⁹⁵⁵ <http://secunia.com/advisories/39100/>⁷⁹⁵⁶ <http://secunia.com/advisories/39501/>⁷⁹⁵⁷ <http://secunia.com/advisories/39628/>⁷⁹⁵⁸ <http://secunia.com/advisories/39632/>⁷⁹⁵⁹ <http://secunia.com/advisories/39656/>⁷⁹⁶⁰ <http://secunia.com/advisories/40096/>⁷⁹⁶¹ http://httpd.apache.org/security/vulnerabilities_22.html⁷⁹⁶² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3094>⁷⁹⁶³ <http://www.debian.org/security/2009/dsa-1934>⁷⁹⁶⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10981>⁷⁹⁶⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8087>⁷⁹⁶⁶ <http://secunia.com/advisories/36549/>⁷⁹⁶⁷ <http://secunia.com/advisories/37152/>⁷⁹⁶⁸ <https://www.suse.com/support/security/advisories/>⁷⁹⁶⁹ http://httpd.apache.org/security/vulnerabilities_22.html

		FTP server, kojem su zahtevi proksirani, mogao bi da iskoristi ovaj propust u smislu obaranja http child procesa uz pomoć izmenjenog odgovora EPSV ili PASV komandi, što bi dovelo do delimičnog odbijanja servisa.			
24.	Browsable web directory (http-generic-browsable-dir)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Otkriven je direktorijum na web serveru koji može biti pretraživan, što znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice - spajdering (prateći hiperlinkove), ili -kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute force napadom na liste uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skriven“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice. Primer: http://172.23.202.195/icons/small/ 4: <title>Index of /icons/small</title> 5: </head> 6: <body> 7: <h1>Index of /icons/small</h1> 8: ...COJ"></th><th>Name</th><th><a href="?C=M;O=A...		Ozbiljan	Za Apache: onemogućiti pretraživanje direktorijuma mreže za sve direktorijume i poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume. Za Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote: Onemogućiti pretraživanje direktorijuma za sve direktorijume i poddirektorijume. Uključiti Tomcat-ov web.xml file. U odeljku „default“, promeniti parametar „listings“ iz „true“ u „false“. Restartovati server. Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripta i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume.
25.	TCP Sequence Number Approximation	TCP reset with incorrect sequence number triggered this fault on 172.23.202.195:22	OSVDB 4030 ⁷⁹⁷⁰ BID: 10183 ⁷⁹⁷¹ CERT-VN: 415294 ⁷⁹⁷²	Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC

⁷⁹⁷⁰ <http://www.osvdb.org/4030>⁷⁹⁷¹ <http://www.securityfocus.com/bid/10183>

	Vulnerability (tcp-seq-num-approximation)	172.23.202.221:80 172.23.202.196:80 172.23.202.222:22 Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	CVE CVE-2004-0230 ⁷⁹⁷³ MS: MS05-019 ⁷⁹⁷⁴ MS: MS06-064 ⁷⁹⁷⁵ NETBSD: NetBSD-SA2004-006 ⁷⁹⁷⁶ OVAL: OVAL2689 ⁷⁹⁷⁷ OVAL: OVAL270 ⁷⁹⁷⁸ OVAL OVAL3508 ⁷⁹⁷⁹ OVAL OVAL4791 ⁷⁹⁸⁰ OVAL OVAL5711 ⁷⁹⁸¹ SECUNIA: 11440 ⁷⁹⁸² SECUNIA 11458 ⁷⁹⁸³ SECUNIA: 22341 ⁷⁹⁸⁴ SGI 20040403-01-A ⁷⁹⁸⁵ XF tcp-rst-dos(15886) ⁷⁹⁸⁶ URL1 ⁷⁹⁸⁷ URL2 ⁷⁹⁸⁸		2385 ⁷⁹⁸⁹ . Ono je napravljeno da smanji opasnost od određenih napada na BGP, kao što su TCP reseti.
26.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podesi na jedinstvenu vrednost i da se koristi u rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da fingerprint-uje operativni sistem.	BID 4314 ⁷⁹⁹⁰ CVE CVE-2002-0510 ⁷⁹⁹¹ XF linux-udp-fingerprint(8588) ⁷⁹⁹²	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili pak ranjivost koju treba popravljati, tako da ne postoje rešenja koja se mogu kupiti. Jedino se može postaviti fajervol ili neka druga sprava za filtriranje između napadnutog i neprijateljskog napada koji je u mogućnosti da randomizuje IP ID-jeve.
27.	Apache HTTPD: mod_imap XSS (CVE-2007-5000) (apache-httpd-cve-2007-5000)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je ranjiv na ovu ranjivost samo ako je pokrenuo sledeće module: mod_imagemap, mod_imap i imagemap fajl je javno dostupan. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti.	BID 26838 ⁷⁹⁹³ CERT TA08-150A ⁷⁹⁹⁴ CVE CVE-2007-5000 ⁷⁹⁹⁵ OSVDB 39134 ⁷⁹⁹⁶ OVAL OVAL9539 ⁷⁹⁹⁷ REDHAT RHSA-2008:0004 ⁷⁹⁹⁸ REDHAT RHSA-2008:0005 ⁷⁹⁹⁹ REDHAT RHSA-2008:0006 ⁸⁰⁰⁰	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.63.tar.gz Apache HTTPD >= 1.3 and < 1.3.41 Ažurirati na Apache HTTPD version 1.3.41 Uraditi download a zatim instalirati:

⁷⁹⁷² <http://www.kb.cert.org/vuls/id/415294>⁷⁹⁷³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁷⁹⁷⁴ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁷⁹⁷⁵ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁷⁹⁷⁶ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁷⁹⁷⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>⁷⁹⁷⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>⁷⁹⁷⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>⁷⁹⁸⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>⁷⁹⁸¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>⁷⁹⁸² <http://secunia.com/advisories/11440/>⁷⁹⁸³ <http://secunia.com/advisories/11458/>⁷⁹⁸⁴ <http://secunia.com/advisories/22341/>⁷⁹⁸⁵ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>⁷⁹⁸⁶ <http://xforce.iss.net/xforce/xfdb/15886>⁷⁹⁸⁷ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁷⁹⁸⁸ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>⁷⁹⁸⁹ <http://www.ietf.org/rfc/rfc2385.txt>⁷⁹⁹⁰ <http://www.securityfocus.com/bid/4314>⁷⁹⁹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>⁷⁹⁹² <http://xforce.iss.net/xforce/xfdb/8588>⁷⁹⁹³ <http://www.securityfocus.com/bid/26838>⁷⁹⁹⁴ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>⁷⁹⁹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-5000>⁷⁹⁹⁶ <http://www.osvdb.org/39134>⁷⁹⁹⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9539>⁷⁹⁹⁸ <http://rhn.redhat.com/errata/RHSA-2008-0004.html>⁷⁹⁹⁹ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>⁸⁰⁰⁰ <http://rhn.redhat.com/errata/RHSA-2008-0006.html>

		Propust je otkriven u modulu mod_imap. Na sajtovima na kojima je omogućen mod_imap i fajl imagemap je javno dostupan, moguće je izvesti napad tipa "crossite scripting attack".	REDHAT RHSA- 2008:0007 ⁸⁰⁰¹ REDHAT RHSA- 2008:0008 ⁸⁰⁰² REDHAT RHSA- 2008:0009 ⁸⁰⁰³ REDHAT RHSA- 2008:0261 ⁸⁰⁰⁴ SECUNIA 28046 ⁸⁰⁰⁵ SECUNIA 28073 ⁸⁰⁰⁶ SECUNIA 28081 ⁸⁰⁰⁷ SECUNIA 28196 ⁸⁰⁰⁸ SECUNIA 28375 ⁸⁰⁰⁹ SECUNIA 28467 ⁸⁰¹⁰ SECUNIA 28471 ⁸⁰¹¹ SECUNIA 28525 ⁸⁰¹² SECUNIA 28526 ⁸⁰¹³ SECUNIA 28607 ⁸⁰¹⁴ SECUNIA 28749 ⁸⁰¹⁵ SECUNIA 28750 ⁸⁰¹⁶ SECUNIA 28922 ⁸⁰¹⁷ SECUNIA 28977 ⁸⁰¹⁸ SECUNIA 29420 ⁸⁰¹⁹ SECUNIA 29640 ⁸⁰²⁰ SECUNIA 29806 ⁸⁰²¹ SECUNIA 29988 ⁸⁰²² SECUNIA 30356 ⁸⁰²³ SECUNIA 30430 ⁸⁰²⁴ SECUNIA 30732 ⁸⁰²⁵ SECUNIA 31142 ⁸⁰²⁶ SUSE SUSE- SA:2008:021 ⁸⁰²⁷ URL1 ⁸⁰²⁸		http://archive.apache.org/dist/httpd/apache-1.3.41.tar.gz Apache HTTPD >= 2.2 and < 2.2.8 Azurirati na Apache HTTPD version 2.2.8 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.8.tar.gz
28.	Apache HTTPD: mod_proxy_ftp globbing XSS (CVE-2008-2939) (apache-	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osjetljiv na ovu	APPLE APPLE-SA- 2009-05-12 ⁸⁰²⁹ BID 30560 ⁸⁰³⁰ CERT TA09-133A ⁸⁰³¹ CERT-VN 663763 ⁸⁰³²	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz

⁸⁰⁰¹ <http://rhn.redhat.com/errata/RHSA-2008-0007.html>⁸⁰⁰² <http://rhn.redhat.com/errata/RHSA-2008-0008.html>⁸⁰⁰³ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>⁸⁰⁰⁴ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>⁸⁰⁰⁵ <http://secunia.com/advisories/28046/>⁸⁰⁰⁶ <http://secunia.com/advisories/28073/>⁸⁰⁰⁷ <http://secunia.com/advisories/28081/>⁸⁰⁰⁸ <http://secunia.com/advisories/28196/>⁸⁰⁰⁹ <http://secunia.com/advisories/28375/>⁸⁰¹⁰ <http://secunia.com/advisories/28467/>⁸⁰¹¹ <http://secunia.com/advisories/28471/>⁸⁰¹² <http://secunia.com/advisories/28525/>⁸⁰¹³ <http://secunia.com/advisories/28526/>⁸⁰¹⁴ <http://secunia.com/advisories/28607/>⁸⁰¹⁵ <http://secunia.com/advisories/28749/>⁸⁰¹⁶ <http://secunia.com/advisories/28750/>⁸⁰¹⁷ <http://secunia.com/advisories/28922/>⁸⁰¹⁸ <http://secunia.com/advisories/28977/>⁸⁰¹⁹ <http://secunia.com/advisories/29420/>⁸⁰²⁰ <http://secunia.com/advisories/29640/>⁸⁰²¹ <http://secunia.com/advisories/29806/>⁸⁰²² <http://secunia.com/advisories/29988/>⁸⁰²³ <http://secunia.com/advisories/30356/>⁸⁰²⁴ <http://secunia.com/advisories/30430/>⁸⁰²⁵ <http://secunia.com/advisories/30732/>⁸⁰²⁶ <http://secunia.com/advisories/31142/>⁸⁰²⁷ <https://www.suse.com/support/security/advisories/>⁸⁰²⁸ http://httpd.apache.org/security/vulnerabilities_20.html⁸⁰²⁹ <http://lists.apple.com/archives/security-announce/2009/May/msg00001.html>⁸⁰³⁰ <http://www.securityfocus.com/bid/30560>⁸⁰³¹ <http://www.us-cert.gov/ncas/alerts/TA09-133A>⁸⁰³² <http://www.kb.cert.org/vuls/id/663763>

	httpd-cve-2008-2939)	ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ftp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u modulu mod_proxy_ftp prilikom obrade "wildcard-a" ukoliko se on nađe u putanji FTP URL. Ukoliko je mod_proxy_ftp omogućen da podržava FTP-over-HTTP, zahtevi koji sadrže specijalne karaktere mogu da dovedu do cross-site scripting napada (XSS).	CVE CVE-2008-2939 ⁸⁰³³ OVAL OVAL11316 ⁸⁰³⁴ OVAL OVAL7716 ⁸⁰³⁵ REDHAT RHSA-2008:0966 ⁸⁰³⁶ REDHAT RHSA-2008:0967 ⁸⁰³⁷ SECUNIA 31384 ⁸⁰³⁸ SECUNIA 31673 ⁸⁰³⁹ SECUNIA 32685 ⁸⁰⁴⁰ SECUNIA 32838 ⁸⁰⁴¹ SECUNIA 33156 ⁸⁰⁴² SECUNIA 33797 ⁸⁰⁴³ SECUNIA 34219 ⁸⁰⁴⁴ SECUNIA 35074 ⁸⁰⁴⁵ XF apache-modproxyftp-xss(44223). ⁸⁰⁴⁶ URL1 ⁸⁰⁴⁷		Apache HTTPD >= 2.2 and < 2.2.10 Ažurirati na Apache HTTPD version 2.2.10 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.10.tar.gz
29.	Apache HTTPD: mod_proxy_ftp UTF-7 XSS (CVE-2008-0005) (apache-httpd-cve-2008-0005)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osetljiv na ovu ranjivost samo ako je pokrenut modul mod_proxy_ftp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. U modul mod_proxy_ftp je dodata zaobilaznica. Na sajtovima na kojima je omogućen mod_proxy_ftp i konfigurisan je forward tipa proxy-ja, moguće je izvesti napad XSS na Web pretraživače koji neprepoznaju određeni character set prema pravilima iz dokumenta RFC 2616.	BID 27234 ⁸⁰⁴⁸ CVE CVE-2008-0005 ⁸⁰⁴⁹ OVAL OVAL10812 ⁸⁰⁵⁰ REDHAT RHSA-2008:0004 ⁸⁰⁵¹ REDHAT RHSA-2008:0005 ⁸⁰⁵² REDHAT RHSA-2008:0006 ⁸⁰⁵³ REDHAT RHSA-2008:0007 ⁸⁰⁵⁴ REDHAT RHSA-2008:0008 ⁸⁰⁵⁵ REDHAT RHSA-2008:0009 ⁸⁰⁵⁶ SECUNIA 28467 ⁸⁰⁵⁷ SECUNIA 28471 ⁸⁰⁵⁸ SECUNIA 28526 ⁸⁰⁵⁹ SECUNIA 28607 ⁸⁰⁶⁰ SECUNIA 28749 ⁸⁰⁶¹ SECUNIA 28977 ⁸⁰⁶² SECUNIA 29348 ⁸⁰⁶³	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.63.tar.gz Apache HTTPD >= 2.2 and < 2.2.8 Ažurirati na Apache HTTPD version 2.2.8 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.8.tar.gz

⁸⁰³³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-2939>
⁸⁰³⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11316>
⁸⁰³⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7716>
⁸⁰³⁶ <http://rhn.redhat.com/errata/RHSA-2008-0966.html>
⁸⁰³⁷ <http://rhn.redhat.com/errata/RHSA-2008-0967.html>
⁸⁰³⁸ <http://secunia.com/advisories/31384/>
⁸⁰³⁹ <http://secunia.com/advisories/31673/>
⁸⁰⁴⁰ <http://secunia.com/advisories/32685/>
⁸⁰⁴¹ <http://secunia.com/advisories/32838/>
⁸⁰⁴² <http://secunia.com/advisories/33156/>
⁸⁰⁴³ <http://secunia.com/advisories/33797/>
⁸⁰⁴⁴ <http://secunia.com/advisories/34219/>
⁸⁰⁴⁵ <http://secunia.com/advisories/35074/>
⁸⁰⁴⁶ <http://xforce.iss.net/xforce/xfdb/44223>
⁸⁰⁴⁷ http://httpd.apache.org/security/vulnerabilities_20.html
⁸⁰⁴⁸ <http://www.securityfocus.com/bid/27234>
⁸⁰⁴⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0005>
⁸⁰⁵⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10812>
⁸⁰⁵¹ <http://rhn.redhat.com/errata/RHSA-2008-0004.html>
⁸⁰⁵² <http://rhn.redhat.com/errata/RHSA-2008-0005.html>
⁸⁰⁵³ <http://rhn.redhat.com/errata/RHSA-2008-0006.html>
⁸⁰⁵⁴ <http://rhn.redhat.com/errata/RHSA-2008-0007.html>
⁸⁰⁵⁵ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>
⁸⁰⁵⁶ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>
⁸⁰⁵⁷ <http://secunia.com/advisories/28467/>
⁸⁰⁵⁸ <http://secunia.com/advisories/28471/>
⁸⁰⁵⁹ <http://secunia.com/advisories/28526/>
⁸⁰⁶⁰ <http://secunia.com/advisories/28607/>
⁸⁰⁶¹ <http://secunia.com/advisories/28749/>
⁸⁰⁶² <http://secunia.com/advisories/28977/>

			SECUNIA 29420 ⁸⁰⁶⁴ SECUNIA 29640 ⁸⁰⁶⁵ SECUNIA 30732 ⁸⁰⁶⁶ SECUNIA 35650 ⁸⁰⁶⁷ SUSE SUSE-SA:2008:021 ⁸⁰⁶⁸ XF apache-modproxyftp-utf7-xss(39615) URL1 ⁸⁰⁶⁹		
30.	Apache HTTPD: mod_status XSS (CVE-2007-6388) (apache-httpd-cve-2007-6388)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osetljiv na ovu ranjivost samo ako je pokrenut modul mod_status i ukoliko su stranice statusa javno dostupne. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u modulu mod_status. Na sajtovima na kojima je status servera javno dostupan, postoji mogućnost XSS napada. Stranica sa statusom servera nije po defaultu omogućena, a dosadašnja praksa je pokazala da je najbolje da ona ne bude javno dostupna.	BID 27237 ⁸⁰⁷⁰ CERT TA08-150A ⁸⁰⁷¹ CVE CVE-2007-6388 ⁸⁰⁷² OVAL OVAL10272 ⁸⁰⁷³ REDHAT RHSA-2008:0004 ⁸⁰⁷⁴ REDHAT RHSA-2008:0005 ⁸⁰⁷⁵ REDHAT RHSA-2008:0006 ⁸⁰⁷⁶ REDHAT RHSA-2008:0007 ⁸⁰⁷⁷ REDHAT RHSA-2008:0008 ⁸⁰⁷⁸ REDHAT RHSA-2008:0009 ⁸⁰⁷⁹ REDHAT RHSA-2008:0261 ⁸⁰⁸⁰ SECUNIA 28467 ⁸⁰⁸¹ SECUNIA 28471 ⁸⁰⁸² SECUNIA 28526 ⁸⁰⁸³ SECUNIA 28607 ⁸⁰⁸⁴ SECUNIA 28749 ⁸⁰⁸⁵ SECUNIA 28922 ⁸⁰⁸⁶ SECUNIA 28965 ⁸⁰⁸⁷ SECUNIA 28977 ⁸⁰⁸⁸ SECUNIA 29420 ⁸⁰⁸⁹ SECUNIA 29504 ⁸⁰⁹⁰ SECUNIA 29640 ⁸⁰⁹¹ SECUNIA 29806 ⁸⁰⁹² SECUNIA 29988 ⁸⁰⁹³	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.63.tar.gz Apache HTTPD >= 1.3 and < 1.3.41 Ažurirati na Apache HTTPD version 1.3.41 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/apache-1.3.41.tar.gz Apache HTTPD >= 2.2 and < 2.2.8 Ažurirati na Apache HTTPD version 2.2.8 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.8.tar.gz

⁸⁰⁶³ <http://secunia.com/advisories/29348/>⁸⁰⁶⁴ <http://secunia.com/advisories/29420/>⁸⁰⁶⁵ <http://secunia.com/advisories/29640/>⁸⁰⁶⁶ <http://secunia.com/advisories/30732/>⁸⁰⁶⁷ <http://secunia.com/advisories/35650/>⁸⁰⁶⁸ <https://www.suse.com/support/security/advisories/>⁸⁰⁶⁹ http://httpd.apache.org/security/vulnerabilities_20.html⁸⁰⁷⁰ <http://www.securityfocus.com/bid/27237>⁸⁰⁷¹ <http://www.cs.ait.ac.th/laboratory/CERT/TA108/msg00016.shtml>⁸⁰⁷² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6388>⁸⁰⁷³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10272>⁸⁰⁷⁴ <http://rhn.redhat.com/errata/RHSA-2008-0004.html>⁸⁰⁷⁵ <http://rhn.redhat.com/errata/RHSA-2008-0005.html>⁸⁰⁷⁶ <http://rhn.redhat.com/errata/RHSA-2008-0006.html>⁸⁰⁷⁷ <http://rhn.redhat.com/errata/RHSA-2008-0007.html>⁸⁰⁷⁸ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>⁸⁰⁷⁹ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>⁸⁰⁸⁰ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>⁸⁰⁸¹ <http://secunia.com/advisories/28467/>⁸⁰⁸² <http://secunia.com/advisories/28471/>⁸⁰⁸³ <http://secunia.com/advisories/28526/>⁸⁰⁸⁴ <http://secunia.com/advisories/28607/>⁸⁰⁸⁵ <http://secunia.com/advisories/28749/>⁸⁰⁸⁶ <http://secunia.com/advisories/28922/>⁸⁰⁸⁷ <http://secunia.com/advisories/28965/>⁸⁰⁸⁸ <http://secunia.com/advisories/28977/>⁸⁰⁸⁹ <http://secunia.com/advisories/29420/>⁸⁰⁹⁰ <http://secunia.com/advisories/29504/>⁸⁰⁹¹ <http://secunia.com/advisories/29640/>⁸⁰⁹² <http://secunia.com/advisories/29806/>

			SECUNIA 30356 ⁸⁰⁹⁴ SECUNIA 30430 ⁸⁰⁹⁵ SECUNIA 30732 ⁸⁰⁹⁶ SECUNIA 31142 ⁸⁰⁹⁷ SECUNIA 33200 ⁸⁰⁹⁸ SUSE SUSE-SA:2008:021 ⁸⁰⁹⁹ XF apache-status-page-xss(39472) ⁸¹⁰⁰		
31.	Apache HTTPD: apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpdcve-2011-0419)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osjetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_autoindex. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_fnmatch() u sklopu APR biblioteke. Ako je omogućen mod_autoindex, a indeksi direktorijuma mod_autoindex su sadržavali fajlove sa dovoljno dugim nazivima, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do preterane upotrebe CPU-a. Ovo bi moglo da bude iskorišćeno u napadu odbijanja servisa. Zahvaljujući Maksymilian Arciemowicz prijavljen je ovaj propust.	CVE CVE-2011-0419 ⁸¹⁰¹ DEBIAN DSA-2237 ⁸¹⁰² IAVM 2012-B-0056 ⁸¹⁰³ OVAL OVAL14638 ⁸¹⁰⁴ OVAL OVAL14804 ⁸¹⁰⁵ REDHAT RHSA-2011:0896 ⁸¹⁰⁶ REDHAT RHSA-2011:0897 ⁸¹⁰⁷ REDHAT RHSA-2011:0507 ⁸¹⁰⁸ SECUNIA 44490 ⁸¹⁰⁹ SECUNIA 44564 ⁸¹¹⁰ SECUNIA 44574 ⁸¹¹¹ URL1 ⁸¹¹²	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.19 Ažurirati na Apache HTTPD version 2.2.19 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.19.tar.gz
32.	Apache HTTPD: APR-util heap underwrite (CVE-2009-0023) (apache-httpd-cve-2009-0023)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osjetljiv na ovu ranjivost SAMO ako napadač poseduje posebno kreiranu ključnu reč za pretraživanje one funkcije koja upravlja kompajliranjem formi	BID 35221 ⁸¹¹³ CVE CVE-2009-0023 ⁸¹¹⁴ DEBIAN DSA-1812 ⁸¹¹⁵ OVAL OVAL10968 ⁸¹¹⁶ OVAL OVAL12321 ⁸¹¹⁷ REDHAT RHSA-2009:1107 ⁸¹¹⁸ REDHAT RHSA-2009:1108 ⁸¹¹⁹	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz

⁸⁰⁹³ <http://secunia.com/advisories/29988/>⁸⁰⁹⁴ <http://secunia.com/advisories/30356/>⁸⁰⁹⁵ <http://secunia.com/advisories/30430/>⁸⁰⁹⁶ <http://secunia.com/advisories/30732/>⁸⁰⁹⁷ <http://secunia.com/advisories/31142/>⁸⁰⁹⁸ <http://secunia.com/advisories/33200/>⁸⁰⁹⁹ <https://www.suse.com/support/security/advisories/>⁸¹⁰⁰ <http://xforce.iss.net/xforce/xfdb/39472> pristupljeno 11.12.2011⁸¹⁰¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419>⁸¹⁰² <http://www.debian.org/security/2011/dsa-2237>⁸¹⁰³ <http://iase.disa.mil/stigs/iavm-cve.html>⁸¹⁰⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14638>⁸¹⁰⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14804>⁸¹⁰⁶ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁸¹⁰⁷ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>⁸¹⁰⁸ <http://rhn.redhat.com/errata/RHSA-2011-0507.html>⁸¹⁰⁹ <http://secunia.com/advisories/44490/>⁸¹¹⁰ <http://secunia.com/advisories/44564/>⁸¹¹¹ <http://secunia.com/advisories/44574/>⁸¹¹² http://httpd.apache.org/security/vulnerabilities_22.html⁸¹¹³ <http://www.securityfocus.com/bid/35221>⁸¹¹⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-0023>⁸¹¹⁵ <http://lists.debian.org/debian-security-announce/2009/msg00124.html>⁸¹¹⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10968>⁸¹¹⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12321>⁸¹¹⁸ <http://rhn.redhat.com/errata/RHSA-2009-1107.html>⁸¹¹⁹ <http://rhn.redhat.com/errata/RHSA-2009-1108.html>

		zahtevane pretrage. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u načinu na koji komplet APR-biblioteke kompajlira forme zahtevanih pretraživanja. Napadač bi mogao da formuliše posebno izrađenu ključnu reč pretraživanja koja bi se proizvoljnim prepisivanjem gomilala u memoriji prilikom obrađivanja zahteva za pretragu.	SECUNIA 34724⁸¹²⁰ SECUNIA 35284⁸¹²¹ SECUNIA 35360⁸¹²² SECUNIA 35395⁸¹²³ SECUNIA 35444⁸¹²⁴ SECUNIA 35487⁸¹²⁵ SECUNIA 35565⁸¹²⁶ SECUNIA 35710⁸¹²⁷ SECUNIA 35797⁸¹²⁸ SECUNIA 35843⁸¹²⁹ SECUNIA 37221⁸¹³⁰ XF apache- aprstrmatchprecompile- dos(50964)⁸¹³¹ URL1⁸¹³²		
33.	Apache HTTPD: mod_proxy_balancer CSRF (CVE-2007-6420) (apache-httpd-cve-2007-6420)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Mod_proxy_balancer je omogućio administrativni interfejs koji bi mogao biti ranjiv na napade lažnih zahteva CSRF (cross-site request forgery).	BID 27236⁸¹³³ BID 31681⁸¹³⁴ CVE CVE-2007-6420⁸¹³⁵ OVAL OVAL8371⁸¹³⁶ REDHAT RHSA-2008:0966⁸¹³⁷ SECUNIA 31026⁸¹³⁸ SECUNIA 32222⁸¹³⁹ SECUNIA 33797⁸¹⁴⁰ SECUNIA 34219⁸¹⁴¹ URL1⁸¹⁴²	Ozbiljan	Apache >= 2.2 and < 2.3 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.9.tar.gz
34.	Apache HTTPD: mod_proxy_balancer DoS (CVE-2007-6422) (apache-httpd-cve-2007-6422)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Propust je otkriven u modulu mod_proxy_balancer. Na sajtovm na kojima je omogućen mod_proxy_balancer, autorizovan korisnik bi mogao poslati pažljivo izrađen zahtev koji bi doveo do toga da krahira child proces Apache-a koji	BID 27236⁸¹⁴³ CVE CVE-2007-6422⁸¹⁴⁴ OVAL OVAL10181⁸¹⁴⁵ OVAL OVAL8690⁸¹⁴⁶ REDHAT RHSA-2008:0008⁸¹⁴⁷ REDHAT RHSA-2008:0009⁸¹⁴⁸ SECUNIA 28526⁸¹⁴⁹ SECUNIA 28749⁸¹⁵⁰ SECUNIA 28977⁸¹⁵¹	Ozbiljan	Apache >= 2.2 and < 2.3 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.8.tar.gz

⁸¹²⁰ <http://secunia.com/advisories/34724/>
⁸¹²¹ <http://secunia.com/advisories/35284/>
⁸¹²² <http://secunia.com/advisories/35360/>
⁸¹²³ <http://secunia.com/advisories/35395/>
⁸¹²⁴ <http://secunia.com/advisories/35444/>
⁸¹²⁵ <http://secunia.com/advisories/35487/>
⁸¹²⁶ <http://secunia.com/advisories/35565/>
⁸¹²⁷ <http://secunia.com/advisories/35710/>
⁸¹²⁸ <http://secunia.com/advisories/35797/>
⁸¹²⁹ <http://secunia.com/advisories/35843/>
⁸¹³⁰ <http://secunia.com/advisories/37221/>
⁸¹³¹ <http://xforce.iss.net/xforce/xfdb/50964>
⁸¹³² http://httpd.apache.org/security/vulnerabilities_22.html
⁸¹³³ <http://www.securityfocus.com/bid/27236>
⁸¹³⁴ <http://www.securityfocus.com/bid/31681>
⁸¹³⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6420>
⁸¹³⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8371>
⁸¹³⁷ <http://rhn.redhat.com/errata/RHSA-2008-0966.html>
⁸¹³⁸ <http://secunia.com/advisories/31026/>
⁸¹³⁹ <http://secunia.com/advisories/32222/>
⁸¹⁴⁰ <http://secunia.com/advisories/33797/>
⁸¹⁴¹ <http://secunia.com/advisories/34219/>
⁸¹⁴² http://httpd.apache.org/security/vulnerabilities_22.html
⁸¹⁴³ <http://www.securityfocus.com/bid/27236>
⁸¹⁴⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6422>
⁸¹⁴⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10181>
⁸¹⁴⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8690>
⁸¹⁴⁷ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>
⁸¹⁴⁸ <http://rhn.redhat.com/errata/RHSA-2008-0009.html>
⁸¹⁴⁹ <http://secunia.com/advisories/28526/>
⁸¹⁵⁰ <http://secunia.com/advisories/28749/>
⁸¹⁵¹ <http://secunia.com/advisories/28977/>

		taj zahtev obrađuje. To može dovesti samo do odbijanja servisa ako se koristi threaded MPM.	SECUNIA 29348 ⁸¹⁵² SECUNIA 29640 ⁸¹⁵³ SUSE SUSE-SA:2008:021 ⁸¹⁵⁴ XF apache-modproxybalancer-dos(39476) ⁸¹⁵⁵ URL1 ⁸¹⁵⁶		
35.	Apache HTTPD: mod_proxy_balancer XSS (CVE-2007-6421) (apache-httpd-cve-2007-6421)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Propust je otkriven u modulu mod_proxy_balancer. Na sajtovmu na kojima je omogućen mod_proxy_balancer, moguć je XSS napad prema autorizovanom korisniku.	BID 27236 ⁸¹⁵⁷ CVE CVE-2007-6421 ⁸¹⁵⁸ OVAL OVAL10664 ⁸¹⁵⁹ OVAL OVAL8651 ⁸¹⁶⁰ REDHAT RHSA-2008:0008 ⁸¹⁶¹ REDHAT RHSA-2008:0009 ⁸¹⁶² SECUNIA 28526 ⁸¹⁶³ SECUNIA 28749 ⁸¹⁶⁴ SECUNIA 28977 ⁸¹⁶⁵ SECUNIA 29420 ⁸¹⁶⁶ SECUNIA 29640 ⁸¹⁶⁷ SUSE SUSE-SA:2008:021 ⁸¹⁶⁸ XF apache-modproxybalancer-dos(39476) ⁸¹⁶⁹ URL1 ⁸¹⁷⁰	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.8.tar.gz
36.	Apache HTTPD: mod_status cross-site scripting (CVE-2006-5752) (apache-httpd-cve-2006-5752)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osjetljiv na ovu ranjivost samo ako je pokrenut modul mod_status i ukoliko su stranice statusa javno dostupan. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u modulu mod_status. Na sajtovmu na kojima je status servera javno dostupan i omogućen je ExtendedStatus, postoji mogućnost XSS napada. Stranica sa	OSVDB 37052 ⁸¹⁷¹ BID 24645 ⁸¹⁷² CVE CVE-2006-5752 ⁸¹⁷³ OVAL OVAL10154 ⁸¹⁷⁴ REDHAT RHSA-2007:0532 ⁸¹⁷⁵ REDHAT RHSA-2007:0533 ⁸¹⁷⁶ REDHAT RHSA-2007:0534 ⁸¹⁷⁷ REDHAT RHSA-2007:0556 ⁸¹⁷⁸ REDHAT RHSA-2007:0557 ⁸¹⁷⁹ REDHAT RHSA-	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.61.tar.gz Apache HTTPD >= 1.3 and < 1.3.39 Ažurirati na Apache HTTPD version 1.3.39 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/apache-1.3.39.tar.gz Apache HTTPD >= 2.2 and < 2.2.6

⁸¹⁵² <http://secunia.com/advisories/29348/>⁸¹⁵³ <http://secunia.com/advisories/29640/>⁸¹⁵⁴ <https://www.suse.com/support/security/advisories/>⁸¹⁵⁵ <http://xforce.iss.net/xforce/xfdb/39476>⁸¹⁵⁶ http://httpd.apache.org/security/vulnerabilities_22.html⁸¹⁵⁷ <http://www.securityfocus.com/bid/27236>⁸¹⁵⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6421>⁸¹⁵⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10664>⁸¹⁶⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8651>⁸¹⁶¹ <http://rhn.redhat.com/errata/RHSA-2008-0008.html>⁸¹⁶² <http://rhn.redhat.com/errata/RHSA-2008-0009.html>⁸¹⁶³ <http://secunia.com/advisories/28526/>⁸¹⁶⁴ <http://secunia.com/advisories/28749/>⁸¹⁶⁵ <http://secunia.com/advisories/28977/>⁸¹⁶⁶ <http://secunia.com/advisories/29420/>⁸¹⁶⁷ <http://secunia.com/advisories/29640/>⁸¹⁶⁸ <https://www.suse.com/support/security/advisories/>⁸¹⁶⁹ <http://xforce.iss.net/xforce/xfdb/39476>⁸¹⁷⁰ http://httpd.apache.org/security/vulnerabilities_22.html⁸¹⁷¹ <http://www.osvdb.org/37052>⁸¹⁷² <http://www.securityfocus.com/bid/24645>⁸¹⁷³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-5752>⁸¹⁷⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10154>⁸¹⁷⁵ <http://rhn.redhat.com/errata/RHSA-2007-0532.html>⁸¹⁷⁶ <http://rhn.redhat.com/errata/RHSA-2007-0533.html>⁸¹⁷⁷ <http://rhn.redhat.com/errata/RHSA-2007-0534.html>⁸¹⁷⁸ <http://rhn.redhat.com/errata/RHSA-2007-0556.html>⁸¹⁷⁹ <http://rhn.redhat.com/errata/RHSA-2007-0557.html>

		statusom servera nije po difoltu omogućena, a dosadašnja praksa je pokazala da je najbolje da ona ne bude javno dostupna.	2008:0261 ⁸¹⁸⁰ SECUNIA 25827 ⁸¹⁸¹ SECUNIA 25830 ⁸¹⁸² SECUNIA 25873 ⁸¹⁸³ SECUNIA 25920 ⁸¹⁸⁴ SECUNIA 26273 ⁸¹⁸⁵ SECUNIA 26443 ⁸¹⁸⁶ SECUNIA 26458 ⁸¹⁸⁷ SECUNIA 26508 ⁸¹⁸⁸ SECUNIA 26822 ⁸¹⁸⁹ SECUNIA 26842 ⁸¹⁹⁰ SECUNIA 26993 ⁸¹⁹¹ SECUNIA 27037 ⁸¹⁹² SECUNIA 27563 ⁸¹⁹³ SECUNIA 27732 ⁸¹⁹⁴ SECUNIA 28212 ⁸¹⁹⁵ SECUNIA 28224 ⁸¹⁹⁶ SECUNIA 28606 ⁸¹⁹⁷ SUSE SA:2007:061 ⁸¹⁹⁸ XF apache-modstatus-xss(35097) URL1 ⁸¹⁹⁹		Ažurirati na Apache HTTPD version 2.2.6 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.6.tar.gz
37.	Apache HTTPD: Subrequest handling of request headers (mod_headers) (CVE-2010-0434) (apache-httpdcve-2010-0434)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_headers. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust u jezgru "subrequest process code" može dovesti do greške tipa segmentation fault-a ili do otkrivanja podataka iz nekog drugog zahteva na thread-ovima servera, kao što su worker ili winnt MPM-ovi.	APPLE APPLE-SA-2010-11-10 ⁸²⁰⁰ BID 38494 ⁸²⁰¹ CVE CVE-2010-0434 ⁸²⁰² DEBIAN DSA-2035 ⁸²⁰³ OVAL OVAL10358 ⁸²⁰⁴ OVAL OVAL8695 ⁸²⁰⁵ REDHAT RHSA-2010:0168 ⁸²⁰⁶ REDHAT RHSA-2010:0175 ⁸²⁰⁷ SECUNIA 39100 ⁸²⁰⁸ SECUNIA 39115 ⁸²⁰⁹ SECUNIA 39501 ⁸²¹⁰ SECUNIA 39628 ⁸²¹¹	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.15 Ažurirati na Apache HTTPD version 2.2.15 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz

⁸¹⁸⁰ <http://rhn.redhat.com/errata/RHSA-2008-0261.html>⁸¹⁸¹ <http://secunia.com/advisories/25827/>⁸¹⁸² <http://secunia.com/advisories/25830/>⁸¹⁸³ <http://secunia.com/advisories/25873/>⁸¹⁸⁴ <http://secunia.com/advisories/25920/>⁸¹⁸⁵ <http://secunia.com/advisories/26273/>⁸¹⁸⁶ <http://secunia.com/advisories/26443/>⁸¹⁸⁷ <http://secunia.com/advisories/26458/>⁸¹⁸⁸ <http://secunia.com/advisories/26508/>⁸¹⁸⁹ <http://secunia.com/advisories/26822/>⁸¹⁹⁰ <http://secunia.com/advisories/26842/>⁸¹⁹¹ <http://secunia.com/advisories/26993/>⁸¹⁹² <http://secunia.com/advisories/27037/>⁸¹⁹³ <http://secunia.com/advisories/27563/>⁸¹⁹⁴ <http://secunia.com/advisories/27732/>⁸¹⁹⁵ <http://secunia.com/advisories/28212/>⁸¹⁹⁶ <http://secunia.com/advisories/28224/>⁸¹⁹⁷ <http://secunia.com/advisories/28606/>⁸¹⁹⁸ <https://www.suse.com/support/security/advisories/>⁸¹⁹⁹ http://httpd.apache.org/security/vulnerabilities_20.html⁸²⁰⁰ <http://support.apple.com/kb/ht4435>⁸²⁰¹ <http://www.securityfocus.com/bid/38494>⁸²⁰² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0434>⁸²⁰³ <http://www.debian.org/security/2010/dsa-2035>⁸²⁰⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10358>⁸²⁰⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8695>⁸²⁰⁶ <http://rhn.redhat.com/errata/RHSA-2010-0168.html>⁸²⁰⁷ <http://rhn.redhat.com/errata/RHSA-2010-0175.html>⁸²⁰⁸ <http://secunia.com/advisories/39100/>⁸²⁰⁹ <http://secunia.com/advisories/39115/>⁸²¹⁰ <http://secunia.com/advisories/39501/>⁸²¹¹ <http://secunia.com/advisories/39628/>

		Zahvaljujući Philip Pickett-u iz Vmware, ovaj propust je prijavljen i predložen je način ispravke.	SECUNIA 39632 ⁸²¹² SECUNIA 39656 ⁸²¹³ SECUNIA 40096 ⁸²¹⁴ XF apache-http-rh-info-disclosure(56625) ⁸²¹⁵ URL1 ⁸²¹⁶		
38.	OpenSSH CBC Mode Information Disclosure Vulnerability (ssh-openssh-cbc-mode-info-disclosure)	172.23.202.195:22 172.23.202.196:22 172.23.202.221:22 172.23.202.222:22 Određene verzije OpenSSH-a poseduju ranjivu implementaciju bloka šifarskog algoritma u CBC modu (Cipher Block Chaining). Ovo bi udaljenom napadaču moglo omogućiti da preko nepoznatih vektora pridobije određene podatke u vidu običnog teksta iz proizvoljnog bloka šifrovanog teksta u SSH sesiji.	BID 32319 ⁸²¹⁷ CVE CVE-2008-5161 ⁸²¹⁸ SECUNIA 32760 ⁸²¹⁹ URL1 ⁸²²⁰ URL2 ⁸²²¹	Ozbiljan	Uraditi download a zatim instalirati: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-5.2p1.tar.gz Verzija 5.2 OpenSSH-a je puštena u promet 22. februara 2009.
39.	OpenSSH „X11UseLocalhost“ X11 Forwarding Session Hijacking Vulnerability (ssh-opensshx11uselocalhost - x11-forwarding-session-hijack)	172.23.202.195:22 172.23.202.196:22 172.23.202.221:22 172.23.202.222:22 Određene verzije OpenSSH-a podešavaju SO_REUSEADDR soket opciju kada je onemogućeno podešavanje X11UseLocalhost konfiguracije. Ovo bi lokalnom napadaču moglo da omogući da preuzme X11 forwarding port preko veze ka pojedinačnoj IP adresi.	BID 30339 ⁸²²² CVE CVE-2008-3259 ⁸²²³ SECUNIA 31179 ⁸²²⁴	Ozbiljan	Uraditi download a zatim instalirati: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-5.1p1.tar.gz Verzija 5.1 OpenSSH-a je puštena u promet 21. jula 2008.
40.	HTTP TRACE Method Enabled (http-trace-method-enabled)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 HTTP TRACE metoda se obično koristi da uzvрати potpuni HTTP zahtev klijentu koji ga zahteva, u cilju debugovanja proxy servera. Napadač bi mogao da kreira web stranicu koristeći XMLHttpRequest, ActiveX ili XMLHttpRequest da natera klijenta da pošalje TRACE zahtev i	CERT-VN 867593 ⁸²²⁵ OSVDB 35511 ⁸²²⁶ OSVDB 3726 ⁸²²⁷ SECUNIA 10726 ⁸²²⁸ SECUNIA 17334 ⁸²²⁹ SECUNIA 21802 ⁸²³⁰ SECUNIA 25636 ⁸²³¹ CVE CVE-2004-2320 ⁸²³² CVE CVE-2004-2763 ⁸²³³ CVE CVE-2005-3398 ⁸²³⁴ CVE CVE-2006-4683 ⁸²³⁵ CVE CVE-2007-3008 ⁸²³⁶	Ozbiljan	Apache Onemogućiti HTTP TRACE metodu za Apache. Novije verzije Apache-a (1.3.34 i 2.0.55 i novije) omogućuju konfiguracionu direktivu koja se zove TraceEnable. Da bi se odbili TRACE zahtevi, dodaje se sledeći red u konfiguraciju servera: TraceEnable off

⁸²¹² <http://secunia.com/advisories/39632/>⁸²¹³ <http://secunia.com/advisories/39656/>⁸²¹⁴ <http://secunia.com/advisories/40096/>⁸²¹⁵ <http://xforce.iss.net/xforce/xfdb/56625>⁸²¹⁶ http://httpd.apache.org/security/vulnerabilities_20.html⁸²¹⁷ <http://www.securityfocus.com/bid/32319>⁸²¹⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-5161>⁸²¹⁹ <http://secunia.com/advisories/32760/>⁸²²⁰ http://www.cpni.gov.uk/Docs/Vulnerability_Advisory_SSH.txt, pristupljeno 20.12.2011⁸²²¹ <http://www.openssh.com/txt/cbc.adv>⁸²²² <http://www.securityfocus.com/bid/30339>⁸²²³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-3259>⁸²²⁴ <http://secunia.com/advisories/31179/>⁸²²⁵ <http://www.kb.cert.org/vuls/id/867593>⁸²²⁶ <http://www.osvdb.org/35511>⁸²²⁷ <http://www.osvdb.org/3726>⁸²²⁸ <http://secunia.com/advisories/10726/>⁸²²⁹ <http://secunia.com/advisories/17334/>⁸²³⁰ <http://secunia.com/advisories/21802/>⁸²³¹ <http://secunia.com/advisories/25636/>⁸²³² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2320>⁸²³³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2763>⁸²³⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-3398>⁸²³⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-4683>⁸²³⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3008>

		da sačuva klijenove kolačiće. Kao posledica može da se javi XSS napad. Primer: 172.23.202.196:80 Running vulnerable HTTP service. http://172.23.202.195/ 1: TRACE / HTTP/1.1 2: Host: 172.23.202.195 3: Cookie: vulnerable=yes	CVE CVE-2008-7253 ⁸²³⁷ CVE CVE-2009-2823 ⁸²³⁸ CVE CVE-2010-0386 ⁸²³⁹ OSVDB 877 ⁸²⁴⁰ SUN 50603 ⁸²⁴¹ BID 9561 ⁸²⁴² URL1 ⁸²⁴³ URL2 ⁸²⁴⁴		Za starije verzije Apache web servera, koristiti modul mod_rewrite da bi se odbili TRACE zahteve: RewriteEngine On RewriteCond %{REQUEST_METHOD} ^TRACE RewriteRule .* - [F]
41.	Database Open Access (database-open-access)	172.23.202.195: 3306 172.23.202.196: 3306 172.23.202.221: 3306 172.23.202.222: 3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7.	URL1 ⁸²⁴⁵	Umeren	Konfigurisati server baze podataka tako da dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.
42.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatišu slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeci ICMP-ov zahtev za vremenski pečat.	CVE CVE-1999-0524 ⁸²⁴⁶ OSVDB 95 ⁸²⁴⁷ XF icmp-netmask(306) ⁸²⁴⁸ XF icmp-timestamp(322) ⁸²⁴⁹	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
43.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1 ⁸²⁵⁰ URL2 ⁸²⁵¹ URL3 ⁸²⁵²	Umeren	Onemogućavanje TCP timestamp odgovora na Linux OS. Podesiti net.ipv4.tcp_timestamps vrednost na sledećem ključu na 0 pokretanjem sledeće komande: sysctl -w net.ipv4.tcp_timestamps=0 Dodatno, sledeću vrednost u

⁸²³⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-7253>⁸²³⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2823>⁸²³⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0386>⁸²⁴⁰ <http://osvdb.org/887>⁸²⁴¹ <https://sunsolve.sun.com/search/document.do?assetkey=1-22-50603-1> pristupljeno 18.12.2011⁸²⁴² <http://www.securityfocus.com/bid/9561>⁸²⁴³ <http://www.apacheweek.com/issues/03-01-24#news>⁸²⁴⁴ <http://www.kb.cert.org/vuls/id/867593>⁸²⁴⁵ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf⁸²⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁸²⁴⁷ <http://www.osvdb.org/95>⁸²⁴⁸ <http://xforce.iss.net/xforce/xfdb/306>⁸²⁴⁹ <http://xforce.iss.net/xforce/xfdb/322>⁸²⁵⁰ http://www.forensicswiki.org/wiki/TCP_timestamps⁸²⁵¹ <http://www.ietf.org/rfc/rfc1323.txt>⁸²⁵² <http://uptime.netcraft.com/>

					difoltnom sysctl konfiguracionom fajlu, generally sysctl.conf: net.ipv4.tcp_timestamps=0
44.	WebDAV Extensions are Enabled (http-generic-webdav-enabled)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 WebDAV je skup ekstenzija za HTTP protokol koji omogućava korisnicima da zajednički edituju i obrađuju fajlove na udaljenim web serverima. Mnogi web serveri po difoltu omogućavaju WebDAV ekstenzije, čak i kada nisu potrebne. S obzirom na dodatnu složenost, dosadašnja praksa je pokazala da treba onemogućiti WebDAV ukoliko se trenutno ne koristi.		Umeren	Apache: Potrebno je onemogućiti WebDAV (eng. Web-based Distributed Authoring and Versioning) za Apache. Proveriti da li je mod_dav modul isključen ili utvrditi da li postoji zahtevana autentifikacija na direktorijumima nad kojima se zahteva DAV.
45.	Apache HTTPD: CRLF injection in mod_negotiation when untrusted uploads are supported (CVE-2008-0456) (apache-httpd-cve-2008-0456)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_negotiation. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Moguće je ubaciti CRLF (Carriage Return and Line Feed) koji omogućava CRLF Injection napade (poznatih i kao HTTP Response Splitting) za sajtove koji koriste mod_negotiation, omogućavajući neproverene upload-ove na lokacije na kojima je omogućen MultiViews (višestruko pregledanje).	APPLE APPLE-SA-2009-05-12 ⁸²⁵³ BID 27409 ⁸²⁵⁴ CERT TA09-133A ⁸²⁵⁵ CVE CVE-2008-0456 ⁸²⁵⁶ REDHAT RHSA-2013:0130 ⁸²⁵⁷ SECUNIA 29348 ⁸²⁵⁸ SECUNIA 35074 ⁸²⁵⁹ XF 39893 ⁸²⁶⁰ URL1 ⁸²⁶¹	Umeren	Apache HTTPD >= 2.2 and < 2.2.12 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.12.tar.gz
46.	Apache HTTPD: insecure LD_LIBRARY_PATH handling (CVE-2012-0883) (apache-httpd-cve-2012-0883)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Otkrivena je nebezbedna obrada rute LD_LIBRARY_PATH koja bi mogla da dovede do toga da direktorijum koji trenutno radi traži DSO-ove. Ovo bi lokalnom korisniku omogućilo da izvrši kôd kao root ako je administrator pokrenuo apachectl sa nepoverljivog direktorijuma.	APPLE APPLE-SA-2013-09-12-1 ⁸²⁶² CVE CVE-2012-0883 ⁸²⁶³ SECUNIA 48849 ⁸²⁶⁴ URL1 ⁸²⁶⁵ URL2 ⁸²⁶⁶	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.23 Ažurirati na Apache HTTPD version 2.2.23 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz Apache HTTPD >= 2.4 and < 2.4.2 Ažurirati na Apache HTTPD version 2.4.2 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.2.tar.gz

⁸²⁵³ <http://lists.apple.com/archives/security-announce/2009/May/msg00001.html>⁸²⁵⁴ <http://www.securityfocus.com/bid/27409>⁸²⁵⁵ <http://www.us-cert.gov/ncas/alerts/ta09-133a>⁸²⁵⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0456>⁸²⁵⁷ <http://rhn.redhat.com/errata/RHSA-2013-0130.html>⁸²⁵⁸ <http://secunia.com/advisories/29348/>⁸²⁵⁹ <http://secunia.com/advisories/35074/>⁸²⁶⁰ <http://xforce.iss.net/xforce/xfdb/39893>⁸²⁶¹ http://httpd.apache.org/security/vulnerabilities_22.html⁸²⁶² <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁸²⁶³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0883>⁸²⁶⁴ <http://secunia.com/advisories/48849/>⁸²⁶⁵ http://httpd.apache.org/security/vulnerabilities_22.html⁸²⁶⁶ http://httpd.apache.org/security/vulnerabilities_24.html

47.	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368) (apache-httpd-cve-2011-3368)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja prisustva mod_proxy modula. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy. Zlonamerni napadač bi mogao da iskoristi ovaj propust na takav način da primora proxy proces da se poveže sa proizvoljnim serverom i potencijalno objavi osetljive informacije sa internih web servera koje inače napadaču nisu direktno dostupne. Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/	APPLE APPLE-SA-2012-09-19-2 ⁸²⁶⁷ BID 49957 ⁸²⁶⁸ CVE CVE-2011-3368 ⁸²⁶⁹ IAVM 2012-A-0017 ⁸²⁷⁰ IAVM 2012-A-0152 ⁸²⁷¹ IAVM 2012-B-0056 ⁸²⁷² OSVDB 76079 ⁸²⁷³ REDHAT RHSA-2011:1391 ⁸²⁷⁴ REDHAT RHSA-2011:1392 ⁸²⁷⁵ SECUNIA 46288 ⁸²⁷⁶ SECUNIA 46414 ⁸²⁷⁷ SECUNIA 48551 ⁸²⁷⁸ XF 70336 ⁸²⁷⁹ URL1 ⁸²⁸⁰ URL2 ⁸²⁸¹ URL3 ⁸²⁸²	Ozbiljan	Apache HTTPD >= 1.3 and < 2 Primeniti zakrpu za CVE-2011-3368 to 1.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
48.	Apache HTTPD: scoreboard parent DoS (CVE-2012-0031) (apache-httpd-cve-2012-0031)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Propust je otkriven u obradi scoreboard-a. Neprivilegovani child proces bi mogao da dovede do toga da parent proces krahira prilikom gašenja.	APPLE APPLE-SA-2012-09-19-2 ⁸²⁸³ BID 51407 ⁸²⁸⁴ CVE CVE-2012-0031 ⁸²⁸⁵ IAVM 2012-A-0017 ⁸²⁸⁶ REDHAT RHSA-2012:0128 ⁸²⁸⁷ SECUNIA 47410 ⁸²⁸⁸ SECUNIA 48551 ⁸²⁸⁹ URL1 ⁸²⁹⁰ URL2 ⁸²⁹¹	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim

⁸²⁶⁷ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁸²⁶⁸ <http://www.securityfocus.com/bid/49957>⁸²⁶⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3368>⁸²⁷⁰ <http://iase.disa.mil/stigs/iavm-cve.html>⁸²⁷¹ <http://iase.disa.mil/stigs/iavm-cve.html>⁸²⁷² <http://iase.disa.mil/stigs/iavm-cve.html>⁸²⁷³ <http://www.osvdb.org/76079>⁸²⁷⁴ <http://rhn.redhat.com/errata/RHSA-2011-1391.html>⁸²⁷⁵ <http://rhn.redhat.com/errata/RHSA-2011-1392.html>⁸²⁷⁶ <http://secunia.com/advisories/46288/>⁸²⁷⁷ <http://secunia.com/advisories/46414/>⁸²⁷⁸ <http://secunia.com/advisories/48551/>⁸²⁷⁹ <http://xforce.iss.net/xforce/xfdb/70336>⁸²⁸⁰ http://httpd.apache.org/security/vulnerabilities_13.html⁸²⁸¹ http://httpd.apache.org/security/vulnerabilities_20.html⁸²⁸² http://httpd.apache.org/security/vulnerabilities_22.html⁸²⁸³ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁸²⁸⁴ <http://www.securityfocus.com/bid/51407>⁸²⁸⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0031>⁸²⁸⁶ <http://iase.disa.mil/stigs/iavm-cve.html>⁸²⁸⁷ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁸²⁸⁸ <http://secunia.com/advisories/47410/>⁸²⁸⁹ <http://secunia.com/advisories/48551/>⁸²⁹⁰ http://httpd.apache.org/security/vulnerabilities_20.html⁸²⁹¹ http://httpd.apache.org/security/vulnerabilities_22.html

					instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
49.	Apache HTTPD: mod_rewrite log escape filtering (CVE-2013-1862) (apache-httpd-cve-2013-1862)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_rewrite. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Modul mod_rewrite ne filtrira završne izlazne sekvence iz logova, što zlonamenrom napadaču olakšava da ubace takve sekvence u završne emulatore koji sadrže ranjivosti koje se odnose na izlazne sekvence.	CVE CVE-2013-1862 ⁸²⁹² OVAL OVAL18790 ⁸²⁹³ REDHAT RHSA-2013:0815 ⁸²⁹⁴ REDHAT RHSA-2013:1207 ⁸²⁹⁵ REDHAT RHSA-2013:1208 ⁸²⁹⁶ REDHAT RHSA-2013:1209 ⁸²⁹⁷ SECUNIA 55032 ⁸²⁹⁸ URL1 ⁸²⁹⁹ URL2 ⁸³⁰⁰	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.25 Ažurirati na Apache HTTPD version 2.2.25 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.25.tar.gz
50.	Apache HTTPD: mod_setenvif .htaccess privilege escalation (CVE-2011-3607) (apache-httpd-cve-2011-3607)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_setenvif. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust preopterećenja je otkriven kada je omogućen modul mod_setenvif, što lokalnim korisnicima omogućava da dobiju privilegije preko fajla .htaccess.	APPLE APPLE-SA-2012-09-19-2 ⁸³⁰¹ BID 50494 ⁸³⁰² CVE CVE-2011-3607 ⁸³⁰³ IAVM 2012-A-0017 ⁸³⁰⁴ IAVM 2012-A-0152 ⁸³⁰⁵ OSVDB 76744 REDHAT RHSA-2012:0128 ⁸³⁰⁶ SECUNIA 45793 ⁸³⁰⁷ SECUNIA 48551 ⁸³⁰⁸ XF 71093 ⁸³⁰⁹ URL1 ⁸³¹⁰ URL2 ⁸³¹¹	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
51.	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-4317) (apache-httpd-cve-2011-4317)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osjetljiv na ovu ranjivost samo ako je pokrenut modul mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja ove	APPLE APPLE-SA-2012-09-19-2 ⁸³¹² CVE CVE-2011-4317 ⁸³¹³ IAVM 2012-A-0017 ⁸³¹⁴ IAVM 2012-A-0152 ⁸³¹⁵ REDHAT RHSA-2012:0128 ⁸³¹⁶ SECUNIA 48551 ⁸³¹⁷	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz

⁸²⁹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1862>
⁸²⁹³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18790>
⁸²⁹⁴ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>
⁸²⁹⁵ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>
⁸²⁹⁶ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>
⁸²⁹⁷ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>
⁸²⁹⁸ <http://secunia.com/advisories/55032/>
⁸²⁹⁹ http://httpd.apache.org/security/vulnerabilities_20.html
⁸³⁰⁰ http://httpd.apache.org/security/vulnerabilities_22.html
⁸³⁰¹ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>
⁸³⁰² <http://www.securityfocus.com/bid/50494>
⁸³⁰³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3607>
⁸³⁰⁴ <http://iase.disa.mil/stigs/iavm-cve.html>
⁸³⁰⁵ <http://iase.disa.mil/stigs/iavm-cve.html>
⁸³⁰⁶ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>
⁸³⁰⁷ <http://secunia.com/advisories/45793/>
⁸³⁰⁸ <http://secunia.com/advisories/48551/>
⁸³⁰⁹ <http://xforce.iss.net/xforce/xfdb/71093>
⁸³¹⁰ http://httpd.apache.org/security/vulnerabilities_20.html
⁸³¹¹ http://httpd.apache.org/security/vulnerabilities_22.html
⁸³¹² <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>
⁸³¹³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4317>
⁸³¹⁴ <http://iase.disa.mil/stigs/iavm-cve.html>
⁸³¹⁵ <http://iase.disa.mil/stigs/iavm-cve.html>
⁸³¹⁶ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>
⁸³¹⁷ <http://secunia.com/advisories/48551/>

		moćnosti. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy U određenim konfiguracijama koje koriste RewriteRule sa proxy flag-om ili ProxyPassMatch, udaljeni napadač bi mogao da primora reverzni proksi da se poveže sa proizvoljnim serverom i potencijalno objavi osetljive informacije sa internih web servera koje inače napadaču nisu direktno dostupne.	URL⁸³¹⁸		
52.	Apache HTTPD: error responses can expose cookies (CVE-2012-0053) (apache-httpd-cve-2012-0053)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Propust je otkriven u difoltnom pogrešnom odgovoru za statusni kôd 400. Zlonamerni napadač bi mogao da iskoristi ovaj propust da objavi "httpOnly" kolačiće ako nije određen dokument custom ErrorDocument.	APPLE APPLE-SA-2012-09-19-2⁸³¹⁹ BID 51706⁸³²⁰ CVE CVE-2012-0053⁸³²¹ IAVM 2012-A-0017⁸³²² REDHAT RHSA-2012:0128⁸³²³ SECUNIA 48551⁸³²⁴ URL1⁸³²⁵ URL2⁸³²⁶	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
53.	Apache HTTPD: XSS due to unescaped hostnames (CVE-2012-3499) (apache-httpd-cve-2012-3499)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut jedan od sledećih modula: mod_imagemap, mod_info, mod_ldap, mod_proxy_ftp, mod_status. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Različiti XSS propusti usled nenapuštenih host imena i URI-ja HTML output-a u mod_info, mod_status, mod_imagemap, mod_ldap i mod_proxy_ftp.	APPLE APPLE-SA-2013-09-12-1⁸³²⁷ CVE CVE-2012-3499⁸³²⁸ DEBIAN DSA-2637⁸³²⁹ REDHAT RHSA-2013:0815⁸³³⁰ REDHAT RHSA-2013:1207⁸³³¹ REDHAT RHSA-2013:1208⁸³³² REDHAT RHSA-2013:1209⁸³³³ SECUNIA 55032⁸³³⁴ URL1⁸³³⁵ URL2⁸³³⁶	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.24 Ažurirati na Apache HTTPD version 2.2.24 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz Apache HTTPD >= 2.4 and < 2.4.4 Ažurirati na Apache HTTPD version 2.4.4 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz
54.	Apache HTTPD: XSS in mod_proxy_balancer (CVE-2012-4558) (apache-httpd-cve-	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80	APPLE APPLE-SA-2013-09-12-1⁸³³⁷ CVE CVE-2012-4558⁸³³⁸ DEBIAN DSA-2637⁸³³⁹	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.24 Ažurirati na Apache HTTPD version 2.2.24

⁸³¹⁸ http://httpd.apache.org/security/vulnerabilities_22.html

⁸³¹⁹ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>

⁸³²⁰ <http://www.securityfocus.com/bid/51706>

⁸³²¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0053>

⁸³²² <http://iase.disa.mil/stigs/iavm-cve.html>

⁸³²³ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>

⁸³²⁴ <http://secunia.com/advisories/48551/>

⁸³²⁵ http://httpd.apache.org/security/vulnerabilities_20.html

⁸³²⁶ http://httpd.apache.org/security/vulnerabilities_22.html

⁸³²⁷ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>

⁸³²⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3499>

⁸³²⁹ <http://www.debian.org/security/2013/dsa-2637>

⁸³³⁰ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>

⁸³³¹ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>

⁸³³² <http://rhn.redhat.com/errata/RHSA-2013-1208.html>

⁸³³³ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>

⁸³³⁴ <http://secunia.com/advisories/55032/>

⁸³³⁵ http://httpd.apache.org/security/vulnerabilities_22.html

⁸³³⁶ http://httpd.apache.org/security/vulnerabilities_24.html

⁸³³⁷ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>

⁸³³⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4558>

	2012-4558)	Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy_balancer. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. XSS propust je uticao na manager interfejs mod_proxy_balancer-a.	REDHAT 2013:0815 ⁸³⁴⁰ REDHAT 2013:1207 ⁸³⁴¹ REDHAT 2013:1208 ⁸³⁴² REDHAT 2013:1209 ⁸³⁴³ URL1 ⁸³⁴⁴ URL2 ⁸³⁴⁵	RHSA- RHSA- RHSA- RHSA-		Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz Apache HTTPD >= 2.4 and < 2.4.4 Ažurirati na Apache HTTPD version 2.4.4 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz
55.	Apache HTTPD: mod_dav crash (CVE-2013-1896) (apache-httpd-cve-2013-1896)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_dav_svn. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Slanje MERGE zahteva URI-ju koji obrađuje mod_dav_svn sa izvorom href (poslato kao deo zahteva XML) ciljajući na URI koji nije konfigurisan za DAV prouzrokuje segmentation fault (segfault).	CVE CVE-2013-1896 ⁸³⁴⁶ OVAL OVAL18835 ⁸³⁴⁷ REDHAT 2013:1156 ⁸³⁴⁸ REDHAT 2013:1207 ⁸³⁴⁹ REDHAT 2013:1208 ⁸³⁵⁰ REDHAT 2013:1209 ⁸³⁵¹ SECUNIA 55032 ⁸³⁵² URL1 ⁸³⁵³ URL2 ⁸³⁵⁴	RHSA- RHSA- RHSA- RHSA- RHSA- RHSA-	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.25 Ažurirati na Apache HTTPD version 2.2.25 Apache HTTPD >= 2.4 and < 2.4.6 Ažurirati na Apache HTTPD version 2.4.6 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.6.tar.gz
56.	Apache HTTPD: XSS in mod_negotiation when untrusted uploads are supported (CVE-2012-2687) (apachehttpd-cve-2012-2687)	172.23.202.195:80 172.23.202.196:80 172.23.202.221:80 172.23.202.222:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_negotiation. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Moguće je ubaciti CRLF (Carriage Return and Line Feed) koji omogućava CRLF Injection napade (poznatih i kao HTTP Response Splitting) za sajtove koji koriste mod_negotiation, omogućavajući neproverene upload-ove na lokacije	APPLE APPLE-SA-2013-09-12-1 ⁸³⁵⁵ BID 55131 ⁸³⁵⁶ CVE CVE-2012-2687 ⁸³⁵⁷ IAVM 2012-A-0139 ⁸³⁵⁸ REDHAT 2012:1591 ⁸³⁵⁹ REDHAT 2012:1592 ⁸³⁶⁰ REDHAT 2012:1594 ⁸³⁶¹ REDHAT 2013:0130 ⁸³⁶² SECUNIA 50894 ⁸³⁶³ SECUNIA 51607 ⁸³⁶⁴ URL1 ⁸³⁶⁵	APPLE-SA- RHSA- RHSA- RHSA- RHSA- RHSA- RHSA-	Umeren	Apache HTTPD >= 2.2 and < 2.2.23 Ažurirati na Apache HTTPD version 2.2.23 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz Apache HTTPD >= 2.4 and < 2.4.3 Ažurirati na Apache HTTPD version 2.4.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.3.tar.gz

⁸³³⁹ <http://www.debian.org/security/2013/dsa-2637>
⁸³⁴⁰ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>
⁸³⁴¹ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>
⁸³⁴² <http://rhn.redhat.com/errata/RHSA-2013-1208.html>
⁸³⁴³ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>
⁸³⁴⁴ http://httpd.apache.org/security/vulnerabilities_22.html
⁸³⁴⁵ http://httpd.apache.org/security/vulnerabilities_24.html
⁸³⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1896>
⁸³⁴⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18835>
⁸³⁴⁸ <http://rhn.redhat.com/errata/RHSA-2013-1156.html>
⁸³⁴⁹ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>
⁸³⁵⁰ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>
⁸³⁵¹ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>
⁸³⁵² <http://secunia.com/advisories/55032/>
⁸³⁵³ http://httpd.apache.org/security/vulnerabilities_22.html
⁸³⁵⁴ http://httpd.apache.org/security/vulnerabilities_24.html
⁸³⁵⁵ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>
⁸³⁵⁶ <http://www.securityfocus.com/bid/55131>
⁸³⁵⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2687>
⁸³⁵⁸ <http://iase.disa.mil/stigs/iavm-cve.html>
⁸³⁵⁹ <http://rhn.redhat.com/errata/RHSA-2012-1591.html>
⁸³⁶⁰ <http://rhn.redhat.com/errata/RHSA-2012-1592.html>
⁸³⁶¹ <http://rhn.redhat.com/errata/RHSA-2012-1594.html>
⁸³⁶² <http://rhn.redhat.com/errata/RHSA-2013-0130.html>
⁸³⁶³ <http://secunia.com/advisories/50894/>
⁸³⁶⁴ <http://secunia.com/advisories/51607/>

		na kojima je omogućen MultiViews (višestruko pregledanje). Ovaj problem je poznat i kao CVE-2008-0455.	URL⁸³⁶⁶		

Tabela 128. Linux OS sa IP adresama 172.23.202.122, 172.23.202.232, 172.23.202.200, 172.23.202.230, 172.23.202.135, 172.23.202.231 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara		Broj ranjivosti	
IP adresa: 172.23.202.122		OS: Kubuntu 11.04 x86 desktop, kubun1104dskx86		39	
IP adresa: 172.23.202.232		OS: Kubuntu 11.04 x86 desktop, kubun1104dskx64		39	
IP adresa: 172.23.202.200		OS: Ubuntu 11.04 x64 desktop, ubunt1104dskx64		39	
IP adresa: 172.23.202.230		OS: Ubuntu 11.04 x86 desktop, ubunt1104dskx86		39	
IP adresa: 172.23.202.135		OS: Ubuntu 11.04 x64 server, ubunt1104srvx64		39	
IP adresa: 172.23.202.231		OS: Ubuntu 11.04 x86 server, ubunt1104srvx86		39	
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Anonymous users can obtain the Windows password policy (cifs-nt-0002)	Korišćenjem CIFS NULL sesije, anonimni korisnik može da dobije uvid u polisu šifri. Polisa šifri sadrži osetljive informacije o najmanjoj mogućoj dužini lozinke, zaključavanje šifre, vremensko trajanje zaključanosti šifre itd.	SANS-01 W5⁸³⁶⁷ CVE CVE-2000-1200⁸³⁶⁸ XF nt-lsa-domain-sid(4015)⁸³⁶⁹ SANS-02 W5⁸³⁷⁰ BID 959⁸³⁷¹ SANS-04 W3⁸³⁷² SANS-03 W5⁸³⁷³ BID 87⁸³⁷⁴	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost.
2.	HTTP Basic Authentication Enabled (http-basic-auth-clear-text)	172.23.202.122:8080 172.23.202.232:8080 172.23.202.200:8080 172.23.202.230:8080 172.23.202.135:8080 172.23.202.231:8080 HTTP Basic Authentication šema se ne smatra sigurnom metodom autentifikacije korisnika (ukoliko se ne koristi u kombinaciji sa nekim spoljnim sigurnosnim sistemom, kao TLS/SSL), s obzirom da se korisničko ime i lozinka preko mreže prenose kao običan tekst. Primer: Pokretanje ranjivog HTTP servisa http://172.23.202.122:8080/manager/html 1: Basic realm="Tomcat Manager Application"	URL⁸³⁷⁵	Kritičan	Koristiti Osnovnu Autentifikaciju preko TLS/SSL (HTTPS). Omogućiti HTTPS na Web serveru. TLS/SSL protokol će zaštititi akreditivne osnovne autentifikacije u običnom tekstu. Koristiti Digest Authentication Replace Basic Authentication sa alternativnom Digest Authentication shemom. Po savremenim kriptografskim standardima, Digest Authentication je slaba. Ali za širok spektar namena, ona je korisna zamena za Basic Authentication (osnovnu autentifikaciju).

⁸³⁶⁵ http://httpd.apache.org/security/vulnerabilities_22.html

⁸³⁶⁶ http://httpd.apache.org/security/vulnerabilities_24.html

⁸³⁶⁷ <http://www.sans.org/critical-security-controls/#w5>

⁸³⁶⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2000-1200>

⁸³⁶⁹ <http://xforce.iss.net/xforce/xfdb/4015>

⁸³⁷⁰ <http://www.sans.org/critical-security-controls/#w5>

⁸³⁷¹ <http://www.securityfocus.com/bid/959>

⁸³⁷² <http://www.sans.org/critical-security-controls/#w3>

⁸³⁷³ <http://www.sans.org/critical-security-controls/#w5>

⁸³⁷⁴ <http://www.securityfocus.com/bid/87>

⁸³⁷⁵ <http://tools.ietf.org/html/rfc2617>

					Ona ispravlja neke, ali ne sve, slabosti Basic Authentication (osnovne autentifikacije). Videti RFC 2617 ⁸³⁷⁶ (odjeljak 4 Security Considerations) za više informacija.
3.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.122:139 172.23.202.122:445 172.23.202.232:139 172.23.202.232:445 172.23.202.200:139 172.23.202.200:445 172.23.202.230:139 172.23.202.230:445 172.23.202.135:139 172.23.202.135:445 172.23.202.231:139 172.23.202.231:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB 887429 URL1 ⁸³⁷⁷	Ozbiljan	Metoda za konfiguraciju SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429 ⁸³⁷⁸ . Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing</i> = <i>auto</i> ili da se zahteva SMB potpisivanje: <i>server signing</i> = <i>mandatory</i> .
4.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.122:139 172.23.202.122:445 172.23.202.232:139 172.23.202.232:445 172.23.202.200:139 172.23.202.200:445 172.23.202.230:139 172.23.202.230:445 172.23.202.135:139 172.23.202.135:445 172.23.202.231:139 172.23.202.231:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti.
5.	X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch)	172.23.202.122:993 172.23.202.122:995 172.23.202.232:993 172.23.202.232:995 172.23.202.200:993 172.23.202.200:995 172.23.202.230:993 172.23.202.230:995 172.23.202.135:993 172.23.202.135:995 172.23.202.231:993 172.23.202.231:995 Rubrika u sertifikatu X.509 sa uobičajenim nazivom subjekta (CN) ne poklapa se sa imenom pojedinca koje je navedeno u sertifikatu. Pre izdavanja sertifikata, Certification Authority (CA) mora da proveri identitet pojedinca koji potražuje sertifikat, kako je navedeno		Ozbiljan	Rubrika sa uobičajenim nazivom subjekta (CN) u sertifikatu X.509 treba da bude podešena da sadrži ime pojedinca koji prikazuje sertifikat (npr. ime hosta). To se postiže izradom novog sertifikata, koji najčešće potpisuje Certification Authority (CA), koji je od poverenja kako za klijenta, tako i za server.

⁸³⁷⁶ <http://tools.ietf.org/html/rfc2617#section-4>⁸³⁷⁷ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>⁸³⁷⁸ <http://support.microsoft.com/kb/887429>

		u CA-ovom Certification Practice Statement (CPS). Zbog toga, uobičajene procedure validacije sertifikata zahtevaju da rubrika sertifikata sa CN subjektom odgovara pravom imenu pojedinca koji prikazuje sertifikat. Na primer, u sertifikatu prikazanom na „https://www.example.com/“, naziv subjekta (CN) treba da bude „www.example.com“. U cilju otkrivanja i sprečavanja napada prisluškivanja, validnost sertifikata mora da bude overena, jer bi u suprotnom napadač mogao da otpočne napad preko posrednika i da stekne potpunu kontrolu nad protokom podataka. Od posebne važnosti je validnost naziva subjekta (CN), koji treba da se poklapa sa imenom pojedinca (imenom host-a). Neodgovarajući CN se najčešće javlja usled greške u konfiguraciji, iako on takođe može da ukazuje na to da se sprovodi napad preko posrednika.			
6.	FTP server does not support AUTH command (ftp-generic-0007)	172.23.202.122:21 172.23.202.232:21 172.23.202.200:21 172.23.202.230:21 172.23.202.135:21 172.23.202.231:21 FTP klijenti po defaultu šalju FTP server-u poverljive podatke (korisnički ID i šifra) u vidu čitkog teksta. Ova okolnost dozvoljava zlonamernim korisnicima da presreću poverljive podatke ukoliko prisluškuju vezu. Noviji FTP serveri podržavaju AUTH komandu, koja omogućava dodatne opcije autentifikacije, kao što su TLS, Kerberos, GSSAPI itd. Ona se može koristiti za sprečavanje prisluškivanja na FTP vezama.		Ozbiljan	Ažurirati/preći na FTP server koji podržava AUTH komandu.
7.	Browsable web directory (http-generic-browsable-dir)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80 172.23.202.231:80 Otkriven je direktorijum na web serveru koji može biti pretraživan, što znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice - spajdering (prateći hiperlinkove), ili -kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute force napadom na liste uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skriven“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice.		Ozbiljan	Za Apache: onemogućiti pretraživanje direktorijuma mreže za sve direktorijume i poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i

		Primer: <pre> http://172.23.202.122/icons/small/ 4: <title>Index of /icons/small</title> 5: </head> 6: <body> 7: <h1>Index of /icons/small</h1> 8: ...COJ"></th><th>Name</th>< th><a href="?C=M;O=A...</pre>			nepoznate fajlove i direktorijume. Za Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote: Onemogućiti pretraživanje direktorijuma za sve direktorijume i poddirektorijume. Uključiti Tomcat-ov web.xml file. U odeljku „default“, promeniti parametar „listings“ iz „true“ u „false“. Restartovati server. Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripta i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume.
8.	Form action submits sensitive data in the clear (http-generic-sensitive-form-data-unencrypted)	<pre> 172.23.202.122:8080 172.23.202.232:8080 172.23.202.200:8080 172.23.202.230:8080 172.23.202.135:8080 172.23.202.231:8080</pre> Web forma sadrži rubrike sa podacima koji su možda po prirodi osetljivi. Ovakvi podaci se prenose preko nezaštićene veze, koja bi mogla da omogući zlonamernim napadačima da prisluškujući mrežu pregledaju podatke u vidu običnog teksta. Formatiranje preko http://localhost:8080/examples/jsp/security/protected/_vti_shm/j_security_check prosleđuje sledeće nezaštićene osetljive rubrike: j_password		Ozbiljan	Isključiti HTTPS protokol na serveru. Promeniti „action“ URL na oznaci rubrike da koristi HTTPS protokol („https://...“) umesto samo HTTP protokol („http://...“). Sve osetljive podatke treba slati preko HTTPS umesto preko HTTP.
9.	TLS/SSL Server Supports Weak Cipher Algorithms (ssl-weak-ciphers)	<pre> 172.23.202.122:993 172.23.202.232:993 172.23.202.200:993 172.23.202.230:993 172.23.202.135:993 172.23.202.231:993 172.23.202.122:995 172.23.202.232:995 172.23.202.200:995 172.23.202.230:995 172.23.202.135:995 172.23.202.231:995</pre> negotiated the SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA cipher suite TLS/SSL server podržava šifre koje se zasnivaju na slabim algoritmima.		Ozbiljan	Konfigurisati server tako da onemogući podršku za slabe šifre. Za Apache web servere sa mod_ssl, uključiti fajl Apache konfiguracije i izmeniti liniju SSLCipherSuite tako da u njoj piše: SSLCipherSuite ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM

		To napadaču može omogućiti da pokrene napade preko posrednika i da pregleda ili čačka osetljive podatke. Uopšteno, sledeće šifre se smatraju slabim: Tzv. „null“ (nula) šifre, jer ne šifruju podatke. Eksportne šifre koje koriste dužine tajnih ključeva ograničene na 40 bitova. Na to najčešće ukazuje reč EXP/EXPORT u nazivu šifre. Zastareli algoritmi za šifrovanje čije se dužine tajnih ključeva po današnjim standardima smatraju kratkim, npr. DES ili RC4 sa 56-bitnim ključevima.			
10.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	TCP reset with incorrect sequence number triggered this fault on 172.23.202.122:21 172.23.202.232:21 172.23.202.200:21 172.23.202.230:21 172.23.202.135:21 172.23.202.231:21 Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183⁸³⁷⁹ CERT-VN: 415294⁸³⁸⁰ CVE CVE-2004-0230⁸³⁸¹ MS: MS05-019⁸³⁸² MS: MS06-064⁸³⁸³ NETBSD: NetBSD-SA2004-006⁸³⁸⁴ OVAL: OVAL2689⁸³⁸⁵ OVAL: OVAL270⁸³⁸⁶ OVAL OVAL3508⁸³⁸⁷ OVAL OVAL4791⁸³⁸⁸ OVAL OVAL5711⁸³⁸⁹ SECUNIA: 11440⁸³⁹⁰ SECUNIA 11458⁸³⁹¹ SECUNIA: 22341⁸³⁹² SGI 20040403-01-A⁸³⁹³ XF tcp-rst-dos(15886)⁸³⁹⁴ URL1⁸³⁹⁵ URL2⁸³⁹⁶	Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC 2385 ⁸³⁹⁷ . Ono je napravljeno da smanji opasnost od određenih napada na BGP, kao što su TCP reseti.
11.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podesi na jedinstvenu vrednost i da se koristi u rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da fingerprint-uje operativni sistem.	BID 4314⁸³⁹⁸ CVE CVE-2002-0510⁸³⁹⁹ XF linux-udp-fingerprint(8588)⁸⁴⁰⁰	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili pak ranjivost koju treba popravljati, tako da ne postoje rešenja koja se mogu kupiti. Jedino se može postaviti fajervol ili neka druga sprava za filtriranje između napadnutog i neprijateljskog napada koji je u mogućnosti da

⁸³⁷⁹ <http://www.securityfocus.com/bid/10183>⁸³⁸⁰ <http://www.kb.cert.org/vuls/id/415294>⁸³⁸¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁸³⁸² <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁸³⁸³ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁸³⁸⁴ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁸³⁸⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>⁸³⁸⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>⁸³⁸⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>⁸³⁸⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>⁸³⁸⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>⁸³⁹⁰ <http://secunia.com/advisories/11440/>⁸³⁹¹ <http://secunia.com/advisories/11458/>⁸³⁹² <http://secunia.com/advisories/22341/>⁸³⁹³ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>⁸³⁹⁴ <http://xforce.iss.net/xforce/xfdb/15886>⁸³⁹⁵ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁸³⁹⁶ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>⁸³⁹⁷ <http://www.ietf.org/rfc/rfc2385.txt>⁸³⁹⁸ <http://www.securityfocus.com/bid/4314>⁸³⁹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>⁸⁴⁰⁰ <http://xforce.iss.net/xforce/xfdb/8588>

					randomizuje IP ID-jeve.
12.	Apache HTTPD: apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpdcve-2011-0419)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80 172.23.202.231:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_autoindex. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_fnmatch() u sklopu APR biblioteke. Ako je omogućen mod_autoindex, a indeksi direktorijuma mod_autoindex su sadržavali fajlove sa dovoljno dugim nazivima, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do preterane upotrebe CPU-a. Ovo bi moglo da bude iskorišćeno u napadu odbijanja servisa. Zahvaljujući Maksymilian Arciemowicz prijavljen je ovaj propust.	CVE CVE-2011-0419 ⁸⁴⁰¹ DEBIAN DSA-2237 ⁸⁴⁰² IAVM 2012-B-0056 ⁸⁴⁰³ OVAL OVAL14638 ⁸⁴⁰⁴ OVAL OVAL14804 ⁸⁴⁰⁵ REDHAT RHSA-2011:0896 ⁸⁴⁰⁶ REDHAT RHSA-2011:0897 ⁸⁴⁰⁷ REDHAT RHSA-2011:0507 ⁸⁴⁰⁸ SECUNIA 44490 ⁸⁴⁰⁹ SECUNIA 44564 ⁸⁴¹⁰ SECUNIA 44574 ⁸⁴¹¹ URL1 ⁸⁴¹²	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.19 Ažurirati na Apache HTTPD version 2.2.19 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.19.tar.gz
13.	Apache HTTPD: ETag Inode Information Leakage (CVE-2003-1418) (apache-httpdcve-2003-1418)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80 172.23.202.231:80 U određenim konfiguracijama, Apache HTTP server dozvoljava udaljenim napadačima da dobiju poverljive informacije preko (1) Etag heder-a, koji otkriva broj inoda ili (2) razdvajачe višedelnih MIME-a, koja ukazuje na ID child procesa (PID). Određene verzije Apache-a koriste zahtevani broj čvorova fajla da bi konstruisali 'Etag' heder za odgovor. Iako sama po sebi nije ranjivost, ova informacija olakšava sprovođenje određenih NFS napada. „Running vulnerable HTTP service: Apache 2.2.17. http://172.23.202.206/1:c2979-b1-4a76e5063f807 “	BID 6939 ⁸⁴¹³ BID 6943 ⁸⁴¹⁴ CVE CVE-2003-1418 ⁸⁴¹⁵ XF apache-mime-information-disclosure(11438) ⁸⁴¹⁶	Ozbiljan	Onemogućiti Etag mehanizam tipa "inod-based" konfiguraciji Apache-a. Takođe, inod informacije je moguće ukloniti iz Etag heder-a tako što će se dodati direktiva u Apache konfiguraciju: <i>FileETag Mtime Size</i>
14.	Apache Tomcat v4.x Example Scripts Information Leakage	172.23.202.122:8080 172.23.202.232:8080 172.23.202.200:8080		Kritičan	U potpunosti obrisati ove skripte. Primeri skripta nikad ne treba da budu

⁸⁴⁰¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419>⁸⁴⁰² <http://www.debian.org/security/2011/dsa-2237>⁸⁴⁰³ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁴⁰⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14638>⁸⁴⁰⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14804>⁸⁴⁰⁶ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁸⁴⁰⁷ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>⁸⁴⁰⁸ <http://rhn.redhat.com/errata/RHSA-2011-0507.html>⁸⁴⁰⁹ <http://secunia.com/advisories/44490/>⁸⁴¹⁰ <http://secunia.com/advisories/44564/>⁸⁴¹¹ <http://secunia.com/advisories/44574/>⁸⁴¹² http://httpd.apache.org/security/vulnerabilities_22.html⁸⁴¹³ <http://www.securityfocus.com/bid/6939>⁸⁴¹⁴ <http://www.securityfocus.com/bid/6943>⁸⁴¹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-1418>⁸⁴¹⁶ <http://xforce.iss.net/xforce/xfdb/11438>

	(http-tomcat-0005)	172.23.202.230:8080 172.23.202.135:8080 172.23.202.231:8080 Sledeće skripte su navedene kao primeri koji dolaze sa Apache Tomcat-om v4.x, a koje napadači mogu da iskoriste da dobiju informacije o sistemu. Poznato je da su ove skripte ranjive na napad tipa "cross site scripting" (XSS): /examples/jsp/num/numguess.jsp /examples/jsp/dates/date.jsp /examples/jsp/snp/snoop.jsp /examples/jsp/error/error.html /examples/jsp/sessions/carts.html /examples/jsp/checkbox/check.html /examples/jsp/colors/colors.html /examples/jsp/cal/login.html /examples/jsp/include/include.jsp /examples/jsp/forward/forward.jsp /examples/jsp/plugin/plugin.jsp /examples/jsp/jstoserv/jstoservlet.jsp p /examples/jsp/simpletag/foo.jsp /examples/jsp/mail/sendmail.jsp /examples/servlet/HelloWorldExample /examples/servlet/RequestInfoExample /examples/servlet/RequestHeaderExample /examples/servlet/RequestParamExample /examples/servlet/CookieExample /examples/servlet/IndiServlet /examples/servlet/SessionExample /tomcat-docs/appdev/sample/web/hello.jsp „Running vulnerable HTTP service: Apache Tomcat. http://172.23.202.122:8080/examples/jsp/sessions/carts.html 24: 25: 26: <form type=POST action=carts.jsp> 27:
 28: Please enter item to add or remove.“			instalirani na serverima koji su u produkciji.
15.	Self-signed TLS/SSL certificate (ssl-self-signed-certificate)	172.23.202.122:993 172.23.202.122:995 172.23.202.232:993 172.23.202.232:995 172.23.202.200:993 172.23.202.200:995 172.23.202.230:993 172.23.202.230:995 172.23.202.135:993 172.23.202.135:995 172.23.202.231:993 172.23.202.231:995 TLS/SSL-a sertifikat servera je samopotpisan. Samopotpisani sertifikati po defaultu nisu od poverenja, naročito zato što napadi na TLS/SSL preko posrednika obično		Ozbiljan	Nabaviti novi TLS/SSL serverov sertifikat koji NIJE samopotpisan i instalirati ga na server. Precizna uputstva za dobijanje novog sertifikata zavise od zahteva organizacije. Uopšteno, treba napraviti zahtev za sertifikat i taj zahtev sačuvati kao fajl. Ovaj fajl se zatim šalje Certificate Authority-ju (CA) na obradu. Organizacija možda poseduje sopstveni interni Certificate Authority. U suprotnom, potrebno je platiti sertifikat iz spoljnog poverljivog Certificate

		koriste samopotpisane sertifikate da prisluškuju TLS/SSL veze.			Authority-ja, kao što su Thawte, Verisign.
16.	Autocomplete enabled for sensitive HTML form fields (spider-sensitive-form-data-autocomplete-enabled)	172.23.202.122:8080 172.23.202.232:8080 172.23.202.200:8080 172.23.202.230:8080 172.23.202.135:8080 172.23.202.231:8080 Web forma sadrži lozinke i druge rubrike sa osetljivim tekstom za koje je otvorena mogućnost auto-complete od strane web pretraživača. Funkcija auto-complete skladišti forme popunjenih rubrika i lozinki lokalno, na web pretraživaču, tako da se ove rubrike automatski popunjavaju kada korisnik ponovo poseti sajt. Osetljivi podaci i lozinke mogu biti ukradeni ako je korisnikov sistem kompromitovan. Međutim, treba imati u vidu da forma auto-complete nije standardna i da je to karakteristika web pretraživača koju svaki web pretraživač tretira na različit način. Na primer Opera zanemaruje ovu opciju i zahteva od korisnika da unese poverljive podatke svaki put kada posećuje određeni web sajt.		Umeren	Za svaku osetljivu rubriku u HTML, stavku „autocomplete“ potrebno je podesiti na „off“. Na primer: <pre><input type="password" autocomplete="off" name="pw"></pre> Ako ima previše rubrika, možda je brže podesiti stavku „autocomplete“ na „off“ u spoljnom tagu <form>. Na primer: <pre><form action="/login.jsp" autocomplete="off" name="pw"> <input type="password" name="pw"> </form></pre>
17.	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server. Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko poziva udaljenih procedura (RPC). Ovi servisi su i u prošlosti bili skloni ranjivostima.. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinjenije napade. Primer : Found user(s): nobody root vanja Found server name: UBUNT1104DSKX64 Found local group(s): Found policy for domain(s): UBUNT1104DSKX64 Builtin	BID: 494⁸⁴¹⁷ CVE: CVE-1999-0519⁸⁴¹⁸ MSKB: 143474⁸⁴¹⁹ URL⁸⁴²⁰	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost.
18.	Apache default installation/welcome page installed (http-apache-default-install-page)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80 172.23.202.231:80 Apache difoltna instalacija ili		Umeren	Ako se od servera zahteva da obezbedi neophodnu funkcionalnost, onda difoltnu stranicu treba zameniti odgovarajućim sadržajem. U suprotnom, ovakav server treba ukloniti sa mreže, prateći

⁸⁴¹⁷ <http://www.securityfocus.com/bid/494>⁸⁴¹⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>⁸⁴¹⁹ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>⁸⁴²⁰ http://www.hsc.fr/ressources/presentations/null_sessions/

		„Welcome“ stranica je instalirana na serveru. To obično ukazuje na novoinstalirani server. U mnogim slučajevima, Apache se instalira zajedno sa drugim aplikacijama i korisnik možda nije svestan da je web server pokrenut. Ovakvi serveri se retko patch-uju i još rede nadgledaju, što zlonamernim napadačima postaje pogodna meta koja najverovatnije neće pokrenuti nikakvo upozorenje. Primer : Running vulnerable HTTP service: Apache 2.2.17. http://172.23.202.122/ 1: <code><html><body><h1>It works!</h1></code>			bezbednosni princip minimalne složenosti (više složenosti = manja bezbednost). Ako server nije potreban, treba ga ukloniti iz svih startup fajlova (npr. /etc/rc*) ili skripti, a zatim prekinuti servis. Proveriti da li se on ponovo pokreće kada se mašina reboot-uje. Apache se uglavnom instalira kao /usr/sbin/httpd na UNIX mašinama ili kao C:\Program Files\Apache Group na Windows mašinama. Razmotriti uklanjanje binara i svih srodnih biblioteka iz sistema.
19.	Apache Tomcat default installation/welcome page installed (http://tomcat-default-install-page)	172.23.202.122:8080 172.23.202.232:8080 172.23.202.200:8080 172.23.202.230:8080 172.23.202.135:8080 172.23.202.231:8080 Tomcat difoltna instalacija ili „Welcome“ stranica je instalirana na serveru. To obično ukazuje na novoinstalirani server. U mnogim slučajevima, Tomcat se instalira zajedno sa drugim aplikacijama i korisnik možda nije svestan da je web server pokrenut. Ovakvi serveri se retko patch-uju i još rede nadgledaju, što zlonamernim napadačima postaje pogodna meta koja najverovatnije neće pokrenuti nikakvo upozorenje. Pokretanje ranjivog HTTP servisa: Apache Tomcat. http://172.23.202.122:8080/ 8: 9: <code><body></code> 10: <code><h1>It works !</h1></code> 11: 12: ... means you've setup Tomcat successfully. Congratulations!</p>		Ozbiljan	Ako se od servera zahteva da obezbedi neophodnu funkcionalnost, onda difoltnu stranicu treba zameniti odgovarajućim sadržajem. U suprotnom, ovakav server treba ukloniti sa mreže, prateći bezbednosni princip minimalne složenosti (više složenosti = manja bezbednost).
20.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	CVE CVE-1999-0524⁸⁴²¹ OSVDB 95⁸⁴²² XF icmp-netmask(306)⁸⁴²³ XF icmp-timestamp(322)⁸⁴²⁴	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.

⁸⁴²¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁸⁴²² <http://www.osvdb.org/95>⁸⁴²³ <http://xforce.iss.net/xforce/xfdb/306>⁸⁴²⁴ <http://xforce.iss.net/xforce/xfdb/322>

21.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1⁸⁴²⁵ URL2⁸⁴²⁶ URL3⁸⁴²⁷	Umeren	Onemogućavanje TCP timestamp odgovora na Linux OS. Podesiti net.ipv4.tcp_timestamps vrednost na sledećem ključu na 0 pokretanjem sledeće komande: sysctl -w net.ipv4.tcp_timestamps=0 Dodatno, sledeću vrednost u difoltnom sysctl konfiguracionom fajlu, generally sysctl.conf: net.ipv4.tcp_timestamps=0
22.	Database Open Access (database-open-access)	172.23.202.122:3306 172.23.202.232:3306 172.23.202.200:3306 172.23.202.230:3306 172.23.202.135:3306 172.23.202.231:3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7.	URL1⁸⁴²⁸	Umeren	Konfigurisati server baze podataka tako da dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.
23.	Samba RPC unauthenticated remote code execution (CVE-2012-1182) (cifs-samba-cve-2012-1182)	172.23.202.122:139 172.23.202.122:445 172.23.202.232:139 172.23.202.232:445 172.23.202.200:139 172.23.202.200:445 172.23.202.230:139 172.23.202.230:445 172.23.202.135:139 172.23.202.135:445 172.23.202.231:139 172.23.202.231:445 Određene verzije Samba-e sadrže sigurnosni propust u interfejsu poziva udaljenih procedura (RPC). Posledica ovog propusta je da udaljeni napadač može pokrenuti daljinsko izvršenje koda u sklopu smbd procesa, preko crafted RPC paketa, koji bi doveo do preopetrecenja bafera. Ova ranjivost ne zahteva autentifikovanu vezu da bi pokrenula nove eksploite, a s obzirom	APPLE APPLE-SA-2012-05-09-1⁸⁴²⁹ CVE CVE-2012-1182⁸⁴³⁰ IAVM 2012-A-0085⁸⁴³¹ SECUNIA 48999⁸⁴³² URL1⁸⁴³³	Kritičan	Uraditi download a zatim instalirati: http://www.samba.org Zakrpljene verzije Samba-e obuhvataju v3.6.4, v3.5.14, i v3.4.16, a puštene su u opticaj 10. aprila 2012. Većina Linux distributera prodaje starije verzije Samba-e, ali poseduje backportovane popravke za bezbednosne propuste (kako od prodavca - Samba-e - tako i od samih distributera). Treba ažurirati dobijenu verziju od distributera preko system package manager-a.

⁸⁴²⁵ http://www.forensicswiki.org/wiki/TCP_timestamps⁸⁴²⁶ <http://www.ietf.org/rfc/rfc1323.txt>⁸⁴²⁷ <http://uptime.netcraft.com/>⁸⁴²⁸ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf⁸⁴²⁹ <http://lists.apple.com/archives/security-announce/2012/May/msg00001.html>⁸⁴³⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1182>⁸⁴³¹ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁴³² <http://secunia.com/advisories/48999/>⁸⁴³³ <http://www.mandriva.com/en/support/security/advisories/advisory/MDVSA-2012:055/?name=MDVSA-2012:055>

		da Samba radi kao root, ovo je jedna od najopasnijih ranjivosti.			
24.	Obsolete Version of Ubuntu (ubuntu-obsolete-version)	Izdannju je istekao rok. Moguće je da postoje bezbednosne ranjivosti. Proveriti na https://wiki.ubuntu.com/Releases radi dobijanja podržanih verzija.		Kritičan	Ažurirati na podržanu verziju Ubuntu Linux-a.
25.	Apache HTTPD: Range header remote DoS (CVE-2011-3192) (apache-httpd-cve-2011-3192)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80 172.23.202.231:80 Propust je otkriven u načinu na koji Apache HTTP Server obrađuje Range HTTP hedere. Zlonamerni napadač bi mogao da iskoristi ovaj propust i dovede do toga da http koristi veliku količinu memorije i CPU vremena preko HTTP zahteva sa posebno kreiranim Range hederom. Ovo bi moglo dovesti do napada odbijanja servisa. Advisory: CVE-2011-3192.txt	APPLE APPLE-SA-2011-10-12-3 ⁸⁴³⁴ BID 49303 ⁸⁴³⁵ CERT-VN 405811 ⁸⁴³⁶ CVE CVE-2011-3192 ⁸⁴³⁷ IAVM 2012-B-0056 ⁸⁴³⁸ OSVDB 74721 ⁸⁴³⁹ OVAL OVAL14762 ⁸⁴⁴⁰ OVAL OVAL14824 ⁸⁴⁴¹ OVAL OVAL18827 ⁸⁴⁴² REDHAT RHSA-2011:1245 ⁸⁴⁴³ REDHAT RHSA-2011:1294 ⁸⁴⁴⁴ REDHAT RHSA-2011:1300 ⁸⁴⁴⁵ REDHAT RHSA-2011:1329 ⁸⁴⁴⁶ REDHAT RHSA-2011:1330 ⁸⁴⁴⁷ REDHAT RHSA-2011:1369 ⁸⁴⁴⁸ SECUNIA 45606 ⁸⁴⁴⁹ SECUNIA 45937 ⁸⁴⁵⁰ SECUNIA 46000 ⁸⁴⁵¹ SECUNIA 46125 ⁸⁴⁵² SECUNIA 46126 ⁸⁴⁵³ XF 69396 ⁸⁴⁵⁴ URL1 ⁸⁴⁵⁵ URL2 ⁸⁴⁵⁶	Kritičan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.20 Ažurirati na Apache HTTPD version 2.2.20 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.20.tar.gz
26.	Apache HTTPD: insecure LD_LIBRARY_PATH handling (CVE-2012-)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80	APPLE APPLE-SA-2013-09-12-1 ⁸⁴⁵⁷ CVE CVE-2012-0883 ⁸⁴⁵⁸ SECUNIA 48849 ⁸⁴⁵⁹ URL1 ⁸⁴⁶⁰	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.23 Ažurirati na Apache HTTPD version 2.2.23 Uraditi download a zatim

⁸⁴³⁴ <http://lists.apple.com/archives/Security-announce/2011/Oct/msg00003.html>⁸⁴³⁵ <http://www.securityfocus.com/bid/49303>⁸⁴³⁶ <http://www.kb.cert.org/vuls/id/405811>⁸⁴³⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3192>⁸⁴³⁸ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁴³⁹ <http://www.osvdb.org/74721>⁸⁴⁴⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14762>⁸⁴⁴¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14824>⁸⁴⁴² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18827>⁸⁴⁴³ <http://rhn.redhat.com/errata/RHSA-2011-1245.html>⁸⁴⁴⁴ <http://rhn.redhat.com/errata/RHSA-2011-1294.html>⁸⁴⁴⁵ <http://rhn.redhat.com/errata/RHSA-2011-1300.html>⁸⁴⁴⁶ <http://rhn.redhat.com/errata/RHSA-2011-1329.html>⁸⁴⁴⁷ <http://rhn.redhat.com/errata/RHSA-2011-1330.html>⁸⁴⁴⁸ <http://rhn.redhat.com/errata/RHSA-2011-1369.html>⁸⁴⁴⁹ <http://secunia.com/advisories/45606/>⁸⁴⁵⁰ <http://secunia.com/advisories/45937/>⁸⁴⁵¹ <http://secunia.com/advisories/46000/>⁸⁴⁵² <http://secunia.com/advisories/46125/>⁸⁴⁵³ <http://secunia.com/advisories/46126/>⁸⁴⁵⁴ <http://xforce.iss.net/xforce/xfdb/69396>⁸⁴⁵⁵ http://httpd.apache.org/security/vulnerabilities_22.html⁸⁴⁵⁶ http://httpd.apache.org/security/vulnerabilities_20.html⁸⁴⁵⁷ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁸⁴⁵⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0883>⁸⁴⁵⁹ <http://secunia.com/advisories/48849/>⁸⁴⁶⁰ http://httpd.apache.org/security/vulnerabilities_22.html

	0883) (apache-httpd-cve-2012-0883)	172.23.202.231:80 Otkrivena je nebezbedna obrada rute LD_LIBRARY_PATH koja bi mogla da dovede do toga da direktorijum koji trenutno radi traži DSO-ove. Ovo bi lokalnom korisniku omogućilo da izvrši kôd kao root ako je administrator pokrenuo apachectl sa nepoverljivog direktorijuma.	URL ⁸⁴⁶¹		instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz Apache HTTPD >= 2.4 and < 2.4.2 Ažurirati na Apache HTTPD version 2.4.2 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.2.tar.gz
27.	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368) (apache-httpd-cve-2011-3368)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80 172.23.202.231:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja prisustva mod_proxy modula. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy. Zlonamerni napadač bi mogao da iskoristi ovaj propust na takav način da primora proxy proces da se poveže sa proizvoljnim serverom i potencijalno objavi osetljive informacije sa internih web servera koje inače napadaču nisu direktno dostupne. Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/	APPLE APPLE-SA-2012-09-19-2 ⁸⁴⁶² BID 49957 ⁸⁴⁶³ CVE CVE-2011-3368 ⁸⁴⁶⁴ IAVM 2012-A-0017 ⁸⁴⁶⁵ IAVM 2012-A-0152 ⁸⁴⁶⁶ IAVM 2012-B-0056 ⁸⁴⁶⁷ OSVDB 76079 ⁸⁴⁶⁸ REDHAT RHSA-2011:1391 ⁸⁴⁶⁹ REDHAT RHSA-2011:1392 ⁸⁴⁷⁰ SECUNIA 46288 ⁸⁴⁷¹ SECUNIA 46414 ⁸⁴⁷² SECUNIA 48551 ⁸⁴⁷³ XF 70336 ⁸⁴⁷⁴ URL ⁸⁴⁷⁵ URL ⁸⁴⁷⁶ URL ⁸⁴⁷⁷	Ozbiljan	Apache HTTPD >= 1.3 and < 2 Primeniti zakrpu za CVE-2011-3368 to 1.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
28.	Apache HTTPD: scoreboard parent DoS (CVE-2012-0031) (apache-httpd-cve-2012-0031)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80 172.23.202.231:80	APPLE APPLE-SA-2012-09-19-2 ⁸⁴⁷⁸ BID 51407 ⁸⁴⁷⁹ CVE CVE-2012-0031 ⁸⁴⁸⁰ IAVM 2012-A-0017 ⁸⁴⁸¹ REDHAT RHSA-	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati:

⁸⁴⁶¹ http://httpd.apache.org/security/vulnerabilities_24.html⁸⁴⁶² <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁸⁴⁶³ <http://www.securityfocus.com/bid/49957>⁸⁴⁶⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3368>⁸⁴⁶⁵ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁴⁶⁶ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁴⁶⁷ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁴⁶⁸ <http://www.osvdb.org/76079>⁸⁴⁶⁹ <http://rhn.redhat.com/errata/RHSA-2011-1391.html>⁸⁴⁷⁰ <http://rhn.redhat.com/errata/RHSA-2011-1392.html>⁸⁴⁷¹ <http://secunia.com/advisories/46288/>⁸⁴⁷² <http://secunia.com/advisories/46414/>⁸⁴⁷³ <http://secunia.com/advisories/48551/>⁸⁴⁷⁴ <http://xforce.iss.net/xforce/xfdb/70336>⁸⁴⁷⁵ http://httpd.apache.org/security/vulnerabilities_13.html⁸⁴⁷⁶ http://httpd.apache.org/security/vulnerabilities_20.html⁸⁴⁷⁷ http://httpd.apache.org/security/vulnerabilities_22.html⁸⁴⁷⁸ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁸⁴⁷⁹ <http://www.securityfocus.com/bid/51407>⁸⁴⁸⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0031>⁸⁴⁸¹ <http://iase.disa.mil/stigs/iavm-cve.html>

		Propust je otkriven u obradi scoreboard-a. Neprivilegovani child proces bi mogao da dovede do toga da parent proces krahira prilikom gašenja.	2012:0128 ⁸⁴⁸² SECUNIA 47410 ⁸⁴⁸³ SECUNIA 48551 ⁸⁴⁸⁴ URL1 ⁸⁴⁸⁵ URL2 ⁸⁴⁸⁶		http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Azurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
29.	Apache HTTPD: mod_proxy_ajp remote DoS (CVE-2012-4557) (apache-httpd-cve-2012-4557)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80 172.23.202.231:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ajp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Mod_proxy_ajp će vratiti pogrešan kôd statusa ako naide na grešku, prouzrokujući da backend server bude stavljen u status greške dok ne istekne vreme za ponovni pokušaj. Udaljeni napadač bi mogao da pošalje zlonameran zahtev da bi pokrenuo ovaj problem, što bi dovelo do odbijanja servisa.	CVE CVE-2012-4557 ⁸⁴⁸⁷ DEBIAN DSA-2579 ⁸⁴⁸⁸ URL1 ⁸⁴⁸⁹	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
30.	Apache HTTPD: mod_proxy_ajp remote DoS (CVE-2011-3348) (apache-httpd-cve-2011-3348)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80 172.23.202.231:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ajp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven kada se mod_proxy_ajp koristi zajedno sa mod_proxy_balancer. Sa specifičnom konfiguracijom, udaljeni napadač može da pošalje zlonameran HTTP zahtev, prouzrokujući da backend server bude stavljen u status greške	APPLE APPLE-SA-2012-02-01-1 ⁸⁴⁹⁰ BID 49616 ⁸⁴⁹¹ CVE CVE-2011-3348 ⁸⁴⁹² IAVM 2012-B-0056 ⁸⁴⁹³ OVAL OVAL14941 ⁸⁴⁹⁴ OVAL OVAL18154 ⁸⁴⁹⁵ REDHAT RHSA-2011:1391 ⁸⁴⁹⁶ SECUNIA 46013 ⁸⁴⁹⁷ XF 69804 ⁸⁴⁹⁸ URL1 ⁸⁴⁹⁹	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.21 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.21.tar.gz

⁸⁴⁸² <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁸⁴⁸³ <http://secunia.com/advisories/47410/>⁸⁴⁸⁴ <http://secunia.com/advisories/48551/>⁸⁴⁸⁵ http://httpd.apache.org/security/vulnerabilities_20.html⁸⁴⁸⁶ http://httpd.apache.org/security/vulnerabilities_22.html⁸⁴⁸⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4557>⁸⁴⁸⁸ <http://www.debian.org/security/2012/dsa-2579>⁸⁴⁸⁹ http://httpd.apache.org/security/vulnerabilities_22.html⁸⁴⁹⁰ <http://lists.apple.com/archives/security-announce/2012/Feb/msg00000.html>⁸⁴⁹¹ <http://www.securityfocus.com/bid/49616>⁸⁴⁹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3348>⁸⁴⁹³ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁴⁹⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14941>⁸⁴⁹⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18154>⁸⁴⁹⁶ <http://rhn.redhat.com/errata/RHSA-2011-1391.html>⁸⁴⁹⁷ <http://secunia.com/advisories/46013/>⁸⁴⁹⁸ <http://xforce.iss.net/xforce/xfdb/69804>⁸⁴⁹⁹ http://httpd.apache.org/security/vulnerabilities_22.html

		dok ne istekne vreme za ponovni pokušaj. To bi dovelo do odbijanja servisa.			
31.	Apache HTTPD: mod_rewrite log escape filtering (CVE-2013-1862) (apache-httpd-cve-2013-1862)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80 172.23.202.231:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_rewrite. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Modul mod_rewrite ne filtrira završne izlazne sekvence iz logova, što zlonamenrom napadaču olakšava da ubace takve sekvence u završne emulatore koji sadrže ranjivosti koje se odnose na izlazne sekvence.	CVE CVE-2013-1862 ⁸⁵⁰⁰ OVAL OVAL18790 ⁸⁵⁰¹ REDHAT RHSA-2013:0815 ⁸⁵⁰² REDHAT RHSA-2013:1207 ⁸⁵⁰³ REDHAT RHSA-2013:1208 ⁸⁵⁰⁴ REDHAT RHSA-2013:1209 ⁸⁵⁰⁵ SECUNIA 55032 ⁸⁵⁰⁶ URL1 ⁸⁵⁰⁷ URL2 ⁸⁵⁰⁸	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.25 Ažurirati na Apache HTTPD version 2.2.25 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.25.tar.gz
32.	Apache HTTPD: mod_setenvif .htaccess privilege escalation (CVE-2011-3607) (apache-httpd-cve-2011-3607)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80 172.23.202.231:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_setenvif. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust preopterećenja je otkriven kada je omogućen modul mod_setenvif, što lokalnim korisnicima omogućava da dobiju privilegije preko fajla .htaccess.	APPLE APPLE-SA-2012-09-19-2 ⁸⁵⁰⁹ BID 50494 ⁸⁵¹⁰ CVE CVE-2011-3607 ⁸⁵¹¹ IAVM 2012-A-0017 ⁸⁵¹² IAVM 2012-A-0152 ⁸⁵¹³ OSVDB 76744 REDHAT RHSA-2012:0128 ⁸⁵¹⁴ SECUNIA 45793 ⁸⁵¹⁵ SECUNIA 48551 ⁸⁵¹⁶ XF 71093 ⁸⁵¹⁷ URL1 ⁸⁵¹⁸ URL2 ⁸⁵¹⁹	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
33.	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-4317) (apache-httpd-cve-2011-4317)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80 172.23.202.231:80 Skenirani servis je osjetljiv na ovu	APPLE APPLE-SA-2012-09-19-2 ⁸⁵²⁰ CVE CVE-2011-4317 ⁸⁵²¹ IAVM 2012-A-0017 ⁸⁵²² IAVM 2012-A-0152 ⁸⁵²³ REDHAT RHSA-2012:0128 ⁸⁵²⁴	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.22 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz

⁸⁵⁰⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1862>
⁸⁵⁰¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18790>
⁸⁵⁰² <http://rhn.redhat.com/errata/RHSA-2013-0815.html>
⁸⁵⁰³ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>
⁸⁵⁰⁴ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>
⁸⁵⁰⁵ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>
⁸⁵⁰⁶ <http://secunia.com/advisories/55032/>
⁸⁵⁰⁷ http://httpd.apache.org/security/vulnerabilities_20.html
⁸⁵⁰⁸ http://httpd.apache.org/security/vulnerabilities_22.html
⁸⁵⁰⁹ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>
⁸⁵¹⁰ <http://www.securityfocus.com/bid/50494>
⁸⁵¹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3607>
⁸⁵¹² <http://iase.disa.mil/stigs/iavm-cve.html>
⁸⁵¹³ <http://iase.disa.mil/stigs/iavm-cve.html>
⁸⁵¹⁴ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>
⁸⁵¹⁵ <http://secunia.com/advisories/45793/>
⁸⁵¹⁶ <http://secunia.com/advisories/48551/>
⁸⁵¹⁷ <http://xforce.iss.net/xforce/xfdb/71093>
⁸⁵¹⁸ http://httpd.apache.org/security/vulnerabilities_20.html
⁸⁵¹⁹ http://httpd.apache.org/security/vulnerabilities_22.html
⁸⁵²⁰ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>
⁸⁵²¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4317>
⁸⁵²² <http://iase.disa.mil/stigs/iavm-cve.html>
⁸⁵²³ <http://iase.disa.mil/stigs/iavm-cve.html>
⁸⁵²⁴ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>

		ranjivost samo ako je pokrenut modul mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy U određenim konfiguracijama koje koriste RewriteRule sa proxy flag-om ili ProxyPassMatch, udaljeni napadač bi mogao da primora reverzni proksi da se poveže sa proizvoljnim serverom i potencijalno objavi osetljive informacije sa internih web servera koje inače napadaču nisu direktno dostupne.	SECUNIA 48551 ⁸⁵²⁵ URL1 ⁸⁵²⁶		
34.	Apache HTTPD: error responses can expose cookies (CVE-2012-0053) (apache-httpd-cve-2012-0053)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80 172.23.202.231:80 Propust je otkriven u difoltnom pogrešnom odgovoru za statusni kôd 400. Zlonamerni napadač bi mogao da iskoristi ovaj propust da objavi "httpOnly" kolačiće ako nije određen dokument custom ErrorDocument.	APPLE APPLE-SA-2012-09-19-2 ⁸⁵²⁷ BID 51706 ⁸⁵²⁸ CVE CVE-2012-0053 ⁸⁵²⁹ IAVM 2012-A-0017 ⁸⁵³⁰ REDHAT RHSA-2012-0128 ⁸⁵³¹ SECUNIA 48551 ⁸⁵³² URL1 ⁸⁵³³ URL2 ⁸⁵³⁴	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
35.	Apache HTTPD: XSS due to unescaped hostnames (CVE-2012-3499) (apache-httpd-cve-2012-3499)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80 172.23.202.231:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut jedan od sledećih modula: mod_imagemap, mod_info, mod_ldap, mod_proxy_ftp, mod_status. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Različiti XSS propusti usled nenapuštenih host imena i URI-ja HTML output-a u mod_info, mod_status, mod_imagemap, mod_ldap i mod_proxy_ftp.	APPLE APPLE-SA-2013-09-12-1 ⁸⁵³⁵ CVE CVE-2012-3499 ⁸⁵³⁶ DEBIAN DSA-2637 ⁸⁵³⁷ REDHAT RHSA-2013-0815 ⁸⁵³⁸ REDHAT RHSA-2013-1207 ⁸⁵³⁹ REDHAT RHSA-2013-1208 ⁸⁵⁴⁰ REDHAT RHSA-2013-1209 ⁸⁵⁴¹ SECUNIA 55032 ⁸⁵⁴² URL1 ⁸⁵⁴³ URL2 ⁸⁵⁴⁴	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.24 Ažurirati na Apache HTTPD version 2.2.24 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz Apache HTTPD >= 2.4 and < 2.4.4 Ažurirati na Apache HTTPD version 2.4.4 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz

⁸⁵²⁵ <http://secunia.com/advisories/48551/>⁸⁵²⁶ http://httpd.apache.org/security/vulnerabilities_22.html⁸⁵²⁷ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁸⁵²⁸ <http://www.securityfocus.com/bid/51706>⁸⁵²⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0053>⁸⁵³⁰ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁵³¹ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁸⁵³² <http://secunia.com/advisories/48551/>⁸⁵³³ http://httpd.apache.org/security/vulnerabilities_20.html⁸⁵³⁴ http://httpd.apache.org/security/vulnerabilities_22.html⁸⁵³⁵ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁸⁵³⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3499>⁸⁵³⁷ <http://www.debian.org/security/2013/dsa-2637>⁸⁵³⁸ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁸⁵³⁹ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁸⁵⁴⁰ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁸⁵⁴¹ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁸⁵⁴² <http://secunia.com/advisories/55032/>⁸⁵⁴³ http://httpd.apache.org/security/vulnerabilities_22.html⁸⁵⁴⁴ http://httpd.apache.org/security/vulnerabilities_24.html

36.	Apache HTTPD: XSS in mod_proxy_balancer (CVE-2012-4558) (apache-httpd-cve-2012-4558)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80 172.23.202.231:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy_balancer. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. XSS propust je uticao na manager interfejs mod_proxy_balancer-a.	APPLE APPLE-SA-2013-09-12-1 ⁸⁵⁴⁵ CVE CVE-2012-4558 ⁸⁵⁴⁶ DEBIAN DSA-2637 ⁸⁵⁴⁷ REDHAT RHSA-2013:0815 ⁸⁵⁴⁸ REDHAT RHSA-2013:1207 ⁸⁵⁴⁹ REDHAT RHSA-2013:1208 ⁸⁵⁵⁰ REDHAT RHSA-2013:1209 ⁸⁵⁵¹ URL1 ⁸⁵⁵² URL2 ⁸⁵⁵³	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.24 Ažurirati na Apache HTTPD version 2.2.24 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz Apache HTTPD >= 2.4 and < 2.4.4 Ažurirati na Apache HTTPD version 2.4.4 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz
37.	Apache HTTPD: mod_dav crash (CVE-2013-1896) (apache-httpd-cve-2013-1896)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80 172.23.202.231:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_dav_svn. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Slanje MERGE zahteva URI-ju koji obrađuje mod_dav_svn sa izvorom href (poslato kao deo zahteva XML) ciljajući na URI koji nije konfigurisan za DAV prouzrokuje segmentation fault (segfault).	CVE CVE-2013-1896 ⁸⁵⁵⁴ OVAL OVAL18835 ⁸⁵⁵⁵ REDHAT RHSA-2013:1156 ⁸⁵⁵⁶ REDHAT RHSA-2013:1207 ⁸⁵⁵⁷ REDHAT RHSA-2013:1208 ⁸⁵⁵⁸ REDHAT RHSA-2013:1209 ⁸⁵⁵⁹ SECUNIA 55032 ⁸⁵⁶⁰ URL1 ⁸⁵⁶¹ URL2 ⁸⁵⁶²	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.25 Ažurirati na Apache HTTPD version 2.2.25 Apache HTTPD >= 2.4 and < 2.4.6 Ažurirati na Apache HTTPD version 2.4.6 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.6.tar.gz
38.	Apache HTTPD: mod_log_config crash (CVE-2012-0021) (apache-httpd-cve-2012-0021)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80 172.23.202.231:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_log_config. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u modulu	APPLE APPLE-SA-2012-09-19-2 ⁸⁵⁶³ CVE CVE-2012-0021 ⁸⁵⁶⁴ IAVM 2012-A-0017 ⁸⁵⁶⁵ SECUNIA 48551 ⁸⁵⁶⁶ URL1 ⁸⁵⁶⁷	Umeren	Apache HTTPD >= 2.2 and < 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz

⁸⁵⁴⁵ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁸⁵⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4558>⁸⁵⁴⁷ <http://www.debian.org/security/2013/dsa-2637>⁸⁵⁴⁸ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁸⁵⁴⁹ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁸⁵⁵⁰ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁸⁵⁵¹ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁸⁵⁵² http://httpd.apache.org/security/vulnerabilities_22.html⁸⁵⁵³ http://httpd.apache.org/security/vulnerabilities_24.html⁸⁵⁵⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1896>⁸⁵⁵⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18835>⁸⁵⁵⁶ <http://rhn.redhat.com/errata/RHSA-2013-1156.html>⁸⁵⁵⁷ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁸⁵⁵⁸ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁸⁵⁵⁹ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁸⁵⁶⁰ <http://secunia.com/advisories/55032/>⁸⁵⁶¹ http://httpd.apache.org/security/vulnerabilities_22.html⁸⁵⁶² http://httpd.apache.org/security/vulnerabilities_24.html⁸⁵⁶³ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁸⁵⁶⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0021>⁸⁵⁶⁵ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁵⁶⁶ <http://secunia.com/advisories/48551/>⁸⁵⁶⁷ http://httpd.apache.org/security/vulnerabilities_22.html

		mod_log_config. Ako je u upotrebi "%{cookienam}C" log format string, udaljeni napadač bi mogao da pošalje specifičan kolačić koji bi doveo do kraha. Krah bi se pokazao kao odbijanje servisa ako se koristi threaded MPM.			
39.	Apache HTTPD: XSS in mod_negotiation when untrusted uploads are supported (CVE-2012-2687) (apachehttpd-cve-2012-2687)	172.23.202.122:80 172.23.202.232:80 172.23.202.200:80 172.23.202.230:80 172.23.202.135:80 172.23.202.231:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_negotiation. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Moguće je ubaciti CRLF (Carriage Return and Line Feed) koji omogućava CRLF Injection napade (poznatih i kao HTTP Response Splitting) za sajtove koji koriste mod_negotiation, omogućavajući neproverene upload-ove na lokacije na kojima je omogućen MultiViews (višestruko pregledanje). Ovaj problem je poznat i kao CVE-2008-0455.	APPLE APPLE-SA-2013-09-12-1⁸⁵⁶⁸ BID 55131⁸⁵⁶⁹ CVE CVE-2012-2687⁸⁵⁷⁰ IAVM 2012-A-0139⁸⁵⁷¹ REDHAT RHSA-2012:1591⁸⁵⁷² REDHAT RHSA-2012:1592⁸⁵⁷³ REDHAT RHSA-2012:1594⁸⁵⁷⁴ REDHAT RHSA-2013:0130⁸⁵⁷⁵ SECUNIA 50894⁸⁵⁷⁶ SECUNIA 51607⁸⁵⁷⁷ URL1⁸⁵⁷⁸ URL2⁸⁵⁷⁹	Umeren	Apache HTTPD >= 2.2 and < 2.2.23 Ažurirati na Apache HTTPD version 2.2.23 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz Apache HTTPD >= 2.4 and < 2.4.3 Ažurirati na Apache HTTPD version 2.4.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.3.tar.gz

Tabela 129. Linux OS sa IP adresama 172.23.202.133, 172.23.202.132, 172.23.202.123, 172.23.202.229 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.133		OS: Ubuntu 10.04.2 lts x64 server, ubuntu1004srvx64			44
IP adresa: 172.23.202.132		OS: Ubuntu 10.04.2 lts x86 server, ubuntu1004srvx86			44
IP adresa: 172.23.202.123		OS: Kubuntu 10.04.2 desktop x86, kubuntu1004dskx86			44
IP adresa: 172.23.202.229		OS: Kubuntu 10.04.2 desktop x64, kubuntu1004dskx64			44
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Apache httpd mod_isapi module unload flaw (CVE-2010-0425)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80	BID 38494⁸⁵⁸⁰ CERT-VN 280613⁸⁵⁸¹ CVE CVE-2010-0425⁸⁵⁸²	Kritičan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati:

⁸⁵⁶⁸ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>

⁸⁵⁶⁹ <http://www.securityfocus.com/bid/55131>

⁸⁵⁷⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2687>

⁸⁵⁷¹ <http://iase.disa.mil/stigs/iavm-cve.html>

⁸⁵⁷² <http://rhn.redhat.com/errata/RHSA-2012-1591.html>

⁸⁵⁷³ <http://rhn.redhat.com/errata/RHSA-2012-1592.html>

⁸⁵⁷⁴ <http://rhn.redhat.com/errata/RHSA-2012-1594.html>

⁸⁵⁷⁵ <http://rhn.redhat.com/errata/RHSA-2013-0130.html>

⁸⁵⁷⁶ <http://secunia.com/advisories/50894/>

⁸⁵⁷⁷ <http://secunia.com/advisories/51607/>

⁸⁵⁷⁸ http://httpd.apache.org/security/vulnerabilities_22.html

⁸⁵⁷⁹ http://httpd.apache.org/security/vulnerabilities_24.html

⁸⁵⁸⁰ <http://www.securityfocus.com/bid/38494>

⁸⁵⁸¹ <http://www.kb.cert.org/vuls/id/280613>

	(apache-httpd-2_2_x-mod_isapi-moduleunload-flaw-cve-2010-0425)	172.23.202.229:80 U modulu mod_isapi je pronađen propust koji će pokušati da ukloni ISAPI dll kada naiđe na greške. To može ostaviti povratne pozive u nedefinisanom stanju greške i kao posledica može da se javi segmentation fault. Na Windows platformama koje koriste mod_isapi, udaljeni napadač bi mogao da pošalje zlonameran zahtev da pokrene ovaj problem, a kako win32 MPM pokreće samo jedan proces, to bi kao ishod imalo odbijanje servisa i potencijalno dozvolilo da se pokrene proizvoljan kôd. Napomena: Zahvaljujući Brett Gervasoni-ju iz "Sense of Security" ovaj problem je prijavljen i za njega je predložena zakrpa.	OVAL OVAL8439⁸⁵⁸³ SECUNIA 38978⁸⁵⁸⁴ SECUNIA 39628⁸⁵⁸⁵ URL1⁸⁵⁸⁶ XF apache-http-modisapi-ocp- unspecified(56624)⁸⁵⁸⁷		http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz
2.	Anonymous users can obtain the Windows password policy (cifs-nt-0002)	Korišćenjem CIFS NULL sesije, anonimni korisnik može da dobije uvid u polisu šifri. Polisa šifri sadrži osetljive informacije o najmanjoj mogućoj dužini lozinke, zaključavanje šifre, vremensko trajanje zaključanosti šifre itd.	SANS-01 W5⁸⁵⁸⁸ CVE CVE-2000-1200⁸⁵⁸⁹ XF nt-lsa-domain-sid(4015)⁸⁵⁹⁰ SANS-02 W5⁸⁵⁹¹ BID 959⁸⁵⁹² SANS-04 W3⁸⁵⁹³ SANS-03 W5⁸⁵⁹⁴ BID 87⁸⁵⁹⁵	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost.
3.	HTTP Basic Authentication Enabled (http-basic-auth-clear-text)	172.23.202.133:8080 172.23.202.132:8080 172.23.202.123:8080 172.23.202.229:8080 HTTP Basic Authentication šema se ne smatra sigurnom metodom autentifikacije korisnika (ukoliko se ne koristi u kombinaciji sa nekim spoljnim sigurnosnim sistemom, kao TLS/SSL), s obzirom da se korisničko ime i lozinka preko mreže prenose kao običan tekst. Primer: Pokretanje ranjivog HTTP servisa http://172.23.202.133:8080/manager/html 1: Basic realm="Tomcat Manager Application"	URL1⁸⁵⁹⁶	Kritičan	Koristiti Osnovnu Autentifikaciju preko TLS/SSL (HTTPS). Omogućiti HTTPS na Web serveru. TLS/SSL protokol će zaštititi akreditive osnovne autentifikacije u običnom tekstu. Koristiti Digest Authentication Replace Basic Authentication sa alternativnom Digest Authentication shemom. Po savremenim kriptografskim standardima, Digest Authentication je slaba. Ali za širok spektar namena, ona je korisna zamena za Basic Authentication (osnovnu autentifikaciju). Ona ispravlja neke, ali ne sve, slabosti Basic Authentication (osnovne

⁸⁵⁸² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0425>
⁸⁵⁸³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8439>
⁸⁵⁸⁴ <http://secunia.com/advisories/38978/>
⁸⁵⁸⁵ <http://secunia.com/advisories/39628/>
⁸⁵⁸⁶ http://httpd.apache.org/security/vulnerabilities_22.html
⁸⁵⁸⁷ <http://xforce.iss.net/xforce/xfdb/56624>
⁸⁵⁸⁸ <http://www.sans.org/critical-security-controls/#w5>
⁸⁵⁸⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2000-1200>
⁸⁵⁹⁰ <http://xforce.iss.net/xforce/xfdb/4015>
⁸⁵⁹¹ <http://www.sans.org/critical-security-controls/#w5>
⁸⁵⁹² <http://www.securityfocus.com/bid/959>
⁸⁵⁹³ <http://www.sans.org/critical-security-controls/#w3>
⁸⁵⁹⁴ <http://www.sans.org/critical-security-controls/#w5>
⁸⁵⁹⁵ <http://www.securityfocus.com/bid/87>
⁸⁵⁹⁶ <http://tools.ietf.org/html/rfc2617>

					autentifikacije). Videti RFC 2617 ⁸⁵⁹⁷ (odjeljak 4 Security Considerations) za više informacija.
4.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.133:139 172.23.202.133:445 172.23.202.132:139 172.23.202.132:445 172.23.202.123:139 172.23.202.123:445 172.23.202.229:139 172.23.202.229:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB 887429 URL1 ⁸⁵⁹⁸	Ozbiljan	Metoda za konfiguracije SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429. ⁸⁵⁹⁹ Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing</i> = <i>auto</i> ili da se zahteva SMB potpisivanje: <i>server signing</i> = <i>mandatory</i> .
5.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.133:139 172.23.202.133:445 172.23.202.132:139 172.23.202.132:445 172.23.202.123:139 172.23.202.123:445 172.23.202.229:139 172.23.202.229:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti.
6.	Apache HTTPD: expat DoS (CVE-2009-3560) (apache-httpd-cve-2009-3560)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u mogućnosti da dovede do toga da Apache parsira nepoverljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepoverljiv XML dokument (na primer kroz mod_dav),	BID 37203 ⁸⁶⁰⁰ CVE CVE-2009-3560 ⁸⁶⁰¹ DEBIAN DSA-1953 ⁸⁶⁰² IAVM 2012-A-0020 ⁸⁶⁰³ OVAL OVAL12942 ⁸⁶⁰⁴ REDHAT RHSA-2011:0896 ⁸⁶⁰⁵ OVAL OVAL10613 ⁸⁶⁰⁶ OVAL OVAL6883 ⁸⁶⁰⁷ SECUNIA 37537 ⁸⁶⁰⁸ SECUNIA 38231 ⁸⁶⁰⁹ SECUNIA 38794 ⁸⁶¹⁰ SECUNIA 38832 ⁸⁶¹¹ SECUNIA 38834 ⁸⁶¹² SECUNIA 39478 ⁸⁶¹³ SECUNIA 41701 ⁸⁶¹⁴ SECUNIA 43300 ⁸⁶¹⁵	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.17 Ažurirati na Apache HTTPD version 2.2.17 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz

⁸⁵⁹⁷ <http://tools.ietf.org/html/rfc2617#section-4>⁸⁵⁹⁸ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>⁸⁵⁹⁹ <http://support.microsoft.com/kb/887429>⁸⁶⁰⁰ <http://www.securityfocus.com/bid/37203>⁸⁶⁰¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3560>⁸⁶⁰² <http://www.debian.org/security/DSA-1953> pristupljeno dana 18.12.2011⁸⁶⁰³ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁶⁰⁴ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval:def:12942>⁸⁶⁰⁵ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁸⁶⁰⁶ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval:def:10613>⁸⁶⁰⁷ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval:def:6883>⁸⁶⁰⁸ <http://secunia.com/advisories/37537/>⁸⁶⁰⁹ <http://secunia.com/advisories/38231/>⁸⁶¹⁰ <http://secunia.com/advisories/38794/>⁸⁶¹¹ <http://secunia.com/advisories/38832/>⁸⁶¹² <http://secunia.com/advisories/38834/>⁸⁶¹³ <http://secunia.com/advisories/39478/>⁸⁶¹⁴ <http://secunia.com/advisories/41701/>

		mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	URL ⁸⁶¹⁶		
7.	Apache HTTPD: expat DoS (CVE-2009-3720) (apache-httpd-cve-2009-3720)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u mogućnosti da dovede do toga da Apache parsira nepoverljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	IAVM 2012-A-0020⁸⁶¹⁷ OVAL OVAL12719⁸⁶¹⁸ REDHAT RHSA-2011:0896⁸⁶¹⁹ CVE CVE-2009-3720⁸⁶²⁰ OVAL OVAL11019⁸⁶²¹ OVAL OVAL7112⁸⁶²² REDHAT RHSA-2010:0002⁸⁶²³ SECUNIA 37324⁸⁶²⁴ SECUNIA 37537⁸⁶²⁵ SECUNIA 37925⁸⁶²⁶ SECUNIA 38050⁸⁶²⁷ SECUNIA 38231⁸⁶²⁸ SECUNIA 38794⁸⁶²⁹ SECUNIA 38832⁸⁶³⁰ SECUNIA 38834⁸⁶³¹ SECUNIA 39478⁸⁶³² SECUNIA 41701⁸⁶³³ SECUNIA 43300⁸⁶³⁴ URL⁸⁶³⁵	Ozbiljan	Apache >= 2.0 and < 2.1 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.17 Ažurirati na Apache HTTPD version 2.2.17 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
8.	Apache HTTPD: apr_bridage_split_line DoS (CVE-2010-1623) (apache-httpd-cve-2010-1623)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako Apache procesira ne-SSL zahteve. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_brigade_split_line() u sklopu kompleta APR-util library, koji se	IAVM 2012-B-0056⁸⁶³⁶ OVAL OVAL12800⁸⁶³⁷ REDHAT RHSA-2011:0896⁸⁶³⁸ REDHAT RHSA-2011:0897⁸⁶³⁹ BID 43673⁸⁶⁴⁰ CVE CVE-2010-1623⁸⁶⁴¹ REDHAT RHSA-2010:0950⁸⁶⁴² SECUNIA 41701⁸⁶⁴³ SECUNIA 42015⁸⁶⁴⁴	Ozbiljan	Apache >= 2.0 and < 2.1 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.17 Ažurirati na Apache HTTPD version 2.2.17 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz

⁸⁶¹⁵ <http://secunia.com/advisories/43300/>⁸⁶¹⁶ http://httpd.apache.org/security/vulnerabilities_20.html⁸⁶¹⁷ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁶¹⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12719>⁸⁶¹⁹ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁸⁶²⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3720>⁸⁶²¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11019>⁸⁶²² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7112>⁸⁶²³ <http://rhn.redhat.com/errata/RHSA-2010-0002.html>⁸⁶²⁴ <http://secunia.com/advisories/37324/>⁸⁶²⁵ <http://secunia.com/advisories/37537/>⁸⁶²⁶ <http://secunia.com/advisories/37925/>⁸⁶²⁷ <http://secunia.com/advisories/38050/>⁸⁶²⁸ <http://secunia.com/advisories/38231/>⁸⁶²⁹ <http://secunia.com/advisories/38794/>⁸⁶³⁰ <http://secunia.com/advisories/38832/>⁸⁶³¹ <http://secunia.com/advisories/38834/>⁸⁶³² <http://secunia.com/advisories/39478/>⁸⁶³³ <http://secunia.com/advisories/41701/>⁸⁶³⁴ <http://secunia.com/advisories/43300/>⁸⁶³⁵ http://httpd.apache.org/security/vulnerabilities_20.html⁸⁶³⁶ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁶³⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12800>⁸⁶³⁸ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁸⁶³⁹ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>⁸⁶⁴⁰ <http://www.securityfocus.com/bid/43673>⁸⁶⁴¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1623>⁸⁶⁴² <http://rhn.redhat.com/errata/RHSA-2010-0950.html>⁸⁶⁴³ <http://secunia.com/advisories/41701/>⁸⁶⁴⁴ <http://secunia.com/advisories/42015/>

		koristi za procesiranje ne-SSL zahteva. Udaljeni napadač bi mogao da šalje zahteve, pažljivo izrađujući tajming za pojedinačne bajtove, što bi polako zauzimalo memoriju i potencijalno dovelo do odbijanja servisa.	SECUNIA 42361 ⁸⁶⁴⁵ SECUNIA 42367 ⁸⁶⁴⁶ SECUNIA 42403 ⁸⁶⁴⁷ SECUNIA 42537 ⁸⁶⁴⁸ SECUNIA 43211 ⁸⁶⁴⁹ SECUNIA 43285 ⁸⁶⁵⁰ URL1 ⁸⁶⁵¹		t/httpd/httpd-2.2.17.tar.gz
9.	Apache HTTPD: mod_dav DoS (CVE-2010-1452) (apache-httpd-cve-2010-1452)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako web server izvršava jedan od sledećih modula: mod_cache, mod_dav. Pregledajte konfiguraciju vašeg web servera radi validacije. Propust je otkriven u obradi zahteva od strane mod_cache i mod_dav. Zlonameran udaljeni napadač bi mogao da pošalje pažljivo izrađen zahtev i prouzrokuje da httpd child proces krahira. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM. Ovaj problem se dalje može ublažiti ako na mod_dav samo utiču zahtevi za koje postoji mogućnost autentifikovanja, a mod_cache je pod uticajem samo ako se koristi neuobičajena „CacheIgnoreURLSessionIdentifiers“ direktiva, uvedena u verziji 2.2.14. Ovaj problem je prijavio Mark Drayton.	IAVM 2012-B-0056 ⁸⁶⁵² OVAL OVAL12341 ⁸⁶⁵³ REDHAT RHSA-2011:0896 ⁸⁶⁵⁴ REDHAT RHSA-2011:0897 ⁸⁶⁵⁵ APPLE APPLE-SA-2011-03-21 ⁸⁶⁵⁶ CVE CVE-2010-1452 ⁸⁶⁵⁷ OVAL OVAL11683 ⁸⁶⁵⁸ REDHAT RHSA-2010:0659 ⁸⁶⁵⁹ SECUNIA 42367 ⁸⁶⁶⁰ URL1 ⁸⁶⁶¹	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.16 Ažurirati na Apache HTTPD version 2.2.16 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.16.tar.gz
10.	Apache httpd Timeout detection flaw (mod_proxy_http) (CVE-2010-2068) (apache-httpd-2_2_x-timeoutdetection-flaw-mod_proxy_http-cve-2010-2068)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Propust sa kojim je omogućeno otkrivanje informacija je otkriven u modulu mod_proxy_http na verzijama 2.2.9 do 2.2.15, 2.3.4-alpha i 2.3.5-alpha. Pod određenim tajmaut	APPLE APPLE-SA-2011-03-21 ⁸⁶⁶² BID 40827 ⁸⁶⁶³ CVE CVE-2010-2068 ⁸⁶⁶⁴ OVAL OVAL11491 ⁸⁶⁶⁵ OVAL OVAL6931 ⁸⁶⁶⁶ SECUNIA 40206 ⁸⁶⁶⁷ SECUNIA 41480 ⁸⁶⁶⁸ SECUNIA 41490 ⁸⁶⁶⁹	Ozbiljan	Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.16.tar.gz

⁸⁶⁴⁵ <http://secunia.com/advisories/42361/>⁸⁶⁴⁶ <http://secunia.com/advisories/42367/>⁸⁶⁴⁷ <http://secunia.com/advisories/42403/>⁸⁶⁴⁸ <http://secunia.com/advisories/42537/>⁸⁶⁴⁹ <http://secunia.com/advisories/43211/>⁸⁶⁵⁰ <http://secunia.com/advisories/43285/>⁸⁶⁵¹ http://httpd.apache.org/security/vulnerabilities_20.html⁸⁶⁵² <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁶⁵³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12341>⁸⁶⁵⁴ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁸⁶⁵⁵ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>⁸⁶⁵⁶ <http://lists.apple.com/archives/security-announce/2011/Mar/msg00006.html>⁸⁶⁵⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1452>⁸⁶⁵⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11683>⁸⁶⁵⁹ <http://rhn.redhat.com/errata/RHSA-2010-0659.html>⁸⁶⁶⁰ <http://secunia.com/advisories/42367/>⁸⁶⁶¹ http://httpd.apache.org/security/vulnerabilities_20.html⁸⁶⁶² <http://lists.apple.com/archives/security-announce/2011/Mar/msg00006.html>⁸⁶⁶³ <http://www.securityfocus.com/bid/40827>⁸⁶⁶⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2068>⁸⁶⁶⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11491>⁸⁶⁶⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6931>⁸⁶⁶⁷ <http://secunia.com/advisories/40206/>⁸⁶⁶⁸ <http://secunia.com/advisories/41480/>⁸⁶⁶⁹ <http://secunia.com/advisories/41490/>

		uslovima, server bi mogao da uzvрати odgovorom koji je namenjen drugom korisniku. Ugroženi su samo operativni sistemi Windows, Netware i OS2. Ugrožene su one konfiguracije koje pokreću korišćenje proxy worker pool-ova. Na ranijim verzijama nije bilo ranjivosti, jer proxy pool-ovi još nisu bili uvedeni. Zahvaljujući Loren Anderson-u ovaj problem je prijavljen, a najjednostavniji način njegovog izbegavanja jeste opšte konfigurisanje.	SECUNIA 41722 ⁸⁶⁷⁰ XF modproxyhttp-timeout- info-disc(59413) ⁸⁶⁷¹ URL1 ⁸⁶⁷²		
11.	X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch)	172.23.202.133:993 172.23.202.133:995 172.23.202.132:993 172.23.202.132:995 172.23.202.123:993 172.23.202.123:995 172.23.202.229:993 172.23.202.229:995 Rubrika u sertifikatu X.509 sa uobičajenim nazivom subjekta (CN) ne poklapa se sa imenom pojedinca koje je navedeno u sertifikatu. Pre izdavanja sertifikata, Certification Authority (CA) mora da proveriti identitet pojedinca koji potražuje sertifikat, kako je navedeno u CA-ovom Certification Practice Statement (CPS). Zbog toga, uobičajene procedure validacije sertifikata zahtevaju da rubrika sertifikata sa CN subjektom odgovara pravom imenu pojedinca koji prikazuje sertifikat. Na primer, u sertifikatu prikazanom na „https://www.example.com/“, naziv subjekta (CN) treba da bude „www.example.com“. U cilju otkrivanja i sprečavanja napada prisluškivanja, validnost sertifikata mora da bude overena, jer bi u suprotnom napadač mogao da otpočne napad preko posrednika i da stekne potpunu kontrolu nad protokom podataka. Od posebne važnosti je validnost naziva subjekta (CN), koji treba da se poklapa sa imenom pojedinca (imenom host-a). Neodgovarajući CN se najčešće javlja usled greške u konfiguraciji, iako on takođe može da ukazuje na to da se sprovodi napad preko posrednika.		Ozbiljan	Rubrika sa uobičajenim nazivom subjekta (CN) u sertifikatu X.509 treba da bude podešena da sadrži ime pojedinca koji prikazuje sertifikat (npr. ime hosta). To se postiže izradom novog sertifikata, koji najčešće potpisuje Certification Authority (CA), koji je od poverenja kako za klijenta, tako i za server.
12.	FTP server does not support AUTH command (ftp-generic-0007)	172.23.202.133:21 172.23.202.132:21 172.23.202.123:21 172.23.202.229:21 FTP klijenti po defaultu šalju FTP server-u poverljive podatke (korisnički ID i šifra) u vidu čitkog teksta. Ova okolnost dozvoljava		Ozbiljan	Ažurirati/preći na FTP server koji podržava AUTH komandu.

⁸⁶⁷⁰ <http://secunia.com/advisories/41722/>⁸⁶⁷¹ <http://xforce.iss.net/xforce/xfdb/59413>⁸⁶⁷² http://httpd.apache.org/security/vulnerabilities_22.html

		zlonamernim korisnicima da presreću poverljive podatke ukoliko prisluškuju vezu. Noviji FTP serveri podržavaju AUTH komandu, koja omogućava dodatne opcije autentifikacije, kao što su TLS, Kerberos, GSSAPI itd. Ona se može koristiti za sprečavanje prisluškivanja na FTP vezama.			
13.	Apache HTTPD: mod_proxy_ajp DoS (CVE-2010-0408) (apache-httpd-cve-2010-0408)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ajp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Mod_proxy_ajp će vratiti pogrešan kôd statusa ako naiđe na grešku, prouzrokujući da backend server bude stavljen u status greške dok ne istekne vreme za ponovni pokušaj. Udaljeni napadač bi mogao da pošalje zlonameran zahtev da bi pokrenuo ovaj problem, što bi dovelo do odbijanja servisa. Zahvaljujući Niku Toivola iz Sulake Corporation ovaj problem je prijavljen uz predloženu adekvatnu meru zaštite u vidu zakrpe.	BID 38491 ⁸⁶⁷³ CVE CVE-2010-0408 ⁸⁶⁷⁴ DEBIAN DSA-2035 ⁸⁶⁷⁵ OVAL OVAL8619 ⁸⁶⁷⁶ OVAL OVAL9935 ⁸⁶⁷⁷ REDHAT RHSA-2010:0168 ⁸⁶⁷⁸ SECUNIA 39100 ⁸⁶⁷⁹ SECUNIA 39501 ⁸⁶⁸⁰ SECUNIA 39628 ⁸⁶⁸¹ SECUNIA 39632 ⁸⁶⁸² SECUNIA 39656 ⁸⁶⁸³ SECUNIA 40096 ⁸⁶⁸⁴ URL1 ⁸⁶⁸⁵	Ozbiljan	Apache >= 2.2 and < 2.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz
14.	Browsable web directory (http-generic-browsable-dir)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Otkriven je direktorijum na web serveru koji može biti pretraživan, što znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice - spajdering (prateći hiperlinkove), ili -kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute force napadom na liste uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skrivena“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice.		Ozbiljan	Za Apache: onemogućiti pretraživanje direktorijuma mreže za sve direktorijume i poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i

⁸⁶⁷³ <http://www.securityfocus.com/bid/38491>⁸⁶⁷⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0408>⁸⁶⁷⁵ <http://www.debian.org/security/2010/dsa-2035>⁸⁶⁷⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8619>⁸⁶⁷⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:9935>⁸⁶⁷⁸ <http://rhn.redhat.com/errata/RHSA-2010-0168.html>⁸⁶⁷⁹ <http://secunia.com/advisories/39100/>⁸⁶⁸⁰ <http://secunia.com/advisories/39501/>⁸⁶⁸¹ <http://secunia.com/advisories/39628/>⁸⁶⁸² <http://secunia.com/advisories/39632/>⁸⁶⁸³ <http://secunia.com/advisories/39656/>⁸⁶⁸⁴ <http://secunia.com/advisories/40096/>⁸⁶⁸⁵ http://httpd.apache.org/security/vulnerabilities_22.html

					nepoznate fajlove i direktorijume. Za Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote: Onemogućiti pretraživanje direktorijuma za sve direktorijume i poddirektorijume. Uključiti Tomcat-ov web.xml file. U odeljku „default“, promeniti parametar „listings“ iz „true“ u „false“. Restartovati server. Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripta i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume.
15.	Form action submits sensitive data in the clear (http-generic-sensitive-form-data-unencrypted)	172.23.202.133:8080 172.23.202.132:8080 172.23.202.123:8080 172.23.202.229:8080 Web forma sadrži rubrike sa podacima koji su možda po prirodi osetljivi. Ovakvi podaci se prenose preko nezaštićene veze, koja bi mogla da omogućiti zlonamernim napadačima da prisluškujući mrežu pregledaju podatke u vidu običnog teksta. Formatiranje preko <code>http://localhost:8080/examples/jsp/security/protected/_vti_shm/j_security_check</code> prosleđuje sledeće nezaštićene osetljive rubrike: <code>j_password</code>		Ozbiljan	Isključiti HTTPS protokol na serveru. Promeniti „action“ URL na oznaci rubrike da koristi HTTPS protokol („https://...“) umesto samo HTTP protokol („http://...“). Sve osetljive podatke treba slati preko HTTPS umesto preko HTTP.
16.	TLS/SSL Server Supports Weak Cipher Algorithms (ssl-weak-ciphers)	172.23.202.133:993 172.23.202.132:993 172.23.202.123:993 172.23.202.229:993 negotiated the SSL_DHE_RSA_WITH_DES_CBC_SHA cipher suite TLS/SSL server podržava šifre koje se zasnivaju na slabim algoritmima. To napadaču može omogućiti da pokrene napade preko posrednika i da pregleda ili čačka osetljive podatke. Uopšteno, sledeće šifre se smatraju slabim: Tzv. „null“ (nula) šifre, jer ne šifruju podatke. Eksportne šifre koje koriste dužine tajnih ključeva ograničene na 40 bitova. Na to najčešće ukazuje reč EXP/EXPORT u nazivu šifre.		Ozbiljan	Konfigurisati server tako da onemogući podršku za slabe šifre. Za Apache web servere sa mod_ssl, uključiti fajl Apache konfiguracije i izmeniti liniju SSLCipherSuite tako da u njoj piše: <code>SSLCipherSuite ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM</code>

		Zastareli algoritmi za šifrovanje čije se dužine tajnih ključeva po današnjim standardima smatraju kratkim, npr. DES ili RC4 sa 56-bitnim ključevima.			
17.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	TCP reset with incorrect sequence number triggered this fault on 172.23.202.133:22 172.23.202.132:22 172.23.202.123:143 172.23.202.229:143 Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hедера i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	OSVDB 4030 ⁸⁶⁸⁶ BID: 10183 ⁸⁶⁸⁷ CERT-VN: 415294 ⁸⁶⁸⁸ CVE CVE-2004-0230 ⁸⁶⁸⁹ MS: MS05-019 ⁸⁶⁹⁰ MS: MS06-064 ⁸⁶⁹¹ NETBSD: NetBSD-SA2004-006 ⁸⁶⁹² OVAL: OVAL2689 ⁸⁶⁹³ OVAL: OVAL270 ⁸⁶⁹⁴ OVAL OVAL3508 ⁸⁶⁹⁵ OVAL OVAL4791 ⁸⁶⁹⁶ OVAL OVAL5711 ⁸⁶⁹⁷ SECUNIA: 11440 ⁸⁶⁹⁸ SECUNIA 11458 ⁸⁶⁹⁹ SECUNIA: 22341 ⁸⁷⁰⁰ SGI 20040403-01-A ⁸⁷⁰¹ XF tcp-rst-dos(15886) ⁸⁷⁰² URL1 ⁸⁷⁰³ URL2 ⁸⁷⁰⁴	Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC 2385 ⁸⁷⁰⁵ . Ono je napravljeno da smanji opasnost od određenih napada na BGP, kao što su TCP reseti.
18.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podesi na jedinstvenu vrednost i da se koristi u rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da fingerprint-uje operativni sistem.	BID 4314 ⁸⁷⁰⁶ CVE CVE-2002-0510 ⁸⁷⁰⁷ XF linux-udp-fingerprint(8588) ⁸⁷⁰⁸	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili pak ranjivost koju treba popravljati, tako da ne postoje rešenja koja se mogu kupiti. Jedino se može postaviti fajervol ili neka druga sprava za filtriranje između napadnutog i neprijateljskog napada koji je u mogućnosti da randomizuje IP ID-jeve.
19.	Apache HTTPD: apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80	CVE CVE-2011-0419 ⁸⁷⁰⁹ DEBIAN DSA-2237 ⁸⁷¹⁰ IAVM 2012-B-0056 ⁸⁷¹¹ OVAL OVAL14638 ⁸⁷¹² OVAL OVAL14804 ⁸⁷¹³	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim

⁸⁶⁸⁶ <http://www.osvdb.org/4030>⁸⁶⁸⁷ <http://www.securityfocus.com/bid/10183>⁸⁶⁸⁸ <http://www.kb.cert.org/vuls/id/415294>⁸⁶⁸⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁸⁶⁹⁰ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁸⁶⁹¹ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁸⁶⁹² <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁸⁶⁹³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>⁸⁶⁹⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>⁸⁶⁹⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>⁸⁶⁹⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>⁸⁶⁹⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>⁸⁶⁹⁸ <http://secunia.com/advisories/11440/>⁸⁶⁹⁹ <http://secunia.com/advisories/11458/>⁸⁷⁰⁰ <http://secunia.com/advisories/22341/>⁸⁷⁰¹ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>⁸⁷⁰² <http://xforce.iss.net/xforce/xfdb/15886>⁸⁷⁰³ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁸⁷⁰⁴ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>⁸⁷⁰⁵ <http://www.ietf.org/rfc/rfc2385.txt>⁸⁷⁰⁶ <http://www.securityfocus.com/bid/4314>⁸⁷⁰⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>⁸⁷⁰⁸ <http://xforce.iss.net/xforce/xfdb/8588>⁸⁷⁰⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419>⁸⁷¹⁰ <http://www.debian.org/security/2011/dsa-2237>⁸⁷¹¹ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁷¹² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14638>

	httpdcve-2011-0419)	Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_autoindex. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_fnmatch() u sklopu APR biblioteke. Ako je omogućen mod_autoindex, a indeksi direktorijuma mod_autoindex su sadržavali fajlove sa dovoljno dugim nazivima, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do preterane upotrebe CPU-a. Ovo bi moglo da bude iskorišćeno u napadu odbijanja servisa. Zahvaljujući Maksymilian Arciemowicz prijavljen je ovaj propust.	REDHAT ⁸⁷¹⁴ 2011:0896 RHSA- REDHAT ⁸⁷¹⁵ 2011:0897 RHSA- REDHAT ⁸⁷¹⁶ 2011:0507 RHSA- SECUNIA ⁸⁷¹⁷ 44490 SECUNIA ⁸⁷¹⁸ 44564 SECUNIA ⁸⁷¹⁹ 44574 URL1 ⁸⁷²⁰		instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.19 Ažurirati na Apache HTTPD version 2.2.19 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.19.tar.gz
20.	Apache Etag Inode Information Leakage (http-apache-etag-inode-leak)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 U određenim konfiguracijama, Apache HTTP server dozvoljava udaljenim napadačima da dobiju poverljive informacije preko (1) Etag heder-a, koji otkriva broj inoda ili (2) razdvajanje višedelnih MIME-a, koja ukazuje na ID child procesa (PID). Određene verzije Apache-a koriste zahtevani broj čvorova fajla da bi konstruisali 'Etag' heder za odgovor. Iako sama po sebi nije ranjivost, ova informacija olakšava sprovođenje određenih NFS napada. „Running vulnerable HTTP service: Apache 2.2.14. <a a3746-b1-4a774f890d43c\""="" href="http://172.23.202.133/1: \">http://172.23.202.133/1: \"a3746-b1-4a774f890d43c\"	BID ⁸⁷²¹ 6939 BID ⁸⁷²² 6943 CVE ⁸⁷²³ CVE-2003-1418 XF ⁸⁷²⁴ apache-mime-information-disclosure(11438)	Ozbiljan	Onemogućiti Etag mehanizam tipa "inod-based" konfiguraciji Apache-a. Takođe, inod informacije je moguće ukloniti iz Etag heder-a tako što će se dodati direktiva u Apache konfiguraciju: <i>FileETag Mtime Size</i>
21.	Apache HTTPD: Subrequest handling of request headers (mod_headers) (CVE-2010-0434) (apache-httpdcve-2010-0434)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_headers. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust u jezgu "subrequest process	APPLE ⁸⁷²⁵ APPLE-SA-2010-11-10 BID ⁸⁷²⁶ 38494 CVE ⁸⁷²⁷ CVE-2010-0434 DEBIAN ⁸⁷²⁸ DSA-2035 OVAL ⁸⁷²⁹ OVAL10358 OVAL ⁸⁷³⁰ OVAL8695 REDHAT ⁸⁷³¹ 2010:0168 RHSA- REDHAT RHSA-	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.15 Ažurirati na Apache HTTPD version 2.2.15 Uraditi download a zatim

⁸⁷¹³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14804>⁸⁷¹⁴ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁸⁷¹⁵ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>⁸⁷¹⁶ <http://rhn.redhat.com/errata/RHSA-2011-0507.html>⁸⁷¹⁷ <http://secunia.com/advisories/44490/>⁸⁷¹⁸ <http://secunia.com/advisories/44564/>⁸⁷¹⁹ <http://secunia.com/advisories/44574/>⁸⁷²⁰ http://httpd.apache.org/security/vulnerabilities_22.html⁸⁷²¹ <http://www.securityfocus.com/bid/6939>⁸⁷²² <http://www.securityfocus.com/bid/6943>⁸⁷²³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-1418>⁸⁷²⁴ <http://xforce.iss.net/xforce/xfdb/11438>⁸⁷²⁵ <http://support.apple.com/kb/ht4435>⁸⁷²⁶ <http://www.securityfocus.com/bid/38494>⁸⁷²⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0434>⁸⁷²⁸ <http://www.debian.org/security/2010/dsa-2035>⁸⁷²⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10358>⁸⁷³⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8695>⁸⁷³¹ <http://rhn.redhat.com/errata/RHSA-2010-0168.html>

		code" može dovesti do greške tipa segmentation fault-a ili do otkrivanja podataka iz nekog drugog zahteva na thread-ovima servera, kao što su worker ili winnt MPM-ovi. Zahvaljujući Philip Pickett-u iz Vmware, ovaj propust je prijavljen i predložen je način ispravke.	2010:0175 ⁸⁷³² SECUNIA 39100 ⁸⁷³³ SECUNIA 39115 ⁸⁷³⁴ SECUNIA 39501 ⁸⁷³⁵ SECUNIA 39628 ⁸⁷³⁶ SECUNIA 39632 ⁸⁷³⁷ SECUNIA 39656 ⁸⁷³⁸ SECUNIA 40096 ⁸⁷³⁹ XF apache-http-rh-info-disclosure(56625) ⁸⁷⁴⁰ URL1 ⁸⁷⁴¹		instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.15.tar.gz
22.	Apache Tomcat v4.x Example Scripts Information Leakage (http-tomcat-0005)	172.23.202.133:8080 172.23.202.132:8080 172.23.202.123:8080 172.23.202.229:8080 Sledeće skripte su navedene kao primeri koji dolaze sa Apache Tomcat-om v4.x, a koje napadači mogu da iskoriste da dobiju informacije o sistemu. Poznato je da su ove skripte ranjive na napad tipa "cross site scripting" (XSS): /examples/jsp/num/numguess.jsp /examples/jsp/dates/date.jsp /examples/jsp/snp/snoop.jsp /examples/jsp/error/error.html /examples/jsp/sessions/carts.html /examples/jsp/checkbox/check.html /examples/jsp/colors/colors.html /examples/jsp/cal/login.html /examples/jsp/include/include.jsp /examples/jsp/forward/forward.jsp /examples/jsp/plugin/plugin.jsp /examples/jsp/jsptoserv/jsptoservlet.jsp p /examples/jsp/simpletag/foo.jsp /examples/jsp/mail/sendmail.jsp /examples/servlet/HelloWorldExample /examples/servlet/RequestInfoExample /examples/servlet/RequestHeaderExample /examples/servlet/RequestParamExample /examples/servlet/CookieExample /examples/servlet/JndiServlet /examples/servlet/SessionExample /tomcat-docs/appdev/sample/web/hello.jsp		Kritičan	U potpunosti obrisati ove skripte. Primeri skripta nikad ne treba da budu instalirani na serverima koji su u produkciji.
23.	Self-signed TLS/SSL certificate (ssl-self- signed-certificate)	172.23.202.133:993 172.23.202.133:995 172.23.202.132:993 172.23.202.132:995 172.23.202.123:993 172.23.202.123:995 172.23.202.229:993		Ozbiljan	Nabaviti novi TLS/SSL serverov sertifikat koji NIJE samopotpisan i instalirati ga na server. Precizna uputstva za dobijanje novog sertifikata zavise od zahteva organizacije. Uopšteno,

⁸⁷³² <http://rhn.redhat.com/errata/RHSA-2010-0175.html>⁸⁷³³ <http://secunia.com/advisories/39100/>⁸⁷³⁴ <http://secunia.com/advisories/39115/>⁸⁷³⁵ <http://secunia.com/advisories/39501/>⁸⁷³⁶ <http://secunia.com/advisories/39628/>⁸⁷³⁷ <http://secunia.com/advisories/39632/>⁸⁷³⁸ <http://secunia.com/advisories/39656/>⁸⁷³⁹ <http://secunia.com/advisories/40096/>⁸⁷⁴⁰ <http://xforce.iss.net/xforce/xfdb/56625>⁸⁷⁴¹ http://httpd.apache.org/security/vulnerabilities_20.html

		172.23.202.229:995 TLS/SSL-a sertifikat servera je samopotpisan. Samopotpisani sertifikati po defaultu nisu od poverenja, naročito zato što napadi na TLS/SSL preko posrednika obično koriste samopotpisane sertifikate da prisluškuju TLS/SSL veze.			treba napraviti zahtev za sertifikat i taj zahtev sačuvati kao fajl. Ovaj fajl se zatim šalje Certificate Authority-ju (CA) na obradu. Organizacija možda poseduje sopstveni interni Certificate Authority. U suprotnom, potrebno je platiti sertifikat iz spoljnog poverljivog Certificate Authority-ja, kao što su Thawte , Verisign .
24.	Autocomplete enabled for sensitive HTML form fields (spider-sensitive-form-data-autocomplete-enabled)	172.23.202.133:8080 172.23.202.132:8080 172.23.202.123:8080 172.23.202.229:8080 Web forma sadrži lozinke i druge rubrike sa osetljivim tekstom za koje je otvorena mogućnost auto-complete od strane web pretraživača. Funkcija auto-complete skladišti forme popunjenih rubrika i lozinke lokalno, na web pretraživaču, tako da se ove rubrike automatski popunjavaju kada korisnik ponovo poseti sajt. Osetljivi podaci i lozinke mogu biti ukradeni ako je korisnikov sistem kompromitovan. Međutim, treba imati u vidu da forma auto-complete nije standardna i da je to karakteristika web pretraživača koju svaki web pretraživač tretira na različit način. Na primer Opera zanemaruje ovu opciju i zahteva od korisnika da unese poverljive podatke svaki put kada posećuje određeni web sajt.		Umeren	Za svaku osetljivu rubriku u HTML, stavku „autocomplete“ potrebno je podesiti na „off“. Na primer: <input type=“password“ autocomplete=“off“ name=“pw“> Ako ima previše rubrika, možda je brže podesiti stavku „autocomplete“ na „off“ u spoljnom tagu <form>. Na primer: <form action=“/login.jsp“ autocomplete=“off“ name=“pw“> <input type=“password“ name=“pw“> </form>
25.	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server . Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko poziva udaljenih procedura (RPC). Ovi servisi su i u prošlosti bili skloni ranjivostima.. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinjenije napade.	BID: 494 ⁸⁷⁴² CVE: CVE-1999-0519 ⁸⁷⁴³ MSKB: 143474 ⁸⁷⁴⁴ URL ⁸⁷⁴⁵	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost.
26.	Apache default installation/welcome page installed (http-apache-default-install-	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80		Umeren	Ako se od servera zahteva da obezbedi neophodnu funkcionalnost, onda defaultnu stranicu treba zameniti odgovarajućim

⁸⁷⁴² <http://www.securityfocus.com/bid/494>⁸⁷⁴³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>⁸⁷⁴⁴ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>⁸⁷⁴⁵ http://www.hsc.fr/ressources/presentations/null_sessions/

	page)	Apache difoltna instalacija ili „Welcome“ stranica je instalirana na serveru. To obično ukazuje na novoinstalirani server. U mnogim slučajevima, Apache se instalira zajedno sa drugim aplikacijama i korisnik možda nije svestan da je web server pokrenut. Ovakvi serveri se retko patch-uju i još rede nadgledaju, što zlonamernim napadačima postaje pogodna meta koja najverovatnije neće pokrenuti nikakvo upozorenje. Primer : Running vulnerable HTTP service: Apache 2.2.14. http://172.23.202.133/ 1: <code><html><body><h1>It works!</h1></code>			sadržajem. U suprotnom, ovakav server treba ukloniti sa mreže, prateći bezbednosni princip minimalne složenosti (više složenosti = manja bezbednost). Ako server nije potreban, treba ga ukloniti iz svih startup fajlova (npr. /etc/rc*) ili skripti, a zatim prekinuti servis. Proveriti da li se on ponovo pokreće kada se mašina reboot-uje. Apache se uglavnom instalira kao /usr/sbin/httpd na UNIX mašinama ili kao C:\Program Files\Apache Group na Windows mašinama. Razmotriti uklanjanje binara i svih srodnih biblioteka iz sistema.
27.	Apache Tomcat default installation/welcome page installed (http-tomcat-default-install-page)	172.23.202.133:8080 172.23.202.132:8080 172.23.202.123:8080 172.23.202.229:8080 Tomcat difoltna instalacija ili „Welcome“ stranica je instalirana na serveru. To obično ukazuje na novoinstalirani server. U mnogim slučajevima, Tomcat se instalira zajedno sa drugim aplikacijama i korisnik možda nije svestan da je web server pokrenut. Ovakvi serveri se retko patch-uju i još rede nadgledaju, što zlonamernim napadačima postaje pogodna meta koja najverovatnije neće pokrenuti nikakvo upozorenje. Pokretanje ranjivog HTTP servisa: Apache Tomcat. http://172.23.202.133:8080/ 8: 9: <code><body></code> 10: <code><h1>It works !</h1></code> 11: 12: ... means you've setup Tomcat successfully. Congratulations!</p>		Umeren	Ako se od servera zahteva da obezbedi neophodnu funkcionalnost, onda difoltnu stranicu treba zameniti odgovarajućim sadržajem. U suprotnom, ovakav server treba ukloniti sa mreže, prateći bezbednosni princip minimalne složenosti (više složenosti = manja bezbednost).
28.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov	CVE CVE-1999-0524⁸⁷⁴⁶ OSVDB 95⁸⁷⁴⁷ XF icmp-netmask(306)⁸⁷⁴⁸ XF icmp-timestamp(322)⁸⁷⁴⁹	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.

⁸⁷⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁸⁷⁴⁷ <http://www.osvdb.org/95>⁸⁷⁴⁸ <http://xforce.iss.net/xforce/xfdb/306>⁸⁷⁴⁹ <http://xforce.iss.net/xforce/xfdb/322>

		zahtev za vremenski pečat.			
29.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1⁸⁷⁵⁰ URL2⁸⁷⁵¹ URL3⁸⁷⁵²	Umeren	Onemogućavanje TCP timestamp odgovora na Linux OS. Podesiti net.ipv4.tcp_timestamps vrednost na sledećem ključu na 0 pokretanjem sledeće komande: sysctl -w net.ipv4.tcp_timestamps=0 Dodatno, sledeću vrednost u difoltnom sysctl konfiguracionom fajlu, generally sysctl.conf: net.ipv4.tcp_timestamps=0
30.	Database Open Access (database-open-access)	172.23.202.133:3306 172.23.202.132:3306 172.23.202.123:3306 172.23.202.229:3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7.	URL1⁸⁷⁵³	Umeren	Konfigurisati server baze podataka tako da dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.
31.	Samba RPC unauthenticated remote code execution (CVE-2012-1182) (cifs-samba-cve-2012-1182)	172.23.202.133:139 172.23.202.133:445 172.23.202.132:139 172.23.202.132:445 172.23.202.123:139 172.23.202.123:445 172.23.202.229:139 172.23.202.229:445 Određene verzije Samba-e sadrže sigurnosni propust u interfejsu poziva udaljenih procedura (RPC). Posledica ovog propusta je da udaljeni napadač može pokrenuti daljinsko izvršenje koda u sklopu smbd procesa, preko crafted RPC paketa, koji bi doveo do preopeterećenja bafera. Ova ranjivost ne zahteva autentifikovanu vezu da bi pokrenula nove eksploite, a s obzirom da Samba radi kao root, ovo je jedna od najopasnijih ranjivosti.	APPLE APPLE-SA-2012-05-09-1⁸⁷⁵⁴ CVE CVE-2012-1182⁸⁷⁵⁵ IAVM 2012-A-0085⁸⁷⁵⁶ SECUNIA 48999⁸⁷⁵⁷ URL1⁸⁷⁵⁸	Kritičan	Uraditi download a zatim instalirati: http://www.samba.org Zakrpljene verzije Samba-e obuhvataju v3.6.4, v3.5.14, i v3.4.16, a puštene su u opticaj 10. aprila 2012. Većina Linux distributera prodaje starije verzije Samba-e, ali poseduje backportovane popravke za bezbednosne propuste (kako od prodavca - Samba-e - tako i od samih distributera). Treba ažurirati dobijenu verziju od distributera preko system package manager-a.

⁸⁷⁵⁰ http://www.forensicswiki.org/wiki/TCP_timestamps⁸⁷⁵¹ <http://www.ietf.org/rfc/rfc1323.txt>⁸⁷⁵² <http://uptime.netcraft.com/>⁸⁷⁵³ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf⁸⁷⁵⁴ <http://lists.apple.com/archives/security-announce/2012/May/msg00001.html>⁸⁷⁵⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1182>⁸⁷⁵⁶ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁷⁵⁷ <http://secunia.com/advisories/48999/>⁸⁷⁵⁸ <http://www.mandriva.com/en/support/security/advisories/advisory/MDVSA-2012:055/?name=MDVSA-2012:055>

32.	Apache HTTPD: Range header remote DoS (CVE-2011-3192) (apache-httpd-cve-2011-3192)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Propust je otkriven u načinu na koji Apache HTTP Server obrađuje Range HTTP hedere. Zlonamerni napadač bi mogao da iskoristi ovaj propust i dovede do toga da http koristi veliku količinu memorije i CPU vremena preko HTTP zahteva sa posebno kreiranim Range hederom. Ovo bi moglo dovesti do napada odbijanja servisa. Advisory: CVE-2011-3192.txt	APPLE APPLE-SA-2011-10-12-3 ⁸⁷⁵⁹ BID 49303 ⁸⁷⁶⁰ CERT-VN 405811 ⁸⁷⁶¹ CVE CVE-2011-3192 ⁸⁷⁶² IAVM 2012-B-0056 ⁸⁷⁶³ OSVDB 74721 ⁸⁷⁶⁴ OVAL OVAL14762 ⁸⁷⁶⁵ OVAL OVAL14824 ⁸⁷⁶⁶ OVAL OVAL18827 ⁸⁷⁶⁷ REDHAT RHSA-2011:1245 ⁸⁷⁶⁸ REDHAT RHSA-2011:1294 ⁸⁷⁶⁹ REDHAT RHSA-2011:1300 ⁸⁷⁷⁰ REDHAT RHSA-2011:1329 ⁸⁷⁷¹ REDHAT RHSA-2011:1330 ⁸⁷⁷² REDHAT RHSA-2011:1369 ⁸⁷⁷³ SECUNIA 45606 ⁸⁷⁷⁴ SECUNIA 45937 ⁸⁷⁷⁵ SECUNIA 46000 ⁸⁷⁷⁶ SECUNIA 46125 ⁸⁷⁷⁷ SECUNIA 46126 ⁸⁷⁷⁸ XF 69396 ⁸⁷⁷⁹ URL1 ⁸⁷⁸⁰ URL2 ⁸⁷⁸¹	Kritičan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.20 Ažurirati na Apache HTTPD version 2.2.20 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.20.tar.gz
33.	Apache HTTPD: insecure LD_LIBRARY_PATH handling (CVE-2012-0883) (apache-httpd-cve-2012-0883)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Otkrivena je nebezbedna obrada rute LD_LIBRARY_PATH koja bi mogla da dovede do toga da direktorijum koji trenutno radi traži DSO-ove. Ovo bi lokalnom korisniku omogućilo da izvrši kôd kao root ako je administrator pokrenuo apachectl sa	APPLE APPLE-SA-2013-09-12-1 ⁸⁷⁸² CVE CVE-2012-0883 ⁸⁷⁸³ SECUNIA 48849 ⁸⁷⁸⁴ URL1 ⁸⁷⁸⁵ URL2 ⁸⁷⁸⁶	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.23 Ažurirati na Apache HTTPD version 2.2.23 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz Apache HTTPD >= 2.4 and < 2.4.2 Ažurirati na Apache

⁸⁷⁵⁹ <http://lists.apple.com/archives/Security-announce/2011/Oct/msg00003.html>⁸⁷⁶⁰ <http://www.securityfocus.com/bid/49303>⁸⁷⁶¹ <http://www.kb.cert.org/vuls/id/405811>⁸⁷⁶² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3192>⁸⁷⁶³ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁷⁶⁴ <http://www.osvdb.org/74721>⁸⁷⁶⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14762>⁸⁷⁶⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14824>⁸⁷⁶⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18827>⁸⁷⁶⁸ <http://rhn.redhat.com/errata/RHSA-2011-1245.html>⁸⁷⁶⁹ <http://rhn.redhat.com/errata/RHSA-2011-1294.html>⁸⁷⁷⁰ <http://rhn.redhat.com/errata/RHSA-2011-1300.html>⁸⁷⁷¹ <http://rhn.redhat.com/errata/RHSA-2011-1329.html>⁸⁷⁷² <http://rhn.redhat.com/errata/RHSA-2011-1330.html>⁸⁷⁷³ <http://rhn.redhat.com/errata/RHSA-2011-1369.html>⁸⁷⁷⁴ <http://secunia.com/advisories/45606/>⁸⁷⁷⁵ <http://secunia.com/advisories/45937/>⁸⁷⁷⁶ <http://secunia.com/advisories/46000/>⁸⁷⁷⁷ <http://secunia.com/advisories/46125/>⁸⁷⁷⁸ <http://secunia.com/advisories/46126/>⁸⁷⁷⁹ <http://xforce.iss.net/xforce/xfdb/69396>⁸⁷⁸⁰ http://httpd.apache.org/security/vulnerabilities_22.html⁸⁷⁸¹ http://httpd.apache.org/security/vulnerabilities_20.html⁸⁷⁸² <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁸⁷⁸³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0883>⁸⁷⁸⁴ <http://secunia.com/advisories/48849/>⁸⁷⁸⁵ http://httpd.apache.org/security/vulnerabilities_22.html⁸⁷⁸⁶ http://httpd.apache.org/security/vulnerabilities_24.html

		nepoverljivog direktorijuma.			HTTPD version 2.4.2 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.2.tar.gz
34.	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368) (apache-httpd-cve-2011-3368)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja prisustva mod_proxy modula. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy. Zlonamerni napadač bi mogao da iskoristi ovaj propust na takav način da primora proxy proces da se poveže sa proizvoljnim serverom i potencijalno objavi osetljive informacije sa internih web servera koje inače napadaču nisu direktno dostupne. Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/	APPLE APPLE-SA-2012-09-19-2 ⁸⁷⁸⁷ BID 49957 ⁸⁷⁸⁸ CVE CVE-2011-3368 ⁸⁷⁸⁹ IAVM 2012-A-0017 ⁸⁷⁹⁰ IAVM 2012-A-0152 ⁸⁷⁹¹ IAVM 2012-B-0056 ⁸⁷⁹² OSVDB 76079 ⁸⁷⁹³ REDHAT RHSA-2011:1391 ⁸⁷⁹⁴ REDHAT RHSA-2011:1392 ⁸⁷⁹⁵ SECUNIA 46288 ⁸⁷⁹⁶ SECUNIA 46414 ⁸⁷⁹⁷ SECUNIA 48551 ⁸⁷⁹⁸ XF 70336 ⁸⁷⁹⁹ URL1 ⁸⁸⁰⁰ URL2 ⁸⁸⁰¹ URL3 ⁸⁸⁰²	Ozbiljan	Apache HTTPD >= 1.3 and < 2 Primeniti zakrpu za CVE-2011-3368 to 1.3 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
35.	Apache HTTPD: scoreboard parent DoS (CVE-2012-0031) (apache-httpd-cve-2012-0031)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Propust je otkriven u obradi scoreboard-a. Neprivilegovani child proces bi mogao da dovede do toga da parent proces krahira prilikom gašenja.	APPLE APPLE-SA-2012-09-19-2 ⁸⁸⁰³ BID 51407 ⁸⁸⁰⁴ CVE CVE-2012-0031 ⁸⁸⁰⁵ IAVM 2012-A-0017 ⁸⁸⁰⁶ REDHAT RHSA-2012:0128 ⁸⁸⁰⁷ SECUNIA 47410 ⁸⁸⁰⁸ SECUNIA 48551 ⁸⁸⁰⁹ URL1 ⁸⁸¹⁰	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22

⁸⁷⁸⁷ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁸⁷⁸⁸ <http://www.securityfocus.com/bid/49957>⁸⁷⁸⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3368>⁸⁷⁹⁰ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁷⁹¹ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁷⁹² <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁷⁹³ <http://www.osvdb.org/76079>⁸⁷⁹⁴ <http://rhn.redhat.com/errata/RHSA-2011-1391.html>⁸⁷⁹⁵ <http://rhn.redhat.com/errata/RHSA-2011-1392.html>⁸⁷⁹⁶ <http://secunia.com/advisories/46288/>⁸⁷⁹⁷ <http://secunia.com/advisories/46414/>⁸⁷⁹⁸ <http://secunia.com/advisories/48551/>⁸⁷⁹⁹ <http://xforce.iss.net/xforce/xfdb/70336>⁸⁸⁰⁰ http://httpd.apache.org/security/vulnerabilities_13.html⁸⁸⁰¹ http://httpd.apache.org/security/vulnerabilities_20.html⁸⁸⁰² http://httpd.apache.org/security/vulnerabilities_22.html⁸⁸⁰³ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁸⁸⁰⁴ <http://www.securityfocus.com/bid/51407>⁸⁸⁰⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0031>⁸⁸⁰⁶ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁸⁰⁷ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁸⁸⁰⁸ <http://secunia.com/advisories/47410/>⁸⁸⁰⁹ <http://secunia.com/advisories/48551/>

			URL ⁸⁸¹¹		Ažurirati na Apache HTTPD version 2.2.22 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
36.	Apache HTTPD: mod_proxy_ajp remote DoS (CVE-2012-4557) (apache-httpd-cve-2012-4557)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_proxy_ajp. Review your web server configuration for validation. A flaw was found when mod_proxy_ajp connects to a backend server that takes too long to respond. Given a specific configuration, a remote attacker could send certain requests, putting a backend server into an error state until the retry timeout expired. This could lead to a temporary denial of service.	CVE CVE-2012-4557 ⁸⁸¹² DEBIAN DSA-2579 ⁸⁸¹³ URL ⁸⁸¹⁴	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.22 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
37.	Apache HTTPD: mod_rewrite log escape filtering (CVE-2013-1862) (apache-httpd-cve-2013-1862)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_rewrite. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Modul mod_rewrite ne filtrira završne izlazne sekvence iz logova, što zlonamenrom napadaču olakšava da ubace takve sekvence u završne emulatore koji sadrže ranjivosti koje se odnose na izlazne sekvence.	CVE CVE-2013-1862 ⁸⁸¹⁵ OVAL OVAL18790 ⁸⁸¹⁶ REDHAT RHSA-2013:0815 ⁸⁸¹⁷ REDHAT RHSA-2013:1207 ⁸⁸¹⁸ REDHAT RHSA-2013:1208 ⁸⁸¹⁹ REDHAT RHSA-2013:1209 ⁸⁸²⁰ SECUNIA 55032 ⁸⁸²¹ URL ⁸⁸²² URL ⁸⁸²³	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.25 Ažurirati na Apache HTTPD version 2.2.25 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.25.tar.gz
38.	Apache HTTPD: mod_proxy_ajp remote DoS (CVE-2011-3348) (apache-httpd-cve-2011-3348)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Skenirani servis je osjetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ajp. Proveriti konfiguraciju web servera	APPLE APPLE-SA-2012-02-01-1 ⁸⁸²⁴ BID 49616 ⁸⁸²⁵ CVE CVE-2011-3348 ⁸⁸²⁶ IAVM 2012-B-0056 ⁸⁸²⁷ OVAL OVAL14941 ⁸⁸²⁸ OVAL OVAL18154 ⁸⁸²⁹ REDHAT RHSA-	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.21 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.21.tar.gz

⁸⁸¹⁰ http://httpd.apache.org/security/vulnerabilities_20.html⁸⁸¹¹ http://httpd.apache.org/security/vulnerabilities_22.html⁸⁸¹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4557>⁸⁸¹³ <http://www.debian.org/security/2012/dsa-2579>⁸⁸¹⁴ http://httpd.apache.org/security/vulnerabilities_22.html⁸⁸¹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1862>⁸⁸¹⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18790>⁸⁸¹⁷ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁸⁸¹⁸ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁸⁸¹⁹ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁸⁸²⁰ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁸⁸²¹ <http://secunia.com/advisories/55032/>⁸⁸²² http://httpd.apache.org/security/vulnerabilities_20.html⁸⁸²³ http://httpd.apache.org/security/vulnerabilities_22.html⁸⁸²⁴ <http://lists.apple.com/archives/security-announce/2012/Feb/msg00000.html>⁸⁸²⁵ <http://www.securityfocus.com/bid/49616>⁸⁸²⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3348>⁸⁸²⁷ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁸²⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14941>⁸⁸²⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18154>

		radi utvrđivanja ove mogućnosti. Propust je otkriven kada se mod_proxy_ajp koristi zajedno sa mod_proxy_balancer. Sa specifičnom konfiguracijom, udaljeni napadač može da pošalje zlonameran HTTP zahtev, prouzrokujući da backend server bude stavljen u status greške dok ne istekne vreme za ponovni pokušaj. To bi dovelo do odbijanja servisa.	2011:1391 ⁸⁸³⁰ SECUNIA 46013 ⁸⁸³¹ XF 69804 ⁸⁸³² URL1 ⁸⁸³³		
39.	Apache HTTPD: mod_setenvif .htaccess privilege escalation (CVE-2011-3607) (apache-httpd-cve-2011-3607)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_setenvif. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust preopterećenja je otkriven kada je omogućen modul mod_setenvif, što lokalnim korisnicima omogućava da dobiju privilegije preko fajla .htaccess.	APPLE APPLE-SA-2012-09-19-2 ⁸⁸³⁴ BID 50494 ⁸⁸³⁵ CVE CVE-2011-3607 ⁸⁸³⁶ IAVM 2012-A-0017 ⁸⁸³⁷ IAVM 2012-A-0152 ⁸⁸³⁸ OSVDB 76744 REDHAT RHSA-2012:0128 ⁸⁸³⁹ SECUNIA 45793 ⁸⁸⁴⁰ SECUNIA 48551 ⁸⁸⁴¹ XF 71093 ⁸⁸⁴² URL1 ⁸⁸⁴³ URL2 ⁸⁸⁴⁴	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
40.	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-4317) (apache-httpd-cve-2011-4317)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Skenirani servis je osetljiv na ovu ranjivost samo ako je pokrenut modul mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy U određenim konfiguracijama koje koriste RewriteRule sa proxy flag-om ili ProxyPassMatch, udaljeni napadač bi mogao da primora reverzni proksi da se poveže sa proizvoljnim serverom i potencijalno objavi osetljive informacije sa internih web servera koje inače napadaču nisu direktno dostupne.	APPLE APPLE-SA-2012-09-19-2 ⁸⁸⁴⁵ CVE CVE-2011-4317 ⁸⁸⁴⁶ IAVM 2012-A-0017 ⁸⁸⁴⁷ IAVM 2012-A-0152 ⁸⁸⁴⁸ REDHAT RHSA-2012:0128 ⁸⁸⁴⁹ SECUNIA 48551 ⁸⁸⁵⁰ URL1 ⁸⁸⁵¹	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz

⁸⁸³⁰ <http://rhn.redhat.com/errata/RHSA-2011-1391.html>⁸⁸³¹ <http://secunia.com/advisories/46013/>⁸⁸³² <http://xforce.iss.net/xforce/xfdb/69804>⁸⁸³³ http://httpd.apache.org/security/vulnerabilities_22.html⁸⁸³⁴ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁸⁸³⁵ <http://www.securityfocus.com/bid/50494>⁸⁸³⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3607>⁸⁸³⁷ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁸³⁸ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁸³⁹ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁸⁸⁴⁰ <http://secunia.com/advisories/45793/>⁸⁸⁴¹ <http://secunia.com/advisories/48551/>⁸⁸⁴² <http://xforce.iss.net/xforce/xfdb/71093>⁸⁸⁴³ http://httpd.apache.org/security/vulnerabilities_20.html⁸⁸⁴⁴ http://httpd.apache.org/security/vulnerabilities_22.html⁸⁸⁴⁵ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁸⁸⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4317>⁸⁸⁴⁷ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁸⁴⁸ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁸⁴⁹ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁸⁸⁵⁰ <http://secunia.com/advisories/48551/>⁸⁸⁵¹ http://httpd.apache.org/security/vulnerabilities_22.html

41.	Apache HTTPD: error responses can expose cookies (CVE-2012-0053) (apache-httpd-cve-2012-0053)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Propust je otkriven u difoltnom pogrešnom odgovoru za statusni kôd 400. Zlonamerni napadač bi mogao da iskoristi ovaj propust da objavi "httpOnly" kolačiće ako nije određen dokument custom ErrorDocument.	APPLE APPLE-SA-2012-09-19-2 ⁸⁸⁵² BID 51706 ⁸⁸⁵³ CVE CVE-2012-0053 ⁸⁸⁵⁴ IAVM 2012-A-0017 ⁸⁸⁵⁵ REDHAT RHSA-2012-0128 ⁸⁸⁵⁶ SECUNIA 48551 ⁸⁸⁵⁷ URL1 ⁸⁸⁵⁸ URL2 ⁸⁸⁵⁹	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
42.	Apache HTTPD: XSS due to unescaped hostnames (CVE-2012-3499) (apache-httpd-cve-2012-3499)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut jedan od sledećih modula: mod_imagemap, mod_info, mod_ldap, mod_proxy_ftp, mod_status. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Različiti XSS propusti usled nenapuštenih host imena i URI-ja HTML output-a u mod_info, mod_status, mod_imagemap, mod_ldap i mod_proxy_ftp.	APPLE APPLE-SA-2013-09-12-1 ⁸⁸⁶⁰ CVE CVE-2012-3499 ⁸⁸⁶¹ DEBIAN DSA-2637 ⁸⁸⁶² REDHAT RHSA-2013-0815 ⁸⁸⁶³ REDHAT RHSA-2013-1207 ⁸⁸⁶⁴ REDHAT RHSA-2013-1208 ⁸⁸⁶⁵ REDHAT RHSA-2013-1209 ⁸⁸⁶⁶ SECUNIA 55032 ⁸⁸⁶⁷ URL1 ⁸⁸⁶⁸ URL2 ⁸⁸⁶⁹	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.24 Upgrade to Apache HTTPD version 2.2.24 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz Apache HTTPD >= 2.4 and < 2.4.4 Upgrade to Apache HTTPD version 2.4.4 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz
43.	Apache HTTPD: XSS in mod_proxy_balancer (CVE-2012-4558) (apache-httpd-cve-2012-4558)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy_balancer. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. XSS propust je uticao na manager interfejs mod_proxy_balancer-a.	APPLE APPLE-SA-2013-09-12-1 ⁸⁸⁷⁰ CVE CVE-2012-4558 ⁸⁸⁷¹ DEBIAN DSA-2637 ⁸⁸⁷² REDHAT RHSA-2013-0815 ⁸⁸⁷³ REDHAT RHSA-2013-1207 ⁸⁸⁷⁴ REDHAT RHSA-2013-1208 ⁸⁸⁷⁵ REDHAT RHSA-2013-1209 ⁸⁸⁷⁶	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.24 Ažurirati na Apache HTTPD version 2.2.24 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz Apache HTTPD >= 2.4 and < 2.4.4 Ažurirati na Apache HTTPD version 2.4.4

⁸⁸⁵² <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁸⁸⁵³ <http://www.securityfocus.com/bid/51706>⁸⁸⁵⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0053>⁸⁸⁵⁵ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁸⁵⁶ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁸⁸⁵⁷ <http://secunia.com/advisories/48551/>⁸⁸⁵⁸ http://httpd.apache.org/security/vulnerabilities_20.html⁸⁸⁵⁹ http://httpd.apache.org/security/vulnerabilities_22.html⁸⁸⁶⁰ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁸⁸⁶¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3499>⁸⁸⁶² <http://www.debian.org/security/2013/dsa-2637>⁸⁸⁶³ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁸⁸⁶⁴ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁸⁸⁶⁵ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁸⁸⁶⁶ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁸⁸⁶⁷ <http://secunia.com/advisories/55032/>⁸⁸⁶⁸ http://httpd.apache.org/security/vulnerabilities_22.html⁸⁸⁶⁹ http://httpd.apache.org/security/vulnerabilities_24.html⁸⁸⁷⁰ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁸⁸⁷¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4558>⁸⁸⁷² <http://www.debian.org/security/2013/dsa-2637>⁸⁸⁷³ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁸⁸⁷⁴ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁸⁸⁷⁵ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁸⁸⁷⁶ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>

			URL1 ⁸⁸⁷⁷ URL2 ⁸⁸⁷⁸		Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz
44.	Apache HTTPD: XSS in mod_negotiation when untrusted uploads are supported (CVE-2012-2687) (apachehttpd-cve-2012-2687)	172.23.202.133:80 172.23.202.132:80 172.23.202.123:80 172.23.202.229:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_negotiation. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Moguće je ubaciti CRLF (Carriage Return and Line Feed) koji omogućava CRLF Injection napade (poznatih i kao HTTP Response Splitting) za sajtove koji koriste mod_negotiation, omogućavajući neproverene upload-ove na lokacije na kojima je omogućen MultiViews (višestruko pregledanje). Ovaj problem je poznat i kao CVE-2008-0455.	APPLE APPLE-SA-2013-09-12-1 ⁸⁸⁷⁹ BID 55131 ⁸⁸⁸⁰ CVE CVE-2012-2687 ⁸⁸⁸¹ IAVM 2012-A-0139 ⁸⁸⁸² REDHAT RHSA-2012:1591 ⁸⁸⁸³ REDHAT RHSA-2012:1592 ⁸⁸⁸⁴ REDHAT RHSA-2012:1594 ⁸⁸⁸⁵ REDHAT RHSA-2013:0130 ⁸⁸⁸⁶ SECUNIA 50894 ⁸⁸⁸⁷ SECUNIA 51607 ⁸⁸⁸⁸ URL1 ⁸⁸⁸⁹ URL2 ⁸⁸⁹⁰	Umeren	Apache HTTPD >= 2.2 and < 2.2.23 Ažurirati na Apache HTTPD version 2.2.23 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz Apache HTTPD >= 2.4 and < 2.4.3 Ažurirati na Apache HTTPD version 2.4.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.3.tar.gz

Tabela 130. Linux OS sa IP adresom 172.23.202.197 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.197		OS: Debian 60 x86, debian60x86			39
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Anonymous users can obtain the Windows password policy (cifs-nt-0002)	Korišćenjem CIFS NULL sesije, anonimni korisnik može da dobije uvid u polisu šifri. Polisa šifri sadrži osetljive informacije o najmanjoj mogućoj dužini lozinke, zaključavanje šifre, vremensko trajanje zaključanosti šifre itd.	SANS-01 W5 ⁸⁸⁹¹ CVE CVE-2000-1200 ⁸⁸⁹² XF nt-lsa-domain-sid(4015) ⁸⁸⁹³ SANS-02 W5 ⁸⁸⁹⁴ BID 959 ⁸⁸⁹⁵ SANS-04 W3 ⁸⁸⁹⁶ SANS-03 W5 ⁸⁸⁹⁷ BID 87 ⁸⁸⁹⁸	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost.

⁸⁸⁷⁷ http://httpd.apache.org/security/vulnerabilities_22.html⁸⁸⁷⁸ http://httpd.apache.org/security/vulnerabilities_24.html⁸⁸⁷⁹ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁸⁸⁸⁰ <http://www.securityfocus.com/bid/55131>⁸⁸⁸¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2687>⁸⁸⁸² <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁸⁸³ <http://rhn.redhat.com/errata/RHSA-2012-1591.html>⁸⁸⁸⁴ <http://rhn.redhat.com/errata/RHSA-2012-1592.html>⁸⁸⁸⁵ <http://rhn.redhat.com/errata/RHSA-2012-1594.html>⁸⁸⁸⁶ <http://rhn.redhat.com/errata/RHSA-2013-0130.html>⁸⁸⁸⁷ <http://secunia.com/advisories/50894/>⁸⁸⁸⁸ <http://secunia.com/advisories/51607/>⁸⁸⁸⁹ http://httpd.apache.org/security/vulnerabilities_22.html⁸⁸⁹⁰ http://httpd.apache.org/security/vulnerabilities_24.html⁸⁸⁹¹ <http://www.sans.org/critical-security-controls/#w5>⁸⁸⁹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2000-1200>⁸⁸⁹³ <http://xforce.iss.net/xforce/xfdb/4015>⁸⁸⁹⁴ <http://www.sans.org/critical-security-controls/#w5>⁸⁸⁹⁵ <http://www.securityfocus.com/bid/959>⁸⁸⁹⁶ <http://www.sans.org/critical-security-controls/#w3>⁸⁸⁹⁷ <http://www.sans.org/critical-security-controls/#w5>⁸⁸⁹⁸ <http://www.securityfocus.com/bid/87>

2.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.197:139 172.23.202.197:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje dozvoljava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB 887429 URL1 ⁸⁸⁹⁹	Ozbiljan	Metoda za konfiguracije SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429. ⁸⁹⁰⁰ Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (na konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: <i>server signing</i> = <i>auto</i> ili da se zahteva SMB potpisivanje: <i>server signing</i> = <i>mandatory</i> .
3.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.197:139 172.23.202.197:445 Sistem omogućava, ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti.
4.	Apache HTTPD: expat DoS (CVE-2009-3560) (apache-httpd-cve-2009-3560)	172.23.202.197:80 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u mogućnosti da dovede do toga da Apache parsira nepoverljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	BID 37203 ⁸⁹⁰¹ CVE CVE-2009-3560 ⁸⁹⁰² DEBIAN DSA-1953 ⁸⁹⁰³ IAVM 2012-A-0020 ⁸⁹⁰⁴ OVAL OVAL12942 ⁸⁹⁰⁵ REDHAT RHSA-2011:0896 ⁸⁹⁰⁶ OVAL OVAL10613 ⁸⁹⁰⁷ OVAL OVAL6883 ⁸⁹⁰⁸ SECUNIA 37537 ⁸⁹⁰⁹ SECUNIA 38231 ⁸⁹¹⁰ SECUNIA 38794 ⁸⁹¹¹ SECUNIA 38832 ⁸⁹¹² SECUNIA 38834 ⁸⁹¹³ SECUNIA 39478 ⁸⁹¹⁴ SECUNIA 41701 ⁸⁹¹⁵ SECUNIA 43300 ⁸⁹¹⁶ URL1 ⁸⁹¹⁷	Ozbiljan	Apache >= 2.0 and < 2.1 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.17 Ažurirati na Apache HTTPD version 2.2.17 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
5.	Apache HTTPD: expat DoS (CVE-2009-3720) (apache-httpd-cve-2009-3720)	172.23.202.197:80 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u mogućnosti da dovede do toga da Apache parsira nepoverljiv XML dokument.	AVM 2012-A-0020 ⁸⁹¹⁸ OVAL OVAL12719 ⁸⁹¹⁹ REDHAT RHSA-2011:0896 ⁸⁹²⁰ CVE CVE-2009-3720 ⁸⁹²¹ OVAL OVAL11019 ⁸⁹²²	Ozbiljan	Apache >= 2.0 and < 2.1 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and

⁸⁸⁹⁹ <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>⁸⁹⁰⁰ <http://support.microsoft.com/kb/887429>⁸⁹⁰¹ <http://www.securityfocus.com/bid/37203>⁸⁹⁰² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3560>⁸⁹⁰³ <http://www.debian.org/security/DSA-1953> pristupljeno dana 18.12.2011⁸⁹⁰⁴ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁹⁰⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12942>⁸⁹⁰⁶ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁸⁹⁰⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10613>⁸⁹⁰⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6883>⁸⁹⁰⁹ <http://secunia.com/advisories/37537/>⁸⁹¹⁰ <http://secunia.com/advisories/38231/>⁸⁹¹¹ <http://secunia.com/advisories/38794/>⁸⁹¹² <http://secunia.com/advisories/38832/>⁸⁹¹³ <http://secunia.com/advisories/38834/>⁸⁹¹⁴ <http://secunia.com/advisories/39478/>⁸⁹¹⁵ <http://secunia.com/advisories/41701/>⁸⁹¹⁶ <http://secunia.com/advisories/43300/>⁸⁹¹⁷ http://httpd.apache.org/security/vulnerabilities_20.html⁸⁹¹⁸ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁹¹⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12719>⁸⁹²⁰ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁸⁹²¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3720>

		Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	OVAL OVAL7112 ⁸⁹²³ REDHAT RHSA-2010:0002 ⁸⁹²⁴ SECUNIA 37324 ⁸⁹²⁵ SECUNIA 37537 ⁸⁹²⁶ SECUNIA 37925 ⁸⁹²⁷ SECUNIA 38050 ⁸⁹²⁸ SECUNIA 38231 ⁸⁹²⁹ SECUNIA 38794 ⁸⁹³⁰ SECUNIA 38832 ⁸⁹³¹ SECUNIA 38834 ⁸⁹³² SECUNIA 39478 ⁸⁹³³ SECUNIA 41701 ⁸⁹³⁴ SECUNIA 43300 ⁸⁹³⁵ URL1 ⁸⁹³⁶		< 2.2.17 Upgrade to Apache HTTPD version 2.2.17 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
6.	Apache HTTPD: apr_bridage_split_line DoS (CVE-2010-1623) (apache-httpd-cve-2010-1623)	172.23.202. 197:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako Apache procesira ne-SSL zahteve. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_brigrade_split_line() u sklopu kompleta APR-util library, koji se koristi za procesiranje ne-SSL zahteva. Udaljeni napadač bi mogao da šalje zahteve, pažljivo izrađujući tajming za pojedinačne bajtove, što bi polako zauzimalo memoriju i potencijalno dovelo do odbijanja servisa.	IAVM 2012-B-0056 ⁸⁹³⁷ OVAL OVAL12800 ⁸⁹³⁸ REDHAT RHSA-2011:0896 ⁸⁹³⁹ REDHAT RHSA-2011:0897 ⁸⁹⁴⁰ BID 43673 ⁸⁹⁴¹ CVE CVE-2010-1623 ⁸⁹⁴² REDHAT RHSA-2010:0950 ⁸⁹⁴³ SECUNIA 41701 ⁸⁹⁴⁴ SECUNIA 42015 ⁸⁹⁴⁵ SECUNIA 42361 ⁸⁹⁴⁶ SECUNIA 42367 ⁸⁹⁴⁷ SECUNIA 42403 ⁸⁹⁴⁸ SECUNIA 42537 ⁸⁹⁴⁹ SECUNIA 43211 ⁸⁹⁵⁰ SECUNIA 43285 ⁸⁹⁵¹ URL1 ⁸⁹⁵²	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.17 Azurirati na Apache HTTPD version 2.2.17 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
7.	X.509 Certificate Subject CN Does Not	172.23.202. 197:993 Rubrika u sertifikatu X.509 sa		Ozbiljan	Rubrika sa uobičajenim nazivom subjekta (CN) u sertifikatu X.509 treba da

⁸⁹²² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11019>⁸⁹²³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7112>⁸⁹²⁴ <http://rhn.redhat.com/errata/RHSA-2010-0002.html>⁸⁹²⁵ <http://secunia.com/advisories/37324/>⁸⁹²⁶ <http://secunia.com/advisories/37537/>⁸⁹²⁷ <http://secunia.com/advisories/37925/>⁸⁹²⁸ <http://secunia.com/advisories/38050/>⁸⁹²⁹ <http://secunia.com/advisories/38231/>⁸⁹³⁰ <http://secunia.com/advisories/38794/>⁸⁹³¹ <http://secunia.com/advisories/38832/>⁸⁹³² <http://secunia.com/advisories/38834/>⁸⁹³³ <http://secunia.com/advisories/39478/>⁸⁹³⁴ <http://secunia.com/advisories/41701/>⁸⁹³⁵ <http://secunia.com/advisories/43300/>⁸⁹³⁶ http://httpd.apache.org/security/vulnerabilities_20.html⁸⁹³⁷ <http://iase.disa.mil/stigs/iavm-cve.html>⁸⁹³⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12800>⁸⁹³⁹ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁸⁹⁴⁰ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>⁸⁹⁴¹ <http://www.securityfocus.com/bid/43673>⁸⁹⁴² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1623>⁸⁹⁴³ <http://rhn.redhat.com/errata/RHSA-2010-0950.html>⁸⁹⁴⁴ <http://secunia.com/advisories/41701/>⁸⁹⁴⁵ <http://secunia.com/advisories/42015/>⁸⁹⁴⁶ <http://secunia.com/advisories/42361/>⁸⁹⁴⁷ <http://secunia.com/advisories/42367/>⁸⁹⁴⁸ <http://secunia.com/advisories/42403/>⁸⁹⁴⁹ <http://secunia.com/advisories/42537/>⁸⁹⁵⁰ <http://secunia.com/advisories/43211/>⁸⁹⁵¹ <http://secunia.com/advisories/43285/>⁸⁹⁵² http://httpd.apache.org/security/vulnerabilities_20.html

	Match the Entity Name (certificate-common-name-mismatch)	uobičajenim nazivom subjekta (CN) ne poklapa se sa imenom pojedinca koje je navedeno u sertifikatu. Pre izdavanja sertifikata, Certification Authority (CA) mora da proveriti identitet pojedinca koji potražuje sertifikat, kako je navedeno u CA-ovom Certification Practice Statement (CPS). Zbog toga, uobičajene procedure validacije sertifikata zahtevaju da rubrika sertifikata sa CN subjektom odgovara pravom imenu pojedinca koji prikazuje sertifikat. Na primer, u sertifikatu prikazanom na „https://www.example.com/“, naziv subjekta (CN) treba da bude „www.example.com“. U cilju otkrivanja i sprečavanja napada prisluškivanja, validnost sertifikata mora da bude overena, jer bi u suprotnom napadač mogao da otpočne napad preko posrednika i da stekne potpunu kontrolu nad protokom podataka. Od posebne važnosti je validnost naziva subjekta (CN), koji treba da se poklapa sa imenom pojedinca (imenom host-a). Neodgovarajući CN se najčešće javlja usled greške u konfiguraciji, iako on takođe može da ukazuje na to da se sprovodi napad preko posrednika.			bude podešena da sadrži ime pojedinca koji prikazuje sertifikat (npr. ime hosta). To se postiže izradom novog sertifikata, koji najčešće potpisuje Certification Authority (CA), koji je od poverenja kako za klijenta, tako i za server.
8.	FTP access with ftp account (ftp-generic-0001)	172.23.202. 197:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisničkim ID-jem „ftp“ i šifrom „ftp“. Dosadašnja praksa je pokazala da treba ukloniti difoltnu naloge, ako je to moguće. Za naloge koje zahteva sistem, treba promeniti difoltnu šifru.	CVE CVE-1999-0497 ⁸⁹⁵³	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko to nije kritično za dalje funkcionisanje sistema. U suprotnom, treba promeniti lozinku u nedifoltnu vrednost.
9.	FTP access with anonymous account (ftp-generic-0002)	172.23.202. 197:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisničkim ID-jem „anonymous“ i šifrom „ftp@“. Dosadašnja praksa je pokazala da treba ukloniti difoltnu naloge, ako je to moguće. Za naloge koje zahteva sistem, treba promeniti difoltnu šifru.	CVE CVE-1999-0497 ⁸⁹⁵⁴	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko to nije kritično za dalje funkcionisanje sistema. U suprotnom, treba promeniti lozinku u nedifoltnu vrednost.
10.	FTP server does not support AUTH command (ftp-generic-0007)	172.23.202. 197:21 FTP klijenti po difoltu šalju FTP server-u poverljive podatke (korisnički ID i šifra) u vidu čitkog teksta. Ova okolnost dozvoljava zlonamernim korisnicima da presreću poverljive podatke ukoliko prisluškuju vezu. Noviji FTP serveri podržavaju AUTH komandu, koja omogućava dodatne opcije autentifikacije, kao što su TLS, Kerberos, GSSAPI itd. Ona se može koristiti za sprečavanje prisluškivanja na FTP vezama.		Ozbiljan	Ažurirati/preći na FTP server koji podržava AUTH komandu.

⁸⁹⁵³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>⁸⁹⁵⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>

11.	Browsable web directory (http-generic-browsable-dir)	172.23.202. 197:80 Otkriven je direktorijum na web serveru koji može biti pretraživan, što znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice - spajdering (prateći hiperlinkove), ili -kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute force napadom na liste uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skrivenne“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice. Primer: <pre> http://172.23.202. 197/icons/small/ 4: <title>Index of /icons/small</title> 5: </head> 6: <body> 7: <h1>Index of /icons/small</h1> 8: ...COJ“<th><th>Name</th><th><a href=“?C=M;O=A... </pre>		Ozbiljan	Za Apache: onemogućiti pretraživanje direktorijuma mreže za sve direktorijume i poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume. Za Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote: Onemogućiti pretraživanje direktorijuma za sve direktorijume i poddirektorijume. Uključiti Tomcat-ov web.xml file. U odeljku „default“, promeniti parametar „listings“ iz „true“ u „false“. Restartovati server. Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skriptu i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume.
12.	TLS/SSL Server Supports Weak Cipher Algorithms (ssl-weak-ciphers)	172.23.202. 197:993 negotiated the SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA cipher suite TLS/SSL server podržava šifre koje se zasnivaju na slabim algoritmima. To napadaču može omogućiti da pokrene napade preko posrednika i da pregleda ili čačka osetljive podatke. Uopšteno, sledeće šifre se smatraju slabim: Tzv. „null“ (nula) šifre, jer ne šifruju podatke.		Ozbiljan	Konfigurisati server tako da onemogući podršku za slabe šifre. Za Apache web servere sa mod_ssl, uključiti fajl Apache konfiguracije i izmeniti liniju SSLCipherSuite tako da u njoj piše: SSLCipherSuite ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM

		Eksportne šifre koje koriste dužine tajnih ključeva ograničene na 40 bitova. Na to najčešće ukazuje reč EXP/EXPORT u nazivu šifre. Zastareli algoritmi za šifrovanje čije se dužine tajnih ključeva po današnjim standardima smatraju kratkim, npr. DES ili RC4 sa 56-bitnim ključevima.			
13.	TLS/SSL Server Supports SSLv2 (ssl2-and-up-enabled)	172.23.202. 197:993 Iako server prihvata klijente koji koriste TLS ili SSLv3, on takođe prihvata klijente koji koriste SSLv2. SSLv2 je starija implementacija Secure Sockets Layer protokola. Ima veliki broj bezbednosnih propusta koji omogućavaju zlonamenrim napadačima da preuzmu i menjaju informacije koje razmenjuju klijent i server, uključujući i slabosti koje se odnose na posredne napade (eng. man in the middle) tokom handshake postupka. Eksportovani setovi šifara nepotrebno oslabljuju MAC-ove. Istovetni kriptografski ključevi se koriste za autentifikaciju poruke i kriptovanje. S obzirom da je ranjiv na napade koji uzrokuju falsifikovanje i odsecanje TCP FIN paketa, SSLv2 je postao nepoželjan i više se ne preporučuje. Ni SSLv2, ni SSLv3 ne odgovaraju U.S. FIPS 140-2 standardima, koji važe u kriptografskim modulima u upotrebi unutar federalnih informacionih sistema. Samo noviji TLS (Transport Layer Security) protokol odgovara FIPS 140-2 zahtevima. Osim toga, isključivo prisustvo SSLv2-a se smatra greškom od strane PCI-a (Payment Card Industry) Data Security Standard. Ova ranjivost će biti prijavljena ako udaljeni server podržava SSLv2, ne uzimajući u obzir da se takođe podržavaju TLS ili SSLv3.	URL1 ⁸⁹⁵⁵ URL2 ⁸⁹⁵⁶	Ozbiljan	Konfigurisati server tako da se od klijenta zahteva upotreba najmanje SSLv3 ili TLS. Kada je reč o Microsoft IIS web serverima konsultovati Microsoft Knowledgebase odeljak Q187498 za instrukcije koje se odnose na onemogućavanje SSL 2.0. Za Apache web servere sa omogućenim mod_ssl, izmeniti Apache konfiguracioni fajl da za sekciju SSLCipherSuite piše: SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:!SSLv2 Znak ! (znak uzvika) ispred SSLv2 je ono što onemogućava ovaj protokol.
14.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	TCP reset with incorrect sequence number triggered this fault on 172.23.202. 197:993 Kada se kod TCP paketa koristi Large Window Size, olakšava se spolnom napadaču da otkrije sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji	OSVDB 4030 ⁸⁹⁵⁷ BID: 10183 ⁸⁹⁵⁸ CERT-VN: 415294 ⁸⁹⁵⁹ CVE CVE-2004-0230 ⁸⁹⁶⁰ MS: MS05-019 ⁸⁹⁶¹ MS: MS06-064 ⁸⁹⁶² NETBSD: NetBSD-SA2004-006 ⁸⁹⁶³ OVAL: OVAL2689 ⁸⁹⁶⁴ OVAL: OVAL270 ⁸⁹⁶⁵	Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC 2385 ⁸⁹⁷⁶ . Ono je napravljeno da smanji opasnost od određenih napada na BGP, kao što su TCP reseti.

⁸⁹⁵⁵ https://www.pcisecuritystandards.org/pdfs/pcissc_assessors_nl_2008-11.pdf⁸⁹⁵⁶ www.eucybervote.org/Reports/MSI-WP2-D7V1-V1.0-02.htm pristupljeno 11.12.2011⁸⁹⁵⁷ <http://www.osvdb.org/4030>⁸⁹⁵⁸ <http://www.securityfocus.com/bid/10183>⁸⁹⁵⁹ <http://www.kb.cert.org/vuls/id/415294>⁸⁹⁶⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁸⁹⁶¹ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁸⁹⁶² <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁸⁹⁶³ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁸⁹⁶⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>

		koriste dugotrajne veze, kao npr. BGP.	OVAL OVAL3508⁸⁹⁶⁶ OVAL OVAL4791⁸⁹⁶⁷ OVAL OVAL5711⁸⁹⁶⁸ SECUNIA: 11440⁸⁹⁶⁹ SECUNIA 11458⁸⁹⁷⁰ SECUNIA: 22341⁸⁹⁷¹ SGI 20040403-01-A⁸⁹⁷² XF tcp-rst-dos(15886)⁸⁹⁷³ URL1⁸⁹⁷⁴ URL2⁸⁹⁷⁵		
15.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podesi na jedinstvenu vrednost i da se koristi u rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da fingerprint-uje operativni sistem.	BID 4314⁸⁹⁷⁷ CVE CVE-2002-0510⁸⁹⁷⁸ XF linux-udp-fingerprint(8588)⁸⁹⁷⁹	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili pak ranjivost koju treba popravljati, tako da ne postoje rešenja koja se mogu kupiti. jedino se može postaviti fajervol ili neka druga sprava za filtriranje između napadnutog i neprijateljskog napada koji je u mogućnosti da randomizuje IP ID-jeve.
16.	Apache HTTPD: apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpdcve-2011-0419)	172.23.202.197:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_autoindex. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_fnmatch() u sklopu APR biblioteke. Ako je omogućen mod_autoindex, a indksi direktorijuma mod_autoindex su sadržavali fajlove sa dovoljno dugim nazivima, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do preterane upotrebe CPU-a. Ovo bi moglo da bude iskorišćeno u napadu odbijanja servisa. Zahvaljujući Maksymilian Arciemowicz prijavljen je ovaj	CVE CVE-2011-0419⁸⁹⁸⁰ DEBIAN DSA-2237⁸⁹⁸¹ IAVM 2012-B-0056⁸⁹⁸² OVAL OVAL14638⁸⁹⁸³ OVAL OVAL14804⁸⁹⁸⁴ REDHAT RHSA-2011:0896⁸⁹⁸⁵ REDHAT RHSA-2011:0897⁸⁹⁸⁶ REDHAT RHSA-2011:0507⁸⁹⁸⁷ SECUNIA 44490⁸⁹⁸⁸ SECUNIA 44564⁸⁹⁸⁹ SECUNIA 44574⁸⁹⁹⁰ URL1⁸⁹⁹¹	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.19 Ažurirati na Apache HTTPD version 2.2.19 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.19.tar.gz

⁸⁹⁶⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>
⁸⁹⁷⁶ <http://www.ietf.org/rfc/rfc2385.txt>
⁸⁹⁶⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>
⁸⁹⁶⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>
⁸⁹⁶⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>
⁸⁹⁶⁹ <http://secunia.com/advisories/11440/>
⁸⁹⁷⁰ <http://secunia.com/advisories/11458/>
⁸⁹⁷¹ <http://secunia.com/advisories/22341/>
⁸⁹⁷² <http://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>
⁸⁹⁷³ <http://xforce.iss.net/xforce/xfdb/15886>
⁸⁹⁷⁴ <http://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>
⁸⁹⁷⁵ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>
⁸⁹⁷⁷ <http://www.securityfocus.com/bid/4314>
⁸⁹⁷⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>
⁸⁹⁷⁹ <http://xforce.iss.net/xforce/xfdb/8588>
⁸⁹⁸⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419>
⁸⁹⁸¹ <http://www.debian.org/security/2011/dsa-2237>
⁸⁹⁸² <http://iase.disa.mil/stigs/iavm-cve.html>
⁸⁹⁸³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14638>
⁸⁹⁸⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14804>
⁸⁹⁸⁵ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>
⁸⁹⁸⁶ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>
⁸⁹⁸⁷ <http://rhn.redhat.com/errata/RHSA-2011-0507.html>
⁸⁹⁸⁸ <http://secunia.com/advisories/44490/>
⁸⁹⁸⁹ <http://secunia.com/advisories/44564/>
⁸⁹⁹⁰ <http://secunia.com/advisories/44574/>
⁸⁹⁹¹ http://httpd.apache.org/security/vulnerabilities_22.html

		propust.			
17.	Apache HTTPD: ETag Inode Information Leakage (CVE-2003-1418) (apache-httpd-cve-2003-1418)	172.23.202.197:80 U određenim konfiguracijama, Apache HTTP server dozvoljava udaljenim napadačima da dobiju poverljive informacije preko (1) Etag heder-a, koji otkriva broj inoda ili (2) razdvajajuće višedelnih MIME-a, koja ukazuje na ID child procesa (PID). Određene verzije Apache-a koriste zahtevani broj čvorova fajla da bi konstruisali 'Etag' heder za odgovor. Iako sama po sebi nije ranjivost, ova informacija olakšava sprovođenje određenih NFS napada. „Running vulnerable HTTP service: Apache 2.2.17. http://172.23.202.206/ 1: "c2979-b1-4a76e5063f807"“	BID 6939 ⁸⁹⁹² BID 6943 ⁸⁹⁹³ CVE CVE-2003-1418 ⁸⁹⁹⁴ XF apache-mime-information-disclosure(11438) ⁸⁹⁹⁵	Ozbiljan	Onemogućiti Etag mehanizam tipa "inod-based" konfiguraciji Apache-a. Takođe, inod informacije je moguće ukloniti iz Etag heder-a tako što će se dodati direktiva u Apache konfiguraciju: <i>FileETag Mtime Size</i>
18.	Self-signed TLS/SSL certificate (ssl-self-signed-certificate)	172.23.202. 197:993 TLS/SSL-a sertifikat servera je samopotpisan. Samopotpisani sertifikati po difoltu nisu od poverenja, naročito zato što napadi na TLS/SSL preko posrednika obično koriste samopotpisane sertifikate da prisluškuju TLS/SSL veze.		Ozbiljan	Nabaviti novi TLS/SSL serverov sertifikat koji NIJE samopotpisan i instalirati ga na server. Precizna uputstva za dobijanje novog sertifikata zavise od zahteva organizacije. Uopšteno, treba napraviti zahtev za sertifikat i taj zahtev sačuvati kao fajl. Ovaj fajl se zatim šalje Certificate Authority-ju (CA) na obradu. Organizacija možda poseduje sopstveni interni Certificate Authority. U suprotnom, potrebno je platiti sertifikat iz spoljnog poverljivog Certificate Authority-ja, kao što su Thawte , Verisign .
19.	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server . Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u mogućnosti i da pristupe različitim MSRPC servisima preko poziva udaljenih procedura (RPC). Ovi servisi su i u prošlosti bili skloni ranjivostima.. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinjenije napade. Primer:	BID: 494 ⁸⁹⁹⁶ CVE: CVE-1999-0519 ⁸⁹⁹⁷ MSKB: 143474 ⁸⁹⁹⁸ URL1 ⁸⁹⁹⁹	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost.

⁸⁹⁹² <http://www.securityfocus.com/bid/6939>⁸⁹⁹³ <http://www.securityfocus.com/bid/6943>⁸⁹⁹⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-1418>⁸⁹⁹⁵ <http://xforce.iss.net/xforce/xfdb/11438>⁸⁹⁹⁶ <http://www.securityfocus.com/bid/494>⁸⁹⁹⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519>⁸⁹⁹⁸ <http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474>⁸⁹⁹⁹ http://www.hsc.fr/ressources/presentations/null_sessions/

		Found user(s): nobody root vanja Found server name: UBUNT1104DSKX64 Found local group(s): Found policy for domain(s): UBUNT1104DSKX64 Builtin			
20.	Apache default installation/welcome page installed (http://apache-default-install-page)	172.23.202.197:80 Apache difoltna instalacija ili „Welcome“ stranica je instalirana na serveru. To obično ukazuje na novoinstalirani server. U mnogim slučajevima, Apache se instalira zajedno sa drugim aplikacijama i korisnik možda nije svestan da je web server pokrenut. Ovakvi serveri se retko patch-uju i još ređe nadgledaju, što zlonamernim napadačima postaje pogodna meta koja najverovatnije neće pokrenuti nikakvo upozorenje. Primer : Running vulnerable HTTP service: Apache 2.2.16. http://172.23.202.197/ 1: <html><body> It works!		Umeren	Ako se od servera zahteva da obezbedi neophodnu funkcionalnost, onda difoltnu stranicu treba zameniti odgovarajućim sadržajem. U suprotnom, ovakav server treba ukloniti sa mreže, prateći bezbednosni princip minimalne složenosti (više složenosti = manja bezbednost). Ako server nije potreban, treba ga ukloniti iz svih startup fajlova (npr. /etc/rc*) ili skripti, a zatim prekinuti servis. Proveriti da li se on ponovo pokreće kada se mašina reboot-uje. Apache se uglavnom instalira kao /usr/sbin/httpd na UNIX mašinama ili kao C:\Program Files\Apache Group na Windows mašinama. Razmotriti uklanjanje binara i svih srodnih biblioteka iz sistema.
21.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeci ICMP-ov zahtev za vremenski pečat.	CVE CVE-1999-0524 ⁹⁰⁰⁰ OSVDB 95 ⁹⁰⁰¹ XF icmp-netmask(306) ⁹⁰⁰² XF icmp-timestamp(322) ⁹⁰⁰³	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
22.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1 ⁹⁰⁰⁴ URL2 ⁹⁰⁰⁵ URL3 ⁹⁰⁰⁶	Umeren	Onemogućavanje TCP timestamp odgovora na Linux OS. Podesiti net.ipv4.tcp_timestamps vrednost na sledećem ključu na 0 pokretanjem sledeće komande: sysctl -w net.ipv4.tcp_timestamps=0 Dodatno, sledeću vrednost u difoltnom sysctl konfiguracionom fajlu,

⁹⁰⁰⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁹⁰⁰¹ <http://www.osvdb.org/95>⁹⁰⁰² <http://xforce.iss.net/xforce/xfdb/306>⁹⁰⁰³ <http://xforce.iss.net/xforce/xfdb/322>⁹⁰⁰⁴ http://www.forensicswiki.org/wiki/TCP_timestamps⁹⁰⁰⁵ <http://www.ietf.org/rfc/rfc1323.txt>⁹⁰⁰⁶ <http://uptime.netcraft.com/>

					generally sysctl.conf: net.ipv4.tcp_timestamps=0
23.	Database Open Access (database-open-access)	172.23.202.197:3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7.	URL ⁹⁰⁰⁷	Umeren	Konfigurisati server baze podataka tako da dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.
24.	Samba RPC unauthenticated remote code execution (CVE-2012-1182) (cifs-samba-cve-2012-1182)	172.23.202.197:139 172.23.202.197:445 Određene verzije Samba-e sadrže sigurnosni propust u interfejsu poziva udaljenih procedura (RPC). Posledica ovog propusta je da udaljeni napadač može pokrenuti daljinsko izvršenje koda u sklopu smbd procesa, preko crafted RPC paketa, koji bi doveo do preopetrecenja bafera. Ova ranjivost ne zahteva autentifikovanu vezu da bi pokrenula nove eksploite, a s obzirom da Samba radi kao root, ovo je jedna od najopasnijih ranjivosti.	APPLE APPLE-SA-2012-05-09-1 ⁹⁰⁰⁸ CVE CVE-2012-1182 ⁹⁰⁰⁹ IAVM 2012-A-0085 ⁹⁰¹⁰ SECUNIA 48999 ⁹⁰¹¹ URL ⁹⁰¹²	Kritičan	Uraditi download a zatim instalirati: http://www.samba.org Zakrpljene verzije Samba-e obuhvataju v3.6.4, v3.5.14, i v3.4.16, a puštene su u opticaj 10. aprila 2012. Većina Linux distributera prodaje starije verzije Samba-e, ali poseduje backportovane popravke za bezbednosne propuste (kako od prodavca - Samba-e - tako i od samih distributera). Treba ažurirati dobijenu verziju od distributera preko system package manager-a.
25.	Apache HTTPD: Range header remote DoS (CVE-2011-3192) (apache-httpd-cve-2011-3192)	172.23.202.197:80 Propust je otkriven u načinu na koji Apache HTTP Server obrađuje Range HTTP hedere. Zlonamerni napadač bi mogao da iskoristi ovaj propust i dovede do toga da http koristi veliku količinu memorije i CPU vremena preko HTTP zahteva sa posebno kreiranim Range hederom. Ovo bi moglo dovesti do napada odbijanja servisa. Advisory: CVE-2011-3192.txt	APPLE APPLE-SA-2011-10-12-3 ⁹⁰¹³ BID 49303 ⁹⁰¹⁴ CERT-VN 405811 ⁹⁰¹⁵ CVE CVE-2011-3192 ⁹⁰¹⁶ IAVM 2012-B-0056 ⁹⁰¹⁷ OSVDB 74721 ⁹⁰¹⁸ OVAL OVAL14762 ⁹⁰¹⁹ OVAL OVAL14824 ⁹⁰²⁰ OVAL OVAL18827 ⁹⁰²¹ REDHAT RHSA-2011:1245 ⁹⁰²² REDHAT RHSA-2011:1294 ⁹⁰²³	Kritičan	Mnoge platforme i mnogi distributeri daju unapred formirane binarne pakete za Apache. Ovi unapred formirani paketi su najčešće standardizovani i optimizirani za određenu distribuciju, pa se zato savetuje korišćenje paketa predefinisanih za određeni OS, ukoliko su dostupni. Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache

⁹⁰⁰⁷ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf⁹⁰⁰⁸ <http://lists.apple.com/archives/security-announce/2012/May/msg00001.html>⁹⁰⁰⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1182>⁹⁰¹⁰ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁰¹¹ <http://secunia.com/advisories/48999/>⁹⁰¹² <http://www.mandriva.com/en/support/security/advisories/advisory/MDVSA-2012:055/?name=MDVSA-2012:055>⁹⁰¹³ <http://lists.apple.com/archives/Security-announce/2011/Oct/msg00003.html>⁹⁰¹⁴ <http://www.securityfocus.com/bid/49303>⁹⁰¹⁵ <http://www.kb.cert.org/vuls/id/405811>⁹⁰¹⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3192>⁹⁰¹⁷ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁰¹⁸ <http://www.osvdb.org/74721>⁹⁰¹⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14762>⁹⁰²⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14824>⁹⁰²¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18827>⁹⁰²² <http://rhn.redhat.com/errata/RHSA-2011-1245.html>⁹⁰²³ <http://rhn.redhat.com/errata/RHSA-2011-1294.html>

			REDHAT 2011:1300 ⁹⁰²⁴ RHSA- REDHAT 2011:1329 ⁹⁰²⁵ RHSA- REDHAT 2011:1330 ⁹⁰²⁶ RHSA- REDHAT 2011:1369 ⁹⁰²⁷ RHSA- SECUNIA 45606 ⁹⁰²⁸ SECUNIA 45937 ⁹⁰²⁹ SECUNIA 46000 ⁹⁰³⁰ SECUNIA 46125 ⁹⁰³¹ SECUNIA 46126 ⁹⁰³² XF 69396 ⁹⁰³³ URL1 9034 URL2 ⁹⁰³⁵		HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.20 Ažurirati na Apache HTTPD version 2.2.20 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.20.tar.gz
26.	Apache HTTPD: insecure LD_LIBRARY_PATH handling (CVE-2012-0883) (apache-httpd-cve-2012-0883)	172.23.202.197:80 Otkrivena je nebezbedna obrada rute LD_LIBRARY_PATH koja bi mogla da dovede do toga da direktorijum koji trenutno radi traži DSO-ove. Ovo bi lokalnom korisniku omogućilo da izvrši kôd kao root ako je adminitrator pokrenuo apachectl sa nepoverljivog direktorijuma.	APPLE APPLE-SA-2013-09-12-1 ⁹⁰³⁶ CVE CVE-2012-0883 ⁹⁰³⁷ SECUNIA 48849 ⁹⁰³⁸ URL1 ⁹⁰³⁹ URL2 ⁹⁰⁴⁰	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.23 Ažurirati na Apache HTTPD version 2.2.23 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz Apache HTTPD >= 2.4 and < 2.4.2 Ažurirati na Apache HTTPD version 2.4.2 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.2.tar.gz
27.	Plaintext credentials transmitted unencrypted (generic-plaintext-credentials)	172.23.202.197:110 Server podržava metode autorizacije kada se poverljivi podaci u vidu čitkog teksta šalju preko nedekriptovanih kanala. Ako napadač presretne komunikaciju između klijenta i servera, poverljivi podaci će biti otkriveni.		Ozbiljan	Onemogućiti metode autorizacije čitkog teksta ili omogućiti kriptovanje, u skladu sa specifičnom dokumentacijom proizvođa.
28.	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368) (apache-httpd-cve-2011-3368)	172.23.202.197:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja prisustva mod_proxy modula. Ranjivost na DOS napad otkrivena je u modulu	APPLE APPLE-SA-2012-09-19-2 ⁹⁰⁴¹ BID 49957 ⁹⁰⁴² CVE CVE-2011-3368 ⁹⁰⁴³ IAVM 2012-A-0017 ⁹⁰⁴⁴ IAVM 2012-A-0152 ⁹⁰⁴⁵ IAVM 2012-B-0056 ⁹⁰⁴⁶	Ozbiljan	Apache HTTPD >= 1.3 and < 2 Primeniti zakrpu za CVE-2011-3368 to 1.3 Uraditi download a zatim instalirati: http://archive.apache.org/dis

⁹⁰²⁴ <http://rhn.redhat.com/errata/RHSA-2011-1300.html>

⁹⁰²⁵ <http://rhn.redhat.com/errata/RHSA-2011-1329.html>

⁹⁰²⁶ <http://rhn.redhat.com/errata/RHSA-2011-1330.html>

⁹⁰²⁷ <http://rhn.redhat.com/errata/RHSA-2011-1369.html>

⁹⁰²⁸ <http://secunia.com/advisories/45606/>

⁹⁰²⁹ <http://secunia.com/advisories/45937/>

⁹⁰³⁰ <http://secunia.com/advisories/46000/>

⁹⁰³¹ <http://secunia.com/advisories/46125/>

⁹⁰³² <http://secunia.com/advisories/46126/>

⁹⁰³³ <http://xforce.iss.net/xforce/xfdb/69396>

⁹⁰³⁴ http://httpd.apache.org/security/vulnerabilities_22.html

⁹⁰³⁵ http://httpd.apache.org/security/vulnerabilities_20.html

⁹⁰³⁶ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>

⁹⁰³⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0883>

⁹⁰³⁸ <http://secunia.com/advisories/48849/>

⁹⁰³⁹ http://httpd.apache.org/security/vulnerabilities_22.html

⁹⁰⁴⁰ http://httpd.apache.org/security/vulnerabilities_24.html

⁹⁰⁴¹ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>

⁹⁰⁴² <http://www.securityfocus.com/bid/49957>

⁹⁰⁴³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3368>

⁹⁰⁴⁴ <http://iase.disa.mil/stigs/iavm-cve.html>

⁹⁰⁴⁵ <http://iase.disa.mil/stigs/iavm-cve.html>

		mod_proxy ukoliko se on koristi kao reverzni proxy. Zlonamerni napadač bi mogao da iskoristi ovaj propust na takav način da primora proxy proces da se poveže sa proizvoljnim serverom i potencijalno objavi osetljive informacije sa internih web servera koje inače napadaču nisu direktno dostupne. Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/	OSVDB 76079 ⁹⁰⁴⁷ REDHAT RHSA-2011:1391 ⁹⁰⁴⁸ REDHAT RHSA-2011:1392 ⁹⁰⁴⁹ SECUNIA 46288 ⁹⁰⁵⁰ SECUNIA 46414 ⁹⁰⁵¹ SECUNIA 48551 ⁹⁰⁵² XF 70336 ⁹⁰⁵³ URL1 ⁹⁰⁵⁴ URL2 ⁹⁰⁵⁵ URL3 ⁹⁰⁵⁶		t/httpd/patches/apply_to_1.3.42/ Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
29.	Apache HTTPD: scoreboard parent DoS (CVE-2012-0031) (apache-httpd-cve-2012-0031)	172.23.202.197:80 Propust je otkriven u obradi scoreboard-a. Neprivilegovani child proces bi mogao da dovede do toga da parent proces krahira prilikom gašenja.	APPLE APPLE-SA-2012-09-19-2 ⁹⁰⁵⁷ BID 51407 ⁹⁰⁵⁸ CVE CVE-2012-0031 ⁹⁰⁵⁹ IAVM 2012-A-0017 ⁹⁰⁶⁰ REDHAT RHSA-2012:0128 ⁹⁰⁶¹ SECUNIA 47410 ⁹⁰⁶² SECUNIA 48551 ⁹⁰⁶³ URL1 ⁹⁰⁶⁴ URL2 ⁹⁰⁶⁵	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
30.	Apache HTTPD: mod_proxy_ajp remote DoS (CVE-2012-4557) (apache-httpd-cve-2012-4557)	172.23.202.197:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ajp. Proveriti konfiguraciju web servera	CVE CVE-2012-4557 ⁹⁰⁶⁶ DEBIAN DSA-2579 ⁹⁰⁶⁷ URL1 ⁹⁰⁶⁸	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz

⁹⁰⁴⁶ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁰⁴⁷ <http://www.osvdb.org/76079>⁹⁰⁴⁸ [http://rhn.redhat.com/errata/RHSA-2011-1391.html](https://rhn.redhat.com/errata/RHSA-2011-1391.html)⁹⁰⁴⁹ [http://rhn.redhat.com/errata/RHSA-2011-1392.html](https://rhn.redhat.com/errata/RHSA-2011-1392.html)⁹⁰⁵⁰ <http://secunia.com/advisories/46288/>⁹⁰⁵¹ <http://secunia.com/advisories/46414/>⁹⁰⁵² <http://secunia.com/advisories/48551/>⁹⁰⁵³ <http://xforce.iss.net/xforce/xfdb/70336>⁹⁰⁵⁴ http://httpd.apache.org/security/vulnerabilities_13.html⁹⁰⁵⁵ http://httpd.apache.org/security/vulnerabilities_20.html⁹⁰⁵⁶ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁰⁵⁷ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁹⁰⁵⁸ <http://www.securityfocus.com/bid/51407>⁹⁰⁵⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0031>⁹⁰⁶⁰ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁰⁶¹ [http://rhn.redhat.com/errata/RHSA-2012-0128.html](https://rhn.redhat.com/errata/RHSA-2012-0128.html)⁹⁰⁶² <http://secunia.com/advisories/47410/>⁹⁰⁶³ <http://secunia.com/advisories/48551/>⁹⁰⁶⁴ http://httpd.apache.org/security/vulnerabilities_20.html⁹⁰⁶⁵ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁰⁶⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4557>⁹⁰⁶⁷ <http://www.debian.org/security/2012/dsa-2579>⁹⁰⁶⁸ http://httpd.apache.org/security/vulnerabilities_22.html

		radi utvrđivanja ove mogućnosti. Mod_proxy_ajp će vratiti pogrešan kôd statusa ako naide na grešku, prouzrokujući da backend server bude stavljen u status greške dok ne istekne vreme za ponovni pokušaj. Udaljeni napadač bi mogao da pošalje zlonameran zahtev da bi pokrenuo ovaj problem, što bi dovelo do privremenog odbijanja servisa.			
31.	Apache HTTPD: mod_rewrite log escape filtering (CVE-2013-1862) (apache-httpd-cve-2013-1862)	172.23.202.197:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_rewrite. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Modul mod_rewrite ne filtrira završne izlazne sekvence iz logova, što zlonamenom napadaču olakšava da ubace takve sekvence u završne emulatore koji sadrže ranjivosti koje se odnose na izlazne sekvence.	CVE CVE-2013-1862 ⁹⁰⁶⁹ OVAL OVAL18790 ⁹⁰⁷⁰ REDHAT RHSA-2013:0815 ⁹⁰⁷¹ REDHAT RHSA-2013:1207 ⁹⁰⁷² REDHAT RHSA-2013:1208 ⁹⁰⁷³ REDHAT RHSA-2013:1209 ⁹⁰⁷⁴ SECUNIA 55032 ⁹⁰⁷⁵ URL1 ⁹⁰⁷⁶ URL2 ⁹⁰⁷⁷	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.25 Ažurirati na Apache HTTPD version 2.2.25 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.25.tar.gz
32.	Apache HTTPD: mod_proxy_ajp remote DoS (CVE-2011-3348) (apache-httpd-cve-2011-3348)	172.23.202.197:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ajp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven kada se mod_proxy_ajp koristi zajedno sa mod_proxy_balancer. Sa specifičnom konfiguracijom, udaljeni napadač može da pošalje zlonameran HTTP zahtev, prouzrokujući da backend server bude stavljen u status greške dok ne istekne vreme za ponovni pokušaj. To bi dovelo do odbijanja servisa.	APPLE APPLE-SA-2012-02-01-1 ⁹⁰⁷⁸ BID 49616 ⁹⁰⁷⁹ CVE CVE-2011-3348 ⁹⁰⁸⁰ IAVM 2012-B-0056 ⁹⁰⁸¹ OVAL OVAL14941 ⁹⁰⁸² OVAL OVAL18154 ⁹⁰⁸³ REDHAT RHSA-2011:1391 ⁹⁰⁸⁴ SECUNIA 46013 ⁹⁰⁸⁵ XF 69804 ⁹⁰⁸⁶ URL1 ⁹⁰⁸⁷	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.21 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.21.tar.gz
33.	Apache HTTPD: mod_setenvif.htaccess privilege escalation (CVE-2011-3607) (apache-httpd-cve-2011-3607)	172.23.202.197:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_setenvif. Proveriti konfiguraciju	APPLE APPLE-SA-2012-09-19-2 ⁹⁰⁸⁸ BID 50494 ⁹⁰⁸⁹ CVE CVE-2011-3607 ⁹⁰⁹⁰ IAVM 2012-A-0017 ⁹⁰⁹¹	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uradi download a zatim

⁹⁰⁶⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1862>
⁹⁰⁷⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18790>
⁹⁰⁷¹ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>
⁹⁰⁷² <http://rhn.redhat.com/errata/RHSA-2013-1207.html>
⁹⁰⁷³ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>
⁹⁰⁷⁴ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>
⁹⁰⁷⁵ <http://secunia.com/advisories/55032/>
⁹⁰⁷⁶ http://httpd.apache.org/security/vulnerabilities_20.html
⁹⁰⁷⁷ http://httpd.apache.org/security/vulnerabilities_22.html
⁹⁰⁷⁸ <http://lists.apple.com/archives/security-announce/2012/Feb/msg00000.html>
⁹⁰⁷⁹ <http://www.securityfocus.com/bid/49616>
⁹⁰⁸⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3348>
⁹⁰⁸¹ <http://iase.disa.mil/stigs/iavm-cve.html>
⁹⁰⁸² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14941>
⁹⁰⁸³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18154>
⁹⁰⁸⁴ <http://rhn.redhat.com/errata/RHSA-2011-1391.html>
⁹⁰⁸⁵ <http://secunia.com/advisories/46013/>
⁹⁰⁸⁶ <http://xforce.iss.net/xforce/xfdb/69804>
⁹⁰⁸⁷ http://httpd.apache.org/security/vulnerabilities_22.html
⁹⁰⁸⁸ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>
⁹⁰⁸⁹ <http://www.securityfocus.com/bid/50494>
⁹⁰⁹⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3607>

	2011-3607)	web servera radi utvrđivanja ove mogućnosti. Propust preopterećenja je otkriven kada je omogućen modul mod_setenvif, što lokalnim korisnicima omogućava da dobiju privilegije preko fajla .htaccess.	IAVM 2012-A-0152 ⁹⁰⁹² OSVDB 76744 REDHAT RHSA-2012:0128 ⁹⁰⁹³ SECUNIA 45793 ⁹⁰⁹⁴ SECUNIA 48551 ⁹⁰⁹⁵ XF 71093 ⁹⁰⁹⁶ URL1 ⁹⁰⁹⁷ URL2 ⁹⁰⁹⁸		instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
34.	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-4317) (apache-httpd-cve-2011-4317)	172.23.202.197:80 Skenirani servis je osjetljiv na ovu ranjivost samo ako je pokrenut modul mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy U određenim konfiguracijama koje koriste RewriteRule sa proxy flag-om ili ProxyPassMatch, udaljeni napadač bi mogao da primora reverzni proksi da se poveže sa proizvoljnim serverom i potencijalno objavi osjetljive informacije sa internih web servera koje inače napadaču nisu direktno dostupne.	APPLE APPLE-SA-2012-09-19-2 ⁹⁰⁹⁹ CVE CVE-2011-4317 ⁹¹⁰⁰ IAVM 2012-A-0017 ⁹¹⁰¹ IAVM 2012-A-0152 ⁹¹⁰² REDHAT RHSA-2012:0128 ⁹¹⁰³ SECUNIA 48551 ⁹¹⁰⁴ URL1 ⁹¹⁰⁵	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
35.	Apache HTTPD: error responses can expose cookies (CVE-2012-0053) (apache-httpd-cve-2012-0053)	172.23.202.197:80 Propust je otkriven u difoltnom pogrešnom odgovoru za statusni kôd 400. Zlonamerni napadač bi mogao da iskoristi ovaj propust da objavi "httpOnly" kolačiće ako nije određen dokument custom ErrorDocument.	APPLE APPLE-SA-2012-09-19-2 ⁹¹⁰⁶ BID 51706 ⁹¹⁰⁷ CVE CVE-2012-0053 ⁹¹⁰⁸ IAVM 2012-A-0017 ⁹¹⁰⁹ REDHAT RHSA-2012:0128 ⁹¹¹⁰ SECUNIA 48551 ⁹¹¹¹ URL1 ⁹¹¹² URL2 ⁹¹¹³	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz

⁹⁰⁹¹ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁰⁹² <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁰⁹³ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁹⁰⁹⁴ <http://secunia.com/advisories/45793/>⁹⁰⁹⁵ <http://secunia.com/advisories/48551/>⁹⁰⁹⁶ <http://xforce.iss.net/xforce/xfdb/71093>⁹⁰⁹⁷ http://httpd.apache.org/security/vulnerabilities_20.html⁹⁰⁹⁸ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁰⁹⁹ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁹¹⁰⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4317>⁹¹⁰¹ <http://iase.disa.mil/stigs/iavm-cve.html>⁹¹⁰² <http://iase.disa.mil/stigs/iavm-cve.html>⁹¹⁰³ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁹¹⁰⁴ <http://secunia.com/advisories/48551/>⁹¹⁰⁵ http://httpd.apache.org/security/vulnerabilities_22.html⁹¹⁰⁶ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁹¹⁰⁷ <http://www.securityfocus.com/bid/51706>⁹¹⁰⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0053>⁹¹⁰⁹ <http://iase.disa.mil/stigs/iavm-cve.html>⁹¹¹⁰ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁹¹¹¹ <http://secunia.com/advisories/48551/>⁹¹¹² http://httpd.apache.org/security/vulnerabilities_20.html⁹¹¹³ http://httpd.apache.org/security/vulnerabilities_22.html

36.	Apache HTTPD: XSS due to unescaped hostnames (CVE-2012-3499) (apache-httpd-cve-2012-3499)	172.23.202.197:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut jedan od sledećih modula: mod_imagemap, mod_info, mod_ldap, mod_proxy_ftp, mod_status. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Različiti XSS propusti usled nenapuštenih host imena i URI-ja HTML output-a u mod_info, mod_status, mod_imagemap, mod_ldap i mod_proxy_ftp.	APPLE APPLE-SA-2013-09-12-1 ⁹¹¹⁴ CVE CVE-2012-3499 ⁹¹¹⁵ DEBIAN DSA-2637 ⁹¹¹⁶ REDHAT RHSA-2013:0815 ⁹¹¹⁷ REDHAT RHSA-2013:1207 ⁹¹¹⁸ REDHAT RHSA-2013:1208 ⁹¹¹⁹ REDHAT RHSA-2013:1209 ⁹¹²⁰ SECUNIA 55032 ⁹¹²¹ URL1 ⁹¹²² URL2 ⁹¹²³	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.24 Ažurirati na Apache HTTPD version 2.2.24 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz Apache HTTPD >= 2.4 and < 2.4.4 Ažurirati na Apache HTTPD version 2.4.4 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz
37.	Apache HTTPD: XSS in mod_proxy_balancer (CVE-2012-4558) (apache-httpd-cve-2012-4558)	172.23.202.197:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy_balancer. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. XSS propust je uticao na manager interfejs mod_proxy_balancer-a.	APPLE APPLE-SA-2013-09-12-1 ⁹¹²⁴ CVE CVE-2012-4558 ⁹¹²⁵ DEBIAN DSA-2637 ⁹¹²⁶ REDHAT RHSA-2013:0815 ⁹¹²⁷ REDHAT RHSA-2013:1207 ⁹¹²⁸ REDHAT RHSA-2013:1208 ⁹¹²⁹ REDHAT RHSA-2013:1209 ⁹¹³⁰ URL1 ⁹¹³¹ URL2 ⁹¹³²	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.24 Ažurirati na Apache HTTPD version 2.2.24 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz Apache HTTPD >= 2.4 and < 2.4.4 Ažurirati na Apache HTTPD version 2.4.4 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz
38.	Apache HTTPD: mod_dav crash (CVE-2013-1896) (apache-httpd-cve-2013-1896)	172.23.202.197:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_dav_svn. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Slanje MERGE zahteva URI-ju koji obrađuje mod_dav_svn sa izvorom href (poslato kao deo zahteva XML) ciljajući na URI koji nije konfigurisan za DAV prouzrokuje segmentation fault	CVE CVE-2013-1896 ⁹¹³³ OVAL OVAL18835 ⁹¹³⁴ REDHAT RHSA-2013:1156 ⁹¹³⁵ REDHAT RHSA-2013:1207 ⁹¹³⁶ REDHAT RHSA-2013:1208 ⁹¹³⁷ REDHAT RHSA-2013:1209 ⁹¹³⁸ SECUNIA 55032 ⁹¹³⁹	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.25 Ažurirati na Apache HTTPD version 2.2.25 Apache HTTPD >= 2.4 and < 2.4.6 Ažurirati na Apache HTTPD version 2.4.6 Uraditi download a zatim instalirati: http://archive.apache.org/dist

⁹¹¹⁴ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁹¹¹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3499>⁹¹¹⁶ <http://www.debian.org/security/2013/dsa-2637>⁹¹¹⁷ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁹¹¹⁸ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁹¹¹⁹ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁹¹²⁰ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁹¹²¹ <http://secunia.com/advisories/55032/>⁹¹²² http://httpd.apache.org/security/vulnerabilities_22.html⁹¹²³ http://httpd.apache.org/security/vulnerabilities_24.html⁹¹²⁴ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁹¹²⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4558>⁹¹²⁶ <http://www.debian.org/security/2013/dsa-2637>⁹¹²⁷ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁹¹²⁸ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁹¹²⁹ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁹¹³⁰ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁹¹³¹ http://httpd.apache.org/security/vulnerabilities_22.html⁹¹³² http://httpd.apache.org/security/vulnerabilities_24.html⁹¹³³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1896>⁹¹³⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18835>⁹¹³⁵ <http://rhn.redhat.com/errata/RHSA-2013-1156.html>⁹¹³⁶ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁹¹³⁷ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁹¹³⁸ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁹¹³⁹ <http://secunia.com/advisories/55032/>

		(segfault).	URL1 ⁹¹⁴⁰ URL2 ⁹¹⁴¹		t/httpd/httpd-2.4.6.tar.gz
39.	Apache HTTPD: XSS in mod_negotiation when untrusted uploads are supported (CVE-2012-2687) (apachehttpd-cve-2012-2687)	172.23.202.197:80 Skenirani servis je osjetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_negotiation. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Moguće je ubaciti CRLF (Carriage Return and Line Feed) koji omogućava CRLF Injection napade (poznatih i kao HTTP Response Splitting) za sajtove koji koriste mod_negotiation, omogućavajući neproverene upload-ove na lokacije na kojima je omogućen MultiViews (višestruko pregledanje). Ovaj problem je poznat i kao CVE-2008-0455.	APPLE APPLE-SA-2013-09-12-1 ⁹¹⁴² BID 55131 ⁹¹⁴³ CVE CVE-2012-2687 ⁹¹⁴⁴ IAVM 2012-A-0139 ⁹¹⁴⁵ REDHAT RHSA-2012:1591 ⁹¹⁴⁶ REDHAT RHSA-2012:1592 ⁹¹⁴⁷ REDHAT RHSA-2012:1594 ⁹¹⁴⁸ REDHAT RHSA-2013:0130 ⁹¹⁴⁹ SECUNIA 50894 ⁹¹⁵⁰ SECUNIA 51607 ⁹¹⁵¹ URL1 ⁹¹⁵² URL2 ⁹¹⁵³	Umeren	Apache HTTPD >= 2.2 and < 2.2.23 Ažurirati na Apache HTTPD version 2.2.23 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz Apache HTTPD >= 2.4 and < 2.4.3 Ažurirati na Apache HTTPD version 2.4.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.3.tar.gz

Tabela 131. Linux OS sa IP adresama 172.23.202.199, 172.23.202.224 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.199		OS: Scilinux 60 x64, scilinux60x64			35
IP adresa: 172.23.202.224		OS: Scilinux 60 x86, scilinux60x86			35
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Apache HTTPD: expat DoS (CVE-2009-3560) (apache-httpd-cve-2009-3560)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u mogućnosti da dovede do toga da Apache parsira nepovreljiv XML dokument. Proveriti konfiguraciju web servera	BID 37203 ⁹¹⁵⁴ CVE CVE-2009-3560 ⁹¹⁵⁵ DEBIAN DSA-1953 ⁹¹⁵⁶ IAVM 2012-A-0020 ⁹¹⁵⁷ OVAL OVAL12942 ⁹¹⁵⁸ REDHAT RHSA-2011:0896 ⁹¹⁵⁹ OVAL OVAL10613 ⁹¹⁶⁰ OVAL OVAL6883 ⁹¹⁶¹ SECUNIA 37537 ⁹¹⁶² SECUNIA 38231 ⁹¹⁶³	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.17 Ažurirati na Apache HTTPD version 2.2.17 Uraditi download a zatim instalirati:

⁹¹⁴⁰ http://httpd.apache.org/security/vulnerabilities_22.html⁹¹⁴¹ http://httpd.apache.org/security/vulnerabilities_24.html⁹¹⁴² <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁹¹⁴³ <http://www.securityfocus.com/bid/55131>⁹¹⁴⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2687>⁹¹⁴⁵ <http://iase.disa.mil/stigs/iavm-cve.html>⁹¹⁴⁶ <http://rhn.redhat.com/errata/RHSA-2012-1591.html>⁹¹⁴⁷ <http://rhn.redhat.com/errata/RHSA-2012-1592.html>⁹¹⁴⁸ <http://rhn.redhat.com/errata/RHSA-2012-1594.html>⁹¹⁴⁹ <http://rhn.redhat.com/errata/RHSA-2013-0130.html>⁹¹⁵⁰ <http://secunia.com/advisories/50894/>⁹¹⁵¹ <http://secunia.com/advisories/51607/>⁹¹⁵² http://httpd.apache.org/security/vulnerabilities_22.html⁹¹⁵³ http://httpd.apache.org/security/vulnerabilities_24.html⁹¹⁵⁴ <http://www.securityfocus.com/bid/37203>⁹¹⁵⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3560>⁹¹⁵⁶ <http://www.debian.org/security/DSA-1953> pristupljeno dana 18.12.2011⁹¹⁵⁷ <http://iase.disa.mil/stigs/iavm-cve.html>⁹¹⁵⁸ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:12942>⁹¹⁵⁹ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁹¹⁶⁰ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:10613>⁹¹⁶¹ <http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.oval.def:6883>⁹¹⁶² <http://secunia.com/advisories/37537/>⁹¹⁶³ <http://secunia.com/advisories/38231/>

		radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepoverljivi XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	SECUNIA 38794 ⁹¹⁶⁴ SECUNIA 38832 ⁹¹⁶⁵ SECUNIA 38834 ⁹¹⁶⁶ SECUNIA 39478 ⁹¹⁶⁷ SECUNIA 41701 ⁹¹⁶⁸ SECUNIA 43300 ⁹¹⁶⁹ URL1 ⁹¹⁷⁰		http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
2.	Apache HTTPD: expat DoS (CVE-2009-3720) (apache-httpd-cve-2009-3720)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Skenirani servis je ranjiv samo ukoliko je zlonamerni napadač u mogućnosti da dovede do toga da Apache parsira nepoverljiv XML dokument. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust prepunjavanja bafera "buffer over-read" je otkriven u sklopu kompleta expat library. Napadač koji je u mogućnosti da dovede do toga da Apache parsira nepoverljivi XML dokument (na primer kroz mod_dav), mogao bi da prouzrokuje krah. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM (Multi-Processing Module).	IAVM 2012-A-0020 ⁹¹⁷¹ OVAL OVAL12719 ⁹¹⁷² REDHAT RHSA-2011:0896 ⁹¹⁷³ CVE CVE-2009-3720 ⁹¹⁷⁴ OVAL OVAL11019 ⁹¹⁷⁵ OVAL OVAL7112 ⁹¹⁷⁶ REDHAT RHSA-2010:0002 ⁹¹⁷⁷ SECUNIA 37324 ⁹¹⁷⁸ SECUNIA 37537 ⁹¹⁷⁹ SECUNIA 37925 ⁹¹⁸⁰ SECUNIA 38050 ⁹¹⁸¹ SECUNIA 38231 ⁹¹⁸² SECUNIA 38794 ⁹¹⁸³ SECUNIA 38832 ⁹¹⁸⁴ SECUNIA 38834 ⁹¹⁸⁵ SECUNIA 39478 ⁹¹⁸⁶ SECUNIA 41701 ⁹¹⁸⁷ SECUNIA 43300 ⁹¹⁸⁸ URL1 ⁹¹⁸⁹	Ozbiljan	Apache >= 2.0 and < 2.1 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.17 Ažurirati na Apache HTTPD version 2.2.17 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
3.	Apache HTTPD: apr_bridage_split_line DoS (CVE-2010-1623) (apache-httpd-cve-2010-1623)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako Apache	IAVM 2012-B-0056 ⁹¹⁹⁰ OVAL OVAL12800 ⁹¹⁹¹ REDHAT RHSA-2011:0896 ⁹¹⁹² REDHAT RHSA-2011:0897 ⁹¹⁹³	Ozbiljan	Apache >= 2.0 and < 2.1 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and

⁹¹⁶⁴ <http://secunia.com/advisories/38794/>⁹¹⁶⁵ <http://secunia.com/advisories/38832/>⁹¹⁶⁶ <http://secunia.com/advisories/38834/>⁹¹⁶⁷ <http://secunia.com/advisories/39478/>⁹¹⁶⁸ <http://secunia.com/advisories/41701/>⁹¹⁶⁹ <http://secunia.com/advisories/43300/>⁹¹⁷⁰ http://httpd.apache.org/security/vulnerabilities_20.html⁹¹⁷¹ <http://iase.disa.mil/stigs/iavm-cve.html>⁹¹⁷² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12719>⁹¹⁷³ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁹¹⁷⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3720>⁹¹⁷⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11019>⁹¹⁷⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7112>⁹¹⁷⁷ <http://rhn.redhat.com/errata/RHSA-2010-0002.html>⁹¹⁷⁸ <http://secunia.com/advisories/37324/>⁹¹⁷⁹ <http://secunia.com/advisories/37537/>⁹¹⁸⁰ <http://secunia.com/advisories/37925/>⁹¹⁸¹ <http://secunia.com/advisories/38050/>⁹¹⁸² <http://secunia.com/advisories/38231/>⁹¹⁸³ <http://secunia.com/advisories/38794/>⁹¹⁸⁴ <http://secunia.com/advisories/38832/>⁹¹⁸⁵ <http://secunia.com/advisories/38834/>⁹¹⁸⁶ <http://secunia.com/advisories/39478/>⁹¹⁸⁷ <http://secunia.com/advisories/41701/>⁹¹⁸⁸ <http://secunia.com/advisories/43300/>⁹¹⁸⁹ http://httpd.apache.org/security/vulnerabilities_20.html⁹¹⁹⁰ <http://iase.disa.mil/stigs/iavm-cve.html>⁹¹⁹¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12800>⁹¹⁹² <http://rhn.redhat.com/errata/RHSA-2011-0896.html>

		procesira ne-SSL zahteve. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_brigade_split_line() u sklopu kompleta APR-util library, koji se koristi za procesiranje ne-SSL zahteva. Udaljeni napadač bi mogao da šalje zahteve, pažljivo izrađujući tajming za pojedinačne bajtove, što bi polako zauzimalo memoriju i potencijalno dovelo do odbijanja servisa.	BID 43673 ⁹¹⁹⁴ CVE CVE-2010-1623 ⁹¹⁹⁵ REDHAT RHSA-2010:0950 ⁹¹⁹⁶ SECUNIA 41701 ⁹¹⁹⁷ SECUNIA 42015 ⁹¹⁹⁸ SECUNIA 42361 ⁹¹⁹⁹ SECUNIA 42367 ⁹²⁰⁰ SECUNIA 42403 ⁹²⁰¹ SECUNIA 42537 ⁹²⁰² SECUNIA 43211 ⁹²⁰³ SECUNIA 43285 ⁹²⁰⁴ URL1 ⁹²⁰⁵		< 2.2.17 Ažurirati na Apache HTTPD version 2.2.17 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.17.tar.gz
4.	Apache httpd Timeout detection flaw (mod_proxy_http) (CVE-2010-2068) (apache-httpd-2_2_x-timeoutdetection-flaw-mod_proxy_http-cve-2010-2068)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Propust sa kojim je omogućeno otkrivanje informacija je otkriven u modulu mod_proxy_http na verzijama 2.2.9 do 2.2.15, 2.3.4-alpha i 2.3.5-alpha. Pod određenim tajmout uslovima, server bi mogao da uzvрати odgovorom koji je namenjen drugom korisniku. Ugroženi su samo operativni sistemi Windows, Netware i OS2. Ugrožene su one konfiguracije koje pokreću korišćenje proxy worker pool-ova. Na ranijim verzijama nije bilo ranjivosti, jer proxy pool-ovi još nisu bili uvedeni. Zahvaljujući Loren Anderson-u ovaj problem je prijavljen, a najjednostavniji način njegovog izbegavanja jeste opšte konfigurisanje.	APPLE APPLE-SA-2011-03-21 ⁹²⁰⁶ BID 40827 ⁹²⁰⁷ CVE CVE-2010-2068 ⁹²⁰⁸ OVAL OVAL11491 ⁹²⁰⁹ OVAL OVAL6931 ⁹²¹⁰ SECUNIA 40206 ⁹²¹¹ SECUNIA 41480 ⁹²¹² SECUNIA 41490 ⁹²¹³ SECUNIA 41722 ⁹²¹⁴ XF apache-modproxyhttp-timeout-info-disc(59413) ⁹²¹⁵ URL1 ⁹²¹⁶	Ozbiljan	Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.16.tar.gz
5.	X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch)	172.23.202.199:443 172.23.202.224:443 Rubrika u sertifikatu X.509 sa uobičajenim nazivom subjekta (CN) ne poklapa se sa imenom pojedinca koje je navedeno u sertifikatu. Pre izdavanja sertifikata,		Ozbiljan	Rubrika sa uobičajenim nazivom subjekta (CN) u sertifikatu X.509 treba da bude podešena da sadrži ime pojedinca koji prikazuje sertifikat (npr. ime hosta). To se postiže

⁹¹⁹³ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>⁹¹⁹⁴ <http://www.securityfocus.com/bid/43673>⁹¹⁹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1623>⁹¹⁹⁶ <http://rhn.redhat.com/errata/RHSA-2010-0950.html>⁹¹⁹⁷ <http://secunia.com/advisories/41701/>⁹¹⁹⁸ <http://secunia.com/advisories/42015/>⁹¹⁹⁹ <http://secunia.com/advisories/42361/>⁹²⁰⁰ <http://secunia.com/advisories/42367/>⁹²⁰¹ <http://secunia.com/advisories/42403/>⁹²⁰² <http://secunia.com/advisories/42537/>⁹²⁰³ <http://secunia.com/advisories/43211/>⁹²⁰⁴ <http://secunia.com/advisories/43285/>⁹²⁰⁵ http://httpd.apache.org/security/vulnerabilities_20.html⁹²⁰⁶ <http://lists.apple.com/archives/security-announce/2011/Mar/msg00006.html>⁹²⁰⁷ <http://www.securityfocus.com/bid/40827>⁹²⁰⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2068>⁹²⁰⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11491>⁹²¹⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6931>⁹²¹¹ <http://secunia.com/advisories/40206/>⁹²¹² <http://secunia.com/advisories/41480/>⁹²¹³ <http://secunia.com/advisories/41490/>⁹²¹⁴ <http://secunia.com/advisories/41722/>⁹²¹⁵ <http://xforce.iss.net/xforce/xfdb/59413>⁹²¹⁶ http://httpd.apache.org/security/vulnerabilities_22.html

		Certification Authority (CA) mora da proveriti identitet pojedinca koji potražuje sertifikat, kako je navedeno u CA-ovom Certification Practice Statement (CPS). Zbog toga, uobičajene procedure validacije sertifikata zahtevaju da rubrika sertifikata sa CN subjektom odgovara pravom imenu pojedinca koji prikazuje sertifikat. Na primer, u sertifikatu prikazanom na „https://www.example.com/“, naziv subjekta (CN) treba da bude „www.example.com“. U cilju otkrivanja i sprečavanja napada prisluškivanja, validnost sertifikata mora da bude overena, jer bi u suprotnom napadač mogao da otpočne napad preko posrednika i da stekne potpunu kontrolu nad protokom podataka. Od posebne važnosti je validnost naziva subjekta (CN), koji treba da se poklapa sa imenom pojedinca (imenom host-a). Neodgovarajući CN se najčešće javlja usled greške u konfiguraciji, iako on takođe može da ukazuje na to da se sprovodi napad preko posrednika.			izradom novog sertifikata, koji najčešće potpisuje Certification Authority (CA), koji je od poverenja kako za klijenta, tako i za server.
6.	FTP access with ftp account (ftp-generic-0001)	172.23.202.199:21 172.23.202.224:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisničkim ID-jem „ftp“ i šifrom „ftp“. Dosadašnja praksa je pokazala da treba ukloniti difoltnu naloge, ako je to moguće. Za naloge koje zahteva sistem, treba promeniti difoltnu šifru.	CVE CVE-1999-0497 ⁹²¹⁷	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko to nije kritično za dalje funkcionisanje sistema. U suprotnom, treba promeniti lozinku u nedifoltnu vrednost.
7.	FTP access with anonymous account (ftp-generic-0002)	172.23.202.199:21 172.23.202.224:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisničkim ID-jem „anonymous“ i šifrom „ftp@“. Dosadašnja praksa je pokazala da treba ukloniti difoltnu naloge, ako je to moguće. Za naloge koje zahteva sistem, treba promeniti difoltnu šifru.	CVE CVE-1999-0497 ⁹²¹⁸	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko to nije kritično za dalje funkcionisanje sistema. U suprotnom, treba promeniti lozinku u nedifoltnu vrednost.
8.	FTP server does not support AUTH command (ftp-generic-0007)	172.23.202.199:21 172.23.202.224:21 FTP klijenti po difoltu šalju FTP server-u poverljive podatke (korisnički ID i šifra) u vidu čitkog teksta. Ova okolnost dozvoljava zlonamernim korisnicima da presreću poverljive podatke ukoliko prisluškuju vezu. Noviji FTP serveri podržavaju AUTH komandu, koja omogućava dodatne opcije autentifikacije, kao što su TLS, Kerberos, GSSAPI itd. Ona se može koristiti za sprečavanje prisluškivanja na FTP vezama.		Ozbiljan	Ažurirati/preći na FTP server koji podržava AUTH komandu.
9.	Browsable web directory (http-generic-0001)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80		Ozbiljan	Za Apache: onemogućiti pretraživanje direktorijuma mreže za sve direktorijume i

⁹²¹⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>⁹²¹⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>

	browsable-dir)	172.23.202.224:443 Otkriven je direktorijum na web serveru koji može biti pretraživan, što znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice - spajdering (prateći hiperlinkove), ili -kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute force napadom na liste uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skrivenne“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice.			poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume. Za Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote: Onemogućiti pretraživanje direktorijuma za sve direktorijume i poddirektorijume. Uključiti Tomcat-ov web.xml file. U odeljku „default“, promeniti parametar „listings“ iz „true“ u „false“. Restartovati server. Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripta i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume.
10.	TLS/SSL Server Supports Weak Cipher Algorithms (ssl-weak-ciphers)	172.23.202.199:443 172.23.202.224:443 negotiated the SSL_DHE_RSA_WITH_DES_CBC_SHA cipher suite TLS/SSL server podržava šifre koje se zasnivaju na slabim algoritmima. To napadaču može omogućiti da pokrene napade preko posrednika i da pregleda ili čačka osetljive podatke. Uopšteno, sledeće šifre se smatraju slabim: Tzv. „null“ (nula) šifre, jer ne šifruju podatke. Eksportne šifre koje koriste dužine tajnih ključeva ograničene na 40 bitova. Na to najčešće ukazuje reč		Ozbiljan	Konfigurisati server tako da onemogući podršku za slabe šifre. Za Apache web servere sa mod_ssl, uključiti fajl Apache konfiguracije i izmeniti liniju SSLCipherSuite tako da u njoj piše: SSLCipherSuite ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM

		EXP/EXPORT u nazivu šifre. Zastareli algoritmi za šifrovanje čije se dužine tajnih ključeva po današnjim standardima smatraju kratkim, npr. DES ili RC4 sa 56-bitnim ključevima.			
11.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	TCP reset with incorrect sequence number triggered this fault on 172.23.202.199:21 172.23.202.224:21 Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183 ⁹²¹⁹ CERT-VN: 415294 ⁹²²⁰ CVE CVE-2004-0230 ⁹²²¹ MS: MS05-019 ⁹²²² MS: MS06-064 ⁹²²³ NETBSD: NetBSD-SA2004-006 ⁹²²⁴ OVAL: OVAL2689 ⁹²²⁵ OVAL: OVAL270 ⁹²²⁶ OVAL OVAL3508 ⁹²²⁷ OVAL OVAL4791 ⁹²²⁸ OVAL OVAL5711 ⁹²²⁹ SECUNIA: 11440 ⁹²³⁰ SECUNIA 11458 ⁹²³¹ SECUNIA: 22341 ⁹²³² SGI 20040403-01-A ⁹²³³ XF tcp-rst-dos(15886) ⁹²³⁴ URL1 ⁹²³⁵ URL2 ⁹²³⁶	Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC 2385 ⁹²³⁷ . Ono je napravljeno da smanji opasnost od određenih napada na BGP, kao što su TCP reseti.
12.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podesi na jedinstvenu vrednost i da se koristi u rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da fingerprint-uje operativni sistem.	BID 4314 ⁹²³⁸ CVE CVE-2002-0510 ⁹²³⁹ XF linux-udp-fingerprint(8588) ⁹²⁴⁰	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili pak ranjivost koju treba popravljati, tako da ne postoje rešenja koja se mogu kupiti. Jedino se može postaviti fajervol ili neka druga sprava za filtriranje između napadnutog i neprijateljskog napada koji je u mogućnosti da randomizuje IP ID-jeve.
13.	Apache HTTPD: apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Skenirani servis je osetljiv na ovu	CVE CVE-2011-0419 ⁹²⁴¹ DEBIAN DSA-2237 ⁹²⁴² IAVM 2012-B-0056 ⁹²⁴³ OVAL OVAL14638 ⁹²⁴⁴ OVAL OVAL14804 ⁹²⁴⁵	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim

⁹²¹⁹ <http://www.securityfocus.com/bid/10183>⁹²²⁰ <http://www.kb.cert.org/vuls/id/415294>⁹²²¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁹²²² <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁹²²³ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁹²²⁴ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁹²²⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>⁹²²⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>⁹²²⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>⁹²²⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>⁹²²⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>⁹²³⁰ <http://secunia.com/advisories/11440/>⁹²³¹ <http://secunia.com/advisories/11458/>⁹²³² <http://secunia.com/advisories/22341/>⁹²³³ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>⁹²³⁴ <http://xforce.iss.net/xforce/xfdb/15886>⁹²³⁵ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁹²³⁶ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>⁹²³⁷ <http://www.ietf.org/rfc/rfc2385.txt>⁹²³⁸ <http://www.securityfocus.com/bid/4314>⁹²³⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>⁹²⁴⁰ <http://xforce.iss.net/xforce/xfdb/8588>⁹²⁴¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419>⁹²⁴² <http://www.debian.org/security/2011/dsa-2237>⁹²⁴³ <http://iase.disa.mil/stigs/iavm-cve.html>⁹²⁴⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14638>⁹²⁴⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14804>

	httpdcve-2011-0419)	ranjivost SAMO ako izvršava jedan od sledećih modula: mod_autoindex. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_fnmatch() u sklopu APR biblioteke. Ako je omogućen mod_autoindex, a indeksi direktorijuma mod_autoindex su sadržavali fajlove sa dovoljno dugim nazivima, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do preterane upotrebe CPU-a. Ovo bi moglo da bude iskorišćeno u napadu odbijanja servisa. Zahvaljujući Maksymilian Arciemowicz prijavljen je ovaj propust.	REDHAT 2011:0896 ⁹²⁴⁶ REDHAT 2011:0897 ⁹²⁴⁷ REDHAT 2011:0507 ⁹²⁴⁸ SECUNIA 44490 ⁹²⁴⁹ SECUNIA 44564 ⁹²⁵⁰ SECUNIA 44574 ⁹²⁵¹ URL1 ⁹²⁵²		instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.19 Ažurirati na Apache HTTPD version 2.2.19 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.19.tar.gz
14.	Self-signed TLS/SSL certificate (ssl-self-signed-certificate)	172.23.202.199:443 172.23.202.224:443 TLS/SSL-a sertifikat servera je samopotpisan. Samopotpisani sertifikati po defaultu nisu od poverenja, naročito zato što napadi na TLS/SSL preko posrednika obično koriste samopotpisane sertifikate da prisluškuju TLS/SSL veze.		Ozbiljan	Nabaviti novi TLS/SSL serverov sertifikat koji NIJE samopotpisan i instalirati ga na server. Precizna uputstva za dobijanje novog sertifikata zavise od zahteva organizacije. Uopšteno, treba napraviti zahtev za sertifikat i taj zahtev sačuvati kao fajl. Ovaj fajl se zatim šalje Certificate Authority-ju (CA) na obradu. Organizacija možda poseduje sopstveni interni Certificate Authority. U suprotnom, potrebno je platiti sertifikat iz spoljnog poverljivog Certificate Authority-ja, kao što su Thawte, Verisign .
15.	HTTP TRACE Method Enabled (http-trace-method-enabled)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 HTTP TRACE metoda se obično koristi da uzvрати potpuni HTTP zahtev klijentu koji ga zahteva, u cilju debugovanja proxy servera. Napadač bi mogao da kreira web stranicu koristeći XMLHTTP, ActiveX ili XMLHttpRequest da natera klijenta da pošalje TRACE zahtev i	CERT-VN 867593 ⁹²⁵³ OSVDB 35511 ⁹²⁵⁴ OSVDB 3726 ⁹²⁵⁵ SECUNIA 10726 ⁹²⁵⁶ SECUNIA 17334 ⁹²⁵⁷ SECUNIA 21802 ⁹²⁵⁸ SECUNIA 25636 ⁹²⁵⁹ CVE CVE-2004-2320 ⁹²⁶⁰ CVE CVE-2004-2763 ⁹²⁶¹ CVE CVE-2005-3398 ⁹²⁶² CVE CVE-2006-4683 ⁹²⁶³ CVE CVE-2007-3008 ⁹²⁶⁴	Ozbiljan	Apache Onemogućiti HTTP TRACE metodu za Apache. Novije verzije Apache-a (1.3.34 i 2.0.55 i novije) omogućuju konfiguracionu direktivu koja se zove TraceEnable. Da bi se odbili TRACE zahtevi, dodaje se sledeći red u konfiguraciju servera: TraceEnable off

⁹²⁴⁶ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁹²⁴⁷ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>⁹²⁴⁸ <http://rhn.redhat.com/errata/RHSA-2011-0507.html>⁹²⁴⁹ <http://secunia.com/advisories/44490/>⁹²⁵⁰ <http://secunia.com/advisories/44564/>⁹²⁵¹ <http://secunia.com/advisories/44574/>⁹²⁵² http://httpd.apache.org/security/vulnerabilities_22.html⁹²⁵³ <http://www.kb.cert.org/vuls/id/867593>⁹²⁵⁴ <http://www.osvdb.org/35511>⁹²⁵⁵ <http://www.osvdb.org/3726>⁹²⁵⁶ <http://secunia.com/advisories/10726/>⁹²⁵⁷ <http://secunia.com/advisories/17334/>⁹²⁵⁸ <http://secunia.com/advisories/21802/>⁹²⁵⁹ <http://secunia.com/advisories/25636/>⁹²⁶⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2320>⁹²⁶¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2763>⁹²⁶² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-3398>⁹²⁶³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-4683>⁹²⁶⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3008>

		da sačuva klijenove kolačiće. Kao posledica može da se javi XSS napad. Primer: 172.23.202.193:80 Running vulnerable HTTP service. http://172.23.202.199/ 1: TRACE / HTTP/1.1 2: Host: 172.23.202.199 3: Cookie: vulnerable=yes	CVE CVE-2008-7253 ⁹²⁶⁵ CVE CVE-2009-2823 ⁹²⁶⁶ CVE CVE-2010-0386 ⁹²⁶⁷ OSVDB 877 ⁹²⁶⁸ SUN 50603 ⁹²⁶⁹ BID 9561 ⁹²⁷⁰ URL1 ⁹²⁷¹ URL2 ⁹²⁷²		Za starije verzije Apache web servera, koristiti modul mod_rewrite da bi se odbili TRACE zahteve: RewriteEngine On RewriteCond %{REQUEST_METHOD} ^TRACE RewriteRule .* - [F]
16.	Database Open Access (database-open-access)	172.23.202.199:3306 172.23.202.224:3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7.	URL1 ⁹²⁷³	Umeren	Konfigurisati server baze podataka tako da dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.
17.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatišu slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	CVE CVE-1999-0524 ⁹²⁷⁴ OSVDB 95 ⁹²⁷⁵ XF icmp-netmask(306) ⁹²⁷⁶ XF icmp-timestamp(322) ⁹²⁷⁷	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
18.	WebDAV Extensions are Enabled (http-generic-webdav-enabled)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 WebDAV je skup ekstenzija za HTTP protokol koji omogućava korisnicima da zajednički edituju i obrađuju fajlove na udaljenim web serverima. Mnogi web serveri po defaultu omogućavaju WebDAV ekstenzije, čak i kada nisu potrebne. S obzirom na dodatnu složenost, dosadašnja praksa je pokazala da treba onemogućiti WebDAV ukoliko se		Umeren	Apache: Potrebno je onemogućiti WebDAV (eng. Web-based Distributed Authoring and Versioning) za Apache. Proveriti da li je mod_dav modul isključen ili utvrditi da li postoji zahtevana autentifikacija na direktorijumima nad kojima se zahteva DAV.

⁹²⁶⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-7253>⁹²⁶⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2823>⁹²⁶⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0386>⁹²⁶⁸ <http://osvdb.org/887>⁹²⁶⁹ <https://sunsolve.sun.com/search/document.do?assetkey=1-22-50603-1> pristupljeno 18.12.2011⁹²⁷⁰ <http://www.securityfocus.com/bid/9561>⁹²⁷¹ <http://www.apacheweek.com/issues/03-01-24#news>⁹²⁷² <http://www.kb.cert.org/vuls/id/867593>⁹²⁷³ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf⁹²⁷⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁹²⁷⁵ <http://www.osvdb.org/95>⁹²⁷⁶ <http://xforce.iss.net/xforce/xfdb/306>⁹²⁷⁷ <http://xforce.iss.net/xforce/xfdb/322>

		trenutno ne koristi.			
19.	Apache HTTPD: insecure LD_LIBRARY_PATH handling (CVE-2012-0883) (apache-httpd-cve-2012-0883)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Otkrivena je nebezbedna obrada rute LD_LIBRARY_PATH koja bi mogla da dovede do toga da direktorijum koji trenutno radi traži DSO-ove. Ovo bi lokalnom korisniku omogućilo da izvrši kôd kao root ako je administrator pokrenuo apachectl sa nepoverljivog direktorijuma.	APPLE APPLE-SA-2013-09-12-1 ⁹²⁷⁸ CVE CVE-2012-0883 ⁹²⁷⁹ SECUNIA 48849 ⁹²⁸⁰ URL1 ⁹²⁸¹ URL2 ⁹²⁸²	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.23 Ažurirati na Apache HTTPD version 2.2.23 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz Apache HTTPD >= 2.4 and < 2.4.2 Ažurirati na Apache HTTPD version 2.4.2 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.2.tar.gz
20.	X.509 Server Certificate Is Invalid/Expired (tls-server-cert-expired)	Sertifikat X.509 na TLS/SSL serveru sadrži početni datum iz budućnosti ili je istekao. Proveriti proof za više detalja.		Ozbiljan	Nabaviti novi TLS/SSL serverov sertifikat i instalirati ga na server. Precizna uputstva za dobijanje novog sertifikata zavise od zahteva organizacije. Uopšteno, treba napraviti zahtev za sertifikat i taj zahtev sačuvati kao fajl. Ovaj fajl se zatim šalje Certificate Authority-ju (CA) na obradu. Proveriti da li su početni i završni datumi na novom sertifikatu validni. Organizacija možda poseduje sopstveni interni Certificate Authority. U suprotnom, potrebno je platiti sertifikat iz spoljnog poverljivog Certificate Authority-ja. Nakon prijema novog sertifikata od Certificate Authority-ja, potrebno je instalirati ga na TLS/SSL server. Tačna uputstva za instaliranje su za svaki proizvod različita. Proveriti njihovu dokumentaciju.
21.	Apache HTTPD: mod_dav DoS (CVE-2010-1452) (apache-httpd-cve-2010-1452)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako web server izvršava jedan od sledećih modula: mod_cache, mod_dav. Pregledajte konfiguraciju vašeg web servera radi validacije.	IAVM 2012-B-0056 ⁹²⁸³ OVAL OVAL12341 ⁹²⁸⁴ REDHAT RHSA-2011:0896 ⁹²⁸⁵ REDHAT RHSA-2011:0897 ⁹²⁸⁶ APPLE APPLE-SA-2011-03-21 ⁹²⁸⁷ CVE CVE-2010-1452 ⁹²⁸⁸ OVAL OVAL11683 ⁹²⁸⁹	Ozbiljan	Apache >= 2.0 and < 2.1 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.64.tar.gz Apache HTTPD >= 2.2 and < 2.2.16 Ažurirati na Apache HTTPD version 2.2.16 Uraditi download a zatim

⁹²⁷⁸ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁹²⁷⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0883>⁹²⁸⁰ <http://secunia.com/advisories/48849/>⁹²⁸¹ http://httpd.apache.org/security/vulnerabilities_22.html⁹²⁸² http://httpd.apache.org/security/vulnerabilities_24.html⁹²⁸³ <http://iase.disa.mil/stigs/iavm-cve.html>⁹²⁸⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:12341>⁹²⁸⁵ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁹²⁸⁶ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>⁹²⁸⁷ <http://lists.apple.com/archives/security-announce/2011/Mar/msg00006.html>⁹²⁸⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1452>

		Propust je otkriven u obradi zahteva od strane mod_cache i mod_dav. Zlonameran udaljeni napadač bi mogao da pošalje pažljivo izrađen zahtev i prouzrokuje da httpd child proces krahira. Ovakav krah bi se manifestovao samo kao odbijanje servisa ako se koristi Worker MPM. Ovaj problem se dalje može ublažiti ako na mod_dav samo utiču zahtevi za koje postoji mogućnost autentifikovanja, a mod_cache je pod uticajem samo ako se koristi neuobičajena „CacheIgnoreURLSessionIdentifiers“ direktiva, uvedena u verziji 2.2.14. Ovaj problem je prijavio Mark Drayton.	REDHAT RHSA-2010:0659⁹²⁹⁰ SECUNIA 42367⁹²⁹¹ URL1⁹²⁹²		instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.16.tar.gz
22.	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368) (apache-httpd-cve-2011-3368)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja prisustva mod_proxy modula. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy. Zlonamerni napadač bi mogao da iskoristi ovaj propust na takav način da primora proxy proces da se poveže sa proizvoljnim serverom i potencijalno objavi osjetljive informacije sa internih web servera koje inače napadaču nisu direktno dostupne. Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/	APPLE APPLE-SA-2012-09-19-2⁹²⁹³ BID 49957⁹²⁹⁴ CVE CVE-2011-3368⁹²⁹⁵ IAVM 2012-A-0017⁹²⁹⁶ IAVM 2012-A-0152⁹²⁹⁷ IAVM 2012-B-0056⁹²⁹⁸ OSVDB 76079⁹²⁹⁹ REDHAT RHSA-2011:1391⁹³⁰⁰ REDHAT RHSA-2011:1392⁹³⁰¹ SECUNIA 46288⁹³⁰² SECUNIA 46414⁹³⁰³ SECUNIA 48551⁹³⁰⁴ XF 70336⁹³⁰⁵ URL1⁹³⁰⁶ URL2⁹³⁰⁷ URL3⁹³⁰⁸	Ozbiljan	Apache HTTPD >= 1.3 and < 2 Primeniti zakrpu za CVE-2011-3368 to 1.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz

⁹²⁸⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11683>

⁹²⁹⁰ <http://rhn.redhat.com/errata/RHSA-2010-0659.html>

⁹²⁹¹ <http://secunia.com/advisories/42367/>

⁹²⁹² http://httpd.apache.org/security/vulnerabilities_20.html

⁹²⁹³ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>

⁹²⁹⁴ <http://www.securityfocus.com/bid/49957>

⁹²⁹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3368>

⁹²⁹⁶ <http://iase.disa.mil/stigs/iavm-cve.html>

⁹²⁹⁷ <http://iase.disa.mil/stigs/iavm-cve.html>

⁹²⁹⁸ <http://iase.disa.mil/stigs/iavm-cve.html>

⁹²⁹⁹ <http://www.osvdb.org/76079>

⁹³⁰⁰ <http://rhn.redhat.com/errata/RHSA-2011-1391.html>

⁹³⁰¹ <http://rhn.redhat.com/errata/RHSA-2011-1392.html>

⁹³⁰² <http://secunia.com/advisories/46288/>

⁹³⁰³ <http://secunia.com/advisories/46414/>

⁹³⁰⁴ <http://secunia.com/advisories/48551/>

⁹³⁰⁵ <http://xforce.iss.net/xforce/xfdb/70336>

⁹³⁰⁶ http://httpd.apache.org/security/vulnerabilities_13.html

⁹³⁰⁷ http://httpd.apache.org/security/vulnerabilities_20.html

⁹³⁰⁸ http://httpd.apache.org/security/vulnerabilities_22.html

23.	Apache HTTPD: scoreboard parent DoS (CVE-2012-0031) (apache-httpd-cve-2012-0031)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Propust je otkriven u obradi scoreboard-a. Neprivilegovani child proces bi mogao da dovede do toga da parent proces krahira prilikom gašenja.	APPLE APPLE-SA-2012-09-19-2 ⁹³⁰⁹ BID 51407 ⁹³¹⁰ CVE CVE-2012-0031 ⁹³¹¹ IAVM 2012-A-0017 ⁹³¹² REDHAT RHSA-2012:0128 ⁹³¹³ SECUNIA 47410 ⁹³¹⁴ SECUNIA 48551 ⁹³¹⁵ URL1 ⁹³¹⁶ URL2 ⁹³¹⁷	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
24.	Apache HTTPD: mod_proxy_ajp remote DoS (CVE-2012-4557) (apache-httpd-cve-2012-4557)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ajp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven kada se mod_proxy_ajp koristi zajedno sa mod_proxy_balancer. Sa specifičnom konfiguracijom, udaljeni napadač može da pošalje zlonameran HTTP zahtev, prouzrokujući da backend server bude stavljen u status greške dok ne istekne vreme za ponovni pokušaj. To bi dovelo do odbijanja servisa.	CVE CVE-2012-4557 ⁹³¹⁸ DEBIAN DSA-2579 ⁹³¹⁹ URL1 ⁹³²⁰	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
25.	Apache HTTPD: mod_rewrite log escape filtering (CVE-2013-1862) (apache-httpd-cve-2013-1862)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_rewrite. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Modul mod_rewrite ne filtrira završne izlazne sekvence iz logova, što zlonamenom napadaču olakšava da ubace takve sekvence u završne	CVE CVE-2013-1862 ⁹³²¹ OVAL OVAL18790 ⁹³²² REDHAT RHSA-2013:0815 ⁹³²³ REDHAT RHSA-2013:1207 ⁹³²⁴ REDHAT RHSA-2013:1208 ⁹³²⁵ REDHAT RHSA-2013:1209 ⁹³²⁶ SECUNIA 55032 ⁹³²⁷ URL1 ⁹³²⁸ URL2 ⁹³²⁹	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.25 Ažurirati na Apache HTTPD version 2.2.25 Uraditi download a zatim

⁹³⁰⁹ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁹³¹⁰ <http://www.securityfocus.com/bid/51407>⁹³¹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0031>⁹³¹² <http://iase.disa.mil/stigs/iavm-cve.html>⁹³¹³ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁹³¹⁴ <http://secunia.com/advisories/47410/>⁹³¹⁵ <http://secunia.com/advisories/48551/>⁹³¹⁶ http://httpd.apache.org/security/vulnerabilities_20.html⁹³¹⁷ http://httpd.apache.org/security/vulnerabilities_22.html⁹³¹⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4557>⁹³¹⁹ <http://www.debian.org/security/2012/dsa-2579>⁹³²⁰ http://httpd.apache.org/security/vulnerabilities_22.html⁹³²¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1862>⁹³²² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18790>⁹³²³ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁹³²⁴ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁹³²⁵ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁹³²⁶ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁹³²⁷ <http://secunia.com/advisories/55032/>⁹³²⁸ http://httpd.apache.org/security/vulnerabilities_20.html

		emulatore koji sadrže ranjivosti koje se odnose na izlazne sekvence.			instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.25.tar.gz
26.	Apache HTTPD: mod_proxy_ajp remote DoS (CVE-2011-3348) (apache-httpd-cve-2011-3348)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Skenirani servis je osjetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ajp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven kada se mod_proxy_ajp koristi zajedno sa mod_proxy_balancer. Sa specifičnom konfiguracijom, udaljeni napadač može da pošalje zlonameran HTTP zahtev, prouzrokujući da backend server bude stavljen u status greške dok ne istekne vreme za ponovni pokušaj. To bi dovelo do odbijanja servisa.	APPLE APPLE-SA-2012-02-01-1 ⁹³³⁰ BID 49616 ⁹³³¹ CVE CVE-2011-3348 ⁹³³² IAVM 2012-B-0056 ⁹³³³ OVAL OVAL14941 ⁹³³⁴ OVAL OVAL18154 ⁹³³⁵ REDHAT RHSA-2011:1391 ⁹³³⁶ SECUNIA 46013 ⁹³³⁷ XF 69804 ⁹³³⁸ URL1 ⁹³³⁹	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.21 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.21.tar.gz
27.	Apache HTTPD: mod_setenvif .htaccess privilege escalation (CVE-2011-3607) (apache-httpd-cve-2011-3607)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_setenvif. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust preopterećenja je otkriven kada je omogućen modul mod_setenvif, što lokalnim korisnicima omogućava da dobiju privilegije preko fajla .htaccess.	APPLE APPLE-SA-2012-09-19-2 ⁹³⁴⁰ BID 50494 ⁹³⁴¹ CVE CVE-2011-3607 ⁹³⁴² IAVM 2012-A-0017 ⁹³⁴³ IAVM 2012-A-0152 ⁹³⁴⁴ OSVDB 76744 REDHAT RHSA-2012:0128 ⁹³⁴⁵ SECUNIA 45793 ⁹³⁴⁶ SECUNIA 48551 ⁹³⁴⁷ XF 71093 ⁹³⁴⁸ URL1 ⁹³⁴⁹ URL2 ⁹³⁵⁰	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
28.	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-4317) (apache-httpd-cve-2011-4317)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Skenirani servis je osjetljiv na ovu	APPLE APPLE-SA-2012-09-19-2 ⁹³⁵¹ CVE CVE-2011-4317 ⁹³⁵² IAVM 2012-A-0017 ⁹³⁵³ IAVM 2012-A-0152 ⁹³⁵⁴	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz

⁹³²⁹ http://httpd.apache.org/security/vulnerabilities_22.html⁹³³⁰ <http://lists.apple.com/archives/security-announce/2012/Feb/msg00000.html>⁹³³¹ <http://www.securityfocus.com/bid/49616>⁹³³² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3348>⁹³³³ <http://iase.disa.mil/stigs/iavm-cve.html>⁹³³⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14941>⁹³³⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18154>⁹³³⁶ <http://rhn.redhat.com/errata/RHSA-2011-1391.html>⁹³³⁷ <http://secunia.com/advisories/46013/>⁹³³⁸ <http://xforce.iss.net/xforce/xfdb/69804>⁹³³⁹ http://httpd.apache.org/security/vulnerabilities_22.html⁹³⁴⁰ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁹³⁴¹ <http://www.securityfocus.com/bid/50494>⁹³⁴² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3607>⁹³⁴³ <http://iase.disa.mil/stigs/iavm-cve.html>⁹³⁴⁴ <http://iase.disa.mil/stigs/iavm-cve.html>⁹³⁴⁵ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁹³⁴⁶ <http://secunia.com/advisories/45793/>⁹³⁴⁷ <http://secunia.com/advisories/48551/>⁹³⁴⁸ <http://xforce.iss.net/xforce/xfdb/71093>⁹³⁴⁹ http://httpd.apache.org/security/vulnerabilities_20.html⁹³⁵⁰ http://httpd.apache.org/security/vulnerabilities_22.html⁹³⁵¹ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁹³⁵² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4317>⁹³⁵³ <http://iase.disa.mil/stigs/iavm-cve.html>

		ranjivost samo ako je pokrenut modul mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy U određenim konfiguracijama koje koriste RewriteRule sa proxy flag-om ili ProxyPassMatch, udaljeni napadač bi mogao da primora reverzni proksi da se poveže sa proizvoljnim serverom i potencijalno objavi osetljive informacije sa internih web servera koje inače napadaču nisu direktno dostupne.	REDHAT RHSA-2012:0128 ⁹³⁵⁵ SECUNIA 48551 ⁹³⁵⁶ URL1 ⁹³⁵⁷		t/httpd/httpd-2.2.22.tar.gz
29.	Apache HTTPD: error responses can expose cookies (CVE-2012-0053) (apache-httpd-cve-2012-0053)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Propust je otkriven u difoltnom pogrešnom odgovoru za statusni kôd 400. Zlonamerni napadač bi mogao da iskoristi ovaj propust da objavi "httpOnly" kolačiće ako nije određen dokument custom ErrorDocument.	APPLE APPLE-SA-2012-09-19-2 ⁹³⁵⁸ BID 51706 ⁹³⁵⁹ CVE CVE-2012-0053 ⁹³⁶⁰ IAVM 2012-A-0017 ⁹³⁶¹ REDHAT RHSA-2012:0128 ⁹³⁶² SECUNIA 48551 ⁹³⁶³ URL1 ⁹³⁶⁴ URL2 ⁹³⁶⁵	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
30.	Apache HTTPD: XSS due to unescaped hostnames (CVE-2012-3499) (apache-httpd-cve-2012-3499)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut jedan od sledećih modula: mod_imagemap, mod_info, mod_ldap, mod_proxy_ftp, mod_status. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Različiti XSS propusti usled nenapuštenih host imena i URI-ja HTML output-a u mod_info, mod_status, mod_imagemap, mod_ldap i mod_proxy_ftp.	APPLE APPLE-SA-2013-09-12-1 ⁹³⁶⁶ CVE CVE-2012-3499 ⁹³⁶⁷ DEBIAN DSA-2637 ⁹³⁶⁸ REDHAT RHSA-2013:0815 ⁹³⁶⁹ REDHAT RHSA-2013:1207 ⁹³⁷⁰ REDHAT RHSA-2013:1208 ⁹³⁷¹ REDHAT RHSA-2013:1209 ⁹³⁷² SECUNIA 55032 ⁹³⁷³ URL1 ⁹³⁷⁴ URL2 ⁹³⁷⁵	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.24 Ažurirati na Apache HTTPD version 2.2.24 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz Apache HTTPD >= 2.4 and < 2.4.4 Ažurirati na Apache HTTPD version 2.4.4 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz

⁹³⁵⁴ <http://iase.disa.mil/stigs/iavm-cve.html>⁹³⁵⁵ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁹³⁵⁶ <http://secunia.com/advisories/48551/>⁹³⁵⁷ http://httpd.apache.org/security/vulnerabilities_22.html⁹³⁵⁸ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁹³⁵⁹ <http://www.securityfocus.com/bid/51706>⁹³⁶⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0053>⁹³⁶¹ <http://iase.disa.mil/stigs/iavm-cve.html>⁹³⁶² <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁹³⁶³ <http://secunia.com/advisories/48551/>⁹³⁶⁴ http://httpd.apache.org/security/vulnerabilities_20.html⁹³⁶⁵ http://httpd.apache.org/security/vulnerabilities_22.html⁹³⁶⁶ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁹³⁶⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3499>⁹³⁶⁸ <http://www.debian.org/security/2013/dsa-2637>⁹³⁶⁹ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁹³⁷⁰ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁹³⁷¹ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁹³⁷² <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁹³⁷³ <http://secunia.com/advisories/55032/>⁹³⁷⁴ http://httpd.apache.org/security/vulnerabilities_22.html⁹³⁷⁵ http://httpd.apache.org/security/vulnerabilities_24.html

31.	Apache HTTPD: XSS in mod_proxy_balancer (CVE-2012-4558) (apache-httpd-cve-2012-4558)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy_balancer. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. XSS propust je uticao na manager interfejs mod_proxy_balancer-a.	APPLE APPLE-SA-2013-09-12-1 ⁹³⁷⁶ CVE CVE-2012-4558 ⁹³⁷⁷ DEBIAN DSA-2637 ⁹³⁷⁸ REDHAT RHSA-2013:0815 ⁹³⁷⁹ REDHAT RHSA-2013:1207 ⁹³⁸⁰ REDHAT RHSA-2013:1208 ⁹³⁸¹ REDHAT RHSA-2013:1209 ⁹³⁸² URL1 ⁹³⁸³ URL2 ⁹³⁸⁴	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.24 Ažurirati na Apache HTTPD version 2.2.24 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz Apache HTTPD >= 2.4 and < 2.4.4 Ažurirati na Apache HTTPD version 2.4.4 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz
32.	Apache HTTPD: mod_dav crash (CVE-2013-1896) (apache-httpd-cve-2013-1896)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_dav_svn. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Slanje MERGE zahteva URI-ju koji obrađuje mod_dav_svn sa izvorom href (poslato kao deo zahteva XML) ciljajući na URI koji nije konfigurisan za DAV prouzrokuje segmentation fault (segfault).	CVE CVE-2013-1896 ⁹³⁸⁵ OVAL OVAL18835 ⁹³⁸⁶ REDHAT RHSA-2013:1156 ⁹³⁸⁷ REDHAT RHSA-2013:1207 ⁹³⁸⁸ REDHAT RHSA-2013:1208 ⁹³⁸⁹ REDHAT RHSA-2013:1209 ⁹³⁹⁰ SECUNIA 55032 ⁹³⁹¹ URL1 ⁹³⁹² URL2 ⁹³⁹³	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.25 Ažurirati na Apache HTTPD version 2.2.25 Apache HTTPD >= 2.4 and < 2.4.6 Ažurirati na Apache HTTPD version 2.4.6 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.6.tar.gz
33.	Apache HTTPD: XSS in mod_negotiation when untrusted uploads are supported (CVE-2012-2687) (apache-httpd-cve-2012-2687)	172.23.202.199:80 172.23.202.199:443 172.23.202.224:80 172.23.202.224:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_negotiation. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Moguće je ubaciti CRLF (Carriage Return and Line Feed) koji omogućava CRLF Injection napade (poznatih i kao HTTP Response	APPLE APPLE-SA-2013-09-12-1 ⁹³⁹⁴ BID 55131 ⁹³⁹⁵ CVE CVE-2012-2687 ⁹³⁹⁶ IAVM 2012-A-0139 ⁹³⁹⁷ REDHAT RHSA-2012:1591 ⁹³⁹⁸ REDHAT RHSA-2012:1592 ⁹³⁹⁹ REDHAT RHSA-2012:1594 ⁹⁴⁰⁰ REDHAT RHSA-2013:0130 ⁹⁴⁰¹	Umeren	Apache HTTPD >= 2.2 and < 2.2.23 Ažurirati na Apache HTTPD version 2.2.23 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz Apache HTTPD >= 2.4 and < 2.4.3 Ažurirati na Apache HTTPD version 2.4.3 Uraditi download a zatim

⁹³⁷⁶ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁹³⁷⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4558>⁹³⁷⁸ <http://www.debian.org/security/2013/dsa-2637>⁹³⁷⁹ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁹³⁸⁰ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁹³⁸¹ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁹³⁸² <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁹³⁸³ http://httpd.apache.org/security/vulnerabilities_22.html⁹³⁸⁴ http://httpd.apache.org/security/vulnerabilities_24.html⁹³⁸⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1896>⁹³⁸⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18835>⁹³⁸⁷ <http://rhn.redhat.com/errata/RHSA-2013-1156.html>⁹³⁸⁸ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁹³⁸⁹ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁹³⁹⁰ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁹³⁹¹ <http://secunia.com/advisories/55032/>⁹³⁹² http://httpd.apache.org/security/vulnerabilities_22.html⁹³⁹³ http://httpd.apache.org/security/vulnerabilities_24.html⁹³⁹⁴ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁹³⁹⁵ <http://www.securityfocus.com/bid/55131>⁹³⁹⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2687>⁹³⁹⁷ <http://iase.disa.mil/stigs/iavm-cve.html>⁹³⁹⁸ <http://rhn.redhat.com/errata/RHSA-2012-1591.html>⁹³⁹⁹ <http://rhn.redhat.com/errata/RHSA-2012-1592.html>⁹⁴⁰⁰ <http://rhn.redhat.com/errata/RHSA-2012-1594.html>

		Splitting) za sajtove koji koriste mod_negotiation, omogućavajući neproverene upload-ove na lokacije na kojima je omogućen MultiViews (višestruko pregledanje). Ovaj problem je poznat i kao CVE-2008-0455.	SECUNIA 50894 ⁹⁴⁰² SECUNIA 51607 ⁹⁴⁰³ URL1 ⁹⁴⁰⁴ URL2 ⁹⁴⁰⁵		instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.3.tar.gz
34.	Weak Cryptographic Key (weak-crypto-key)	172.23.202.199:443 172.23.202.224:443 Dužina RSA modula u sertifikatu X.509: 1024 bita (manje od 2047 bita). Dužina tajnog ključa koju koristi kriptografski algoritam određuje najviši mogući nivo bezbednosti. Nedavno otkriveni teoretski napadi i sve napredniji hardware stalno snižavaju nivo bezbednosti. Zbog ovoga, od 2011-te godine, vladine, akademske i privatne organizacije koje se bave kriptografskom bezbednošću, kao National Institute of Standards and Technology (NIST), European Network of Excellence in Cryptology II (ECRYPT II), daju sledeće preporuke da bi se obezbedila kratkoročna ili duža bezbednost čak i od najbolje opremljenih napadača (npr. agencije inteligencije): Dužine simetričnih tajnih ključeva od minimum 80-112 bitova. Dužine eliptičnih tajnih ključeva od minimum 160-224 bitova. Dužine RSA tajnih ključeva od minimum 1248-2048 bitova. CA/Browser Forum Extended Validation (EV) Guidelines izričito zahteva da dužina tajnog ključa bude minimum 2048 bitova. Ispitivanja pokazuju da je izrada 1024-bitnog RSA modula praktično dostupna. Dužine DSA tajnih ključeva od minimum 2048 bitova. Dodatno, od 2014-te, Certificate Authority/Browser Forum zahteva da SSL sertifikati i kôd potpisivanje više ne podržavaju 1024-bitne RSA tajne ključeve.	URL1 ⁹⁴⁰⁶ URL2 ⁹⁴⁰⁷ URL3 ⁹⁴⁰⁸ URL4 ⁹⁴⁰⁹ URL5 ⁹⁴¹⁰ URL6 ⁹⁴¹¹ URL7 ⁹⁴¹²	Umeren	Slab tajni ključ se koristi u sertifikatu X.509 (npr. za HTTPS server), da generiše duži tajni ključ i osveži sertifikat. Pogledati NIST's preporuke za kriptografske algoritme i dužine tajnih ključeva. ⁹⁴¹³
35.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za	URL1 ⁹⁴¹⁴ URL2 ⁹⁴¹⁵ URL3 ⁹⁴¹⁶	Umeren	Onemogućavanje TCP timestamp odgovora na Linux OS. Podesiti

⁹⁴⁰¹ <http://rhn.redhat.com/errata/RHSA-2013-0130.html>⁹⁴⁰² <http://secunia.com/advisories/50894/>⁹⁴⁰³ <http://secunia.com/advisories/51607/>⁹⁴⁰⁴ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁴⁰⁵ http://httpd.apache.org/security/vulnerabilities_24.html⁹⁴⁰⁶ <http://www.symantec.com/page.jsp?id=1024-bit-certificate-support>⁹⁴⁰⁷ <http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf>⁹⁴⁰⁸ http://csrc.nist.gov/groups/ST/toolkit/key_management.html⁹⁴⁰⁹www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2011_2_AlgoKatpdf.pdf⁹⁴¹⁰ <http://www.ecrypt.eu.org/documents/D.SPA.17.pdf>⁹⁴¹¹ <http://www.keylength.com/>⁹⁴¹² http://www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf⁹⁴¹³ <http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf>⁹⁴¹⁴ http://www.forensicswiki.org/wiki/TCP_timestamps⁹⁴¹⁵ <http://www.ietf.org/rfc/rfc1323.txt>

		procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.			net.ipv4.tcp_timestamps vrednost na sledećem ključu na 0 pokretanjem sledeće komande: sysctl -w net.ipv4.tcp_timestamps=0 Dodatno, sledeću vrednost u difoltnom sysctl konfiguracionom fajlu, generally sysctl.conf: net.ipv4.tcp_timestamps=0

Tabela 132. Linux OS sa IP adresama 172.23.202.198, 172.23.202.223 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.198		OS: Fedora 15 x86, fedora15x86			30
IP adresa: 172.23.202.223		OS: Fedora 15 x64, fedora15x64			30
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mismatch)	172.23.202.198:443 172.23.202.223:443 Rubrika u sertifikatu X.509 sa uobičajenim nazivom subjekta (CN) ne poklapa se sa imenom pojedinca koje je navedeno u sertifikatu. Pre izdavanja sertifikata, Certification Authority (CA) mora da proveri identitet pojedinca koji potražuje sertifikat, kako je navedeno u CA-ovom Certification Practice Statement (CPS). Zbog toga, uobičajene procedure validacije sertifikata zahtevaju da rubrika sertifikata sa CN subjektom odgovara pravom imenu pojedinca koji prikazuje sertifikat. Na primer, u sertifikatu prikazanom na „https://www.example.com/“, naziv subjekta (CN) treba da bude „www.example.com“. U cilju otkrivanja i sprečavanja napada prisluškivanja, validnost sertifikata mora da bude overena, jer bi u suprotnom napadač mogao da otpočne napad preko posrednika i da stekne potpunu kontrolu nad protokom podataka. Od posebne važnosti je validnost naziva subjekta (CN), koji treba da se poklapa sa imenom pojedinca (imenom host-a). Neodgovarajući CN se najčešće javlja usled greške u konfiguraciji, iako on takođe može da ukazuje na to da se sprovodi napad preko posrednika.		Ozbiljan	Rubrika sa uobičajenim nazivom subjekta (CN) u sertifikatu X.509 treba da bude podešena da sadrži ime pojedinca koji prikazuje sertifikat (npr. ime hosta). To se postiže izradom novog sertifikata, koji najčešće potpisuje Certification Authority (CA), koji je od poverenja kako za klijenta, tako i za server.
2.	FTP access with ftp account (ftp-generic-0001)	172.23.202.198:21 172.23.202.223:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisničkim ID-jem „ftp“ i šifrom „ftp“. Dosadašnja praksa je pokazala da treba ukloniti	CVE CVE-1999-0497 ⁹⁴¹⁷	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko to nije kritično za dalje funkcionisanje sistema. U suprotnom, treba promeniti lozinku u nedifoltnu

⁹⁴¹⁶ <http://uptime.netcraft.com/>⁹⁴¹⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>

		difoltna naloge, ako je to moguće. Za naloge koje zahteva sistem, treba promeniti difoltnu šifru.			vrednost.
3.	FTP access with anonymous account (ftp-generic-0002)	172.23.202.198:21 172.23.202.223:21 Mnogi FTP serveri podržavaju difoltni nalog sa korisničkim ID-jem „anonymous“ i šifrom „ftp@“. Dosadašnja praksa je pokazala da treba ukloniti difoltna naloge, ako je to moguće. Za naloge koje zahteva sistem, treba promeniti difoltnu šifru.	CVE CVE-1999-0497 ⁹⁴¹⁸	Ozbiljan	Ukloniti ili onemogućiti nalog ukoliko to nije kritično za dalje funkcionisanje sistema. U suprotnom, treba promeniti lozinku u nedifoltnu vrednost.
4.	FTP server does not support AUTH command (ftp-generic-0007)	172.23.202.198:21 172.23.202.223:21 FTP klijenti po difoltu šalju FTP server-u poverljive podatke (korisnički ID i šifra) u vidu čitkog teksta. Ova okolnost dozvoljava zlonamernim korisnicima da presreću poverljive podatke ukoliko prisluškuju vezu. Noviji FTP serveri podržavaju AUTH komandu, koja omogućava dodatne opcije autentifikacije, kao što su TLS, Kerberos, GSSAPI itd. Ona se može koristiti za sprečavanje prisluškivanja na FTP vezama.		Ozbiljan	Ažurirati/preći na FTP server koji podržava AUTH komandu.
5.	Browsable web directory (http-generic-browsable-dir)	172.23.202.198:80 172.23.202.223:80 172.23.202.198:443 172.23.202.223:443 Otkriven je direktorijum na web serveru koji može biti pretraživan, što znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice - spajdering (prateći hiperlinkove), ili -kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute force napadom na liste uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skrivena“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice. Primer: http://172.23.202.198/icons/ 4: <title>Index of /icons</title> 5: </head> 6: <body> 7: Index of /icons 8: ...CO]"></th><th>Name</th><th><a href="?C=M;O=A...		Ozbiljan	Za Apache: onemogućiti pretraživanje direktorijuma mreže za sve direktorijume i poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume. Za Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote: Onemogućiti pretraživanje direktorijuma za sve direktorijume i poddirektorijume. Uključiti Tomcat-ov web.xml file. U odeljku „default“, promeniti parametar „listings“ iz „true“ u „false“.

⁹⁴¹⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497>

					Restartovati server. Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripta i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume.
6.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	TCP reset with incorrect sequence number triggered this fault on 172.23.202.198:80 172.23.202.223:80 Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	OSVDB 4030 ⁹⁴¹⁹ BID: 10183 ⁹⁴²⁰ CERT-VN: 415294 ⁹⁴²¹ CVE CVE-2004-0230 ⁹⁴²² MS: MS05-019 ⁹⁴²³ MS: MS06-064 ⁹⁴²⁴ NETBSD: NetBSD-SA2004-006 ⁹⁴²⁵ OVAL: OVAL2689 ⁹⁴²⁶ OVAL: OVAL270 ⁹⁴²⁷ OVAL OVAL3508 ⁹⁴²⁸ OVAL OVAL4791 ⁹⁴²⁹ OVAL OVAL5711 ⁹⁴³⁰ SECUNIA: 11440 ⁹⁴³¹ SECUNIA 11458 ⁹⁴³² SECUNIA: 22341 ⁹⁴³³ SGI 20040403-01-A ⁹⁴³⁴ XF tcp-rst-dos(15886) ⁹⁴³⁵ URL1 ⁹⁴³⁶ URL2 ⁹⁴³⁷	Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC 2385 ⁹⁴³⁸ . Ono je napravljeno da smanji opasnost od određenih napada na BGP, kao što su TCP reseti.
7.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podesi na jedinstvenu vrednost i da se koristi u rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da	BID 4314 ⁹⁴³⁹ CVE CVE-2002-0510 ⁹⁴⁴⁰ XF linux-udp-fingerprint(8588) ⁹⁴⁴¹	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili pak ranjivost koju treba popravljati, tako da ne postoje rešenja koja se mogu kupiti. Jedino se može postaviti fajervol ili neka druga sprava za filtriranje

⁹⁴¹⁹ <http://www.osvdb.org/4030>⁹⁴²⁰ <http://www.securityfocus.com/bid/10183>⁹⁴²¹ <http://www.kb.cert.org/vuls/id/415294>⁹⁴²² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁹⁴²³ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁹⁴²⁴ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁹⁴²⁵ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁹⁴²⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>⁹⁴²⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>⁹⁴²⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>⁹⁴²⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>⁹⁴³⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>⁹⁴³¹ <http://secunia.com/advisories/11440/>⁹⁴³² <http://secunia.com/advisories/11458/>⁹⁴³³ <http://secunia.com/advisories/22341/>⁹⁴³⁴ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>⁹⁴³⁵ <http://xforce.iss.net/xforce/xfdb/15886>⁹⁴³⁶ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁹⁴³⁷ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>⁹⁴³⁸ <http://www.ietf.org/rfc/rfc2385.txt>⁹⁴³⁹ <http://www.securityfocus.com/bid/4314>⁹⁴⁴⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>⁹⁴⁴¹ <http://xforce.iss.net/xforce/xfdb/8588>

		fingerprint-uje operativni sistem.			između napadnutog i neprijateljskog napada koji je u mogućnosti da randomizuje IP ID-jeve.
8.	Apache HTTPD: apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpdcve-2011-0419)	172.23.202.198:80 172.23.202.198:443 172.23.202.223:80 172.23.202.223:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_autoindex. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_fnmatch() u sklopu APR biblioteke. Ako je omogućen mod_autoindex, a indeksi direktorijuma mod_autoindex su sadržavali fajlove sa dovoljno dugim nazivima, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do preterane upotrebe CPU-a. Ovo bi moglo da bude iskorišćeno u napadu odbijanja servisa. Zahvaljujući Maksymilian Arciemowicz prijavljen je ovaj propust.	CVE CVE-2011-0419 ⁹⁴⁴² DEBIAN DSA-2237 ⁹⁴⁴³ IAVM 2012-B-0056 ⁹⁴⁴⁴ OVAL OVAL14638 ⁹⁴⁴⁵ OVAL OVAL14804 ⁹⁴⁴⁶ REDHAT RHSA-2011:0896 ⁹⁴⁴⁷ REDHAT RHSA-2011:0897 ⁹⁴⁴⁸ REDHAT RHSA-2011:0507 ⁹⁴⁴⁹ SECUNIA 44490 ⁹⁴⁵⁰ SECUNIA 44564 ⁹⁴⁵¹ SECUNIA 44574 ⁹⁴⁵² URL1 ⁹⁴⁵³	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.19 Ažurirati na Apache HTTPD version 2.2.19 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.19.tar.gz
9.	Self-signed TLS/SSL certificate (ssl-self-signed-certificate)	172.23.202.198:443 172.23.202.223:443 TLS/SSL-a sertifikat servera je samopotpisan. Samopotpisani sertifikati po difoltu nisu od poverenja, naročito zato što napadi na TLS/SSL preko posrednika obično koriste samopotpisane sertifikate da prisluškuju TLS/SSL veze.		Ozbiljan	Nabaviti novi TLS/SSL serverov sertifikat koji NIJE samopotpisan i instalirati ga na server. Precizna uputstva za dobijanje novog sertifikata zavise od zahteva organizacije. Uopšteno, treba napraviti zahtev za sertifikat i taj zahtev sačuvati kao fajl. Ovaj fajl se zatim šalje Certificate Authority-ju (CA) na obradu. Organizacija možda poseduje sopstveni interni Certificate Authority. U suprotnom, potrebno je platiti sertifikat iz spoljnog poverljivog Certificate Authority-ja, kao što su Thawte, Verisign .
10.	HTTP TRACE Method Enabled (http-trace-method-enabled)	172.23.202.198:80 172.23.202.223:80 172.23.202.198:443 172.23.202.223:443	CERT-VN 867593 ⁹⁴⁵⁴ OSVDB 35511 ⁹⁴⁵⁵ OSVDB 3726 ⁹⁴⁵⁶ SECUNIA 10726 ⁹⁴⁵⁷ SECUNIA 17334 ⁹⁴⁵⁸	Ozbiljan	Apache Onemogućiti HTTP TRACE metodu za Apache. Novije verzije Apache-a (1.3.34 i 2.0.55 i novije)

⁹⁴⁴² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419>⁹⁴⁴³ <http://www.debian.org/security/2011/dsa-2237>⁹⁴⁴⁴ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁴⁴⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14638>⁹⁴⁴⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14804>⁹⁴⁴⁷ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁹⁴⁴⁸ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>⁹⁴⁴⁹ <http://rhn.redhat.com/errata/RHSA-2011-0507.html>⁹⁴⁵⁰ <http://secunia.com/advisories/44490/>⁹⁴⁵¹ <http://secunia.com/advisories/44564/>⁹⁴⁵² <http://secunia.com/advisories/44574/>⁹⁴⁵³ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁴⁵⁴ <http://www.kb.cert.org/vuls/id/867593>⁹⁴⁵⁵ <http://www.osvdb.org/35511>⁹⁴⁵⁶ <http://www.osvdb.org/3726>⁹⁴⁵⁷ <http://secunia.com/advisories/10726/>

		HTTP TRACE metoda se obično koristi da uzvрати potpuni HTTP zahtev klijentu koji ga zahteva, u cilju debagovanja proxy servera. Napadač bi mogao da kreira web stranicu koristeći XMLHTTP, ActiveX ili XMLDOM da natera klijenta da pošalje TRACE zahtev i da sačuva klijenove kolačiće. Kao posledica može da se javi XSS napad. Primer: 172.23.202.193:80 Running vulnerable HTTP service. https://172.23.202.198/ 1: TRACE / HTTP/1.1 2: Host: 172.23.202.198:443 3: Cookie: vulnerable=yes	SECUNIA 21802⁹⁴⁵⁹ SECUNIA 25636⁹⁴⁶⁰ CVE CVE-2004-2320⁹⁴⁶¹ CVE CVE-2004-2763⁹⁴⁶² CVE CVE-2005-3398⁹⁴⁶³ CVE CVE-2006-4683⁹⁴⁶⁴ CVE CVE-2007-3008⁹⁴⁶⁵ CVE CVE-2008-7253⁹⁴⁶⁶ CVE CVE-2009-2823⁹⁴⁶⁷ CVE CVE-2010-0386⁹⁴⁶⁸ OSVDB 877⁹⁴⁶⁹ SUN 50603⁹⁴⁷⁰ BID 9561⁹⁴⁷¹ URL1⁹⁴⁷² URL2⁹⁴⁷³		omogućuju konfiguracionu direktivu koja se zove TraceEnable. Da bi se odbili TRACE zahtevi, dodaje se sledeći red u konfiguraciju servera: TraceEnable off Za starije verzije Apache web servera, koristiti modul mod_rewrite da bi se odbili TRACE zahteve: RewriteEngine On RewriteCond %{REQUEST_METHOD} ^TRACE RewriteRule .* - [F]
11.	Database Open Access (database-open-access)	172.23.202.198:3306 172.23.202.223:3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7.	URL1 ⁹⁴⁷⁴	Umeren	Konfigurisati server baze podataka tako da dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenju od DMZ.
12.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatišu slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	CVE CVE-1999-0524⁹⁴⁷⁵ OSVDB 95⁹⁴⁷⁶ XF icmp-netmask(306)⁹⁴⁷⁷ XF icmp-timestamp(322)⁹⁴⁷⁸	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost

⁹⁴⁵⁸ <http://secunia.com/advisories/17334/>⁹⁴⁵⁹ <http://secunia.com/advisories/21802/>⁹⁴⁶⁰ <http://secunia.com/advisories/25636/>⁹⁴⁶¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2320>⁹⁴⁶² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2763>⁹⁴⁶³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-3398>⁹⁴⁶⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-4683>⁹⁴⁶⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3008>⁹⁴⁶⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-7253>⁹⁴⁶⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2823>⁹⁴⁶⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0386>⁹⁴⁶⁹ <http://osvdb.org/877>⁹⁴⁷⁰ <https://sunsolve.sun.com/search/document.do?assetkey=1-22-50603-1> pristupljeno 18.12.2011⁹⁴⁷¹ <http://www.securityfocus.com/bid/9561>⁹⁴⁷² <http://www.apacheweek.com/issues/03-01-24#news>⁹⁴⁷³ <http://www.kb.cert.org/vuls/id/867593>⁹⁴⁷⁴ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf⁹⁴⁷⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁹⁴⁷⁶ <http://www.osvdb.org/95>⁹⁴⁷⁷ <http://xforce.iss.net/xforce/xfdb/306>⁹⁴⁷⁸ <http://xforce.iss.net/xforce/xfdb/322>

13.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1⁹⁴⁷⁹ URL2⁹⁴⁸⁰ URL3⁹⁴⁸¹	Umeren	Onemogućavanje TCP timestamp odgovora na Linux OS. Podesiti net.ipv4.tcp_timestamps vrednost na sledećem ključu na 0 pokretanjem sledeće komande: sysctl -w net.ipv4.tcp_timestamps=0 Dodatno, sledeću vrednost u difoltnom sysctl konfiguracionom fajlu, generally sysctl.conf: net.ipv4.tcp_timestamps=0
14.	WebDAV Extensions are Enabled (http-generic-webdav-enabled)	172.23.202.198:80 172.23.202.223:80 172.23.202.198:443 172.23.202.223:443 WebDAV je skup ekstenzija za HTTP protokol koji omogućava korisnicima da zajednički edituju i obrađuju fajlove na udaljenim web serverima. Mnogi web serveri po difoltu omogućavaju WebDAV ekstenzije, čak i kada nisu potrebne. S obzirom na dodatnu složenost, dosadašnja praksa je pokazala da treba onemogućiti WebDAV ukoliko se trenutno ne koristi.		Umeren	Apache: Potrebno je onemogućiti WebDAV (eng. Web-based Distributed Authoring and Versioning) za Apache. Proveriti da li je mod_dav modul isključen ili utvrditi da li postoji zahtevana autentifikacija na direktorijumima nad kojima se zahteva DAV.
15.	Apache HTTPD: insecure LD_LIBRARY_PATH handling (CVE-2012-0883) (apache-httpd-cve-2012-0883)	172.23.202.198:80 172.23.202.198:443 172.23.202.223:80 172.23.202.223:443 Otkrivena je nebezbedna obrada rute LD_LIBRARY_PATH koja bi mogla da dovede do toga da direktorijum koji trenutno radi traži DSO-ove. Ovo bi lokalnom korisniku omogućilo da izvrši kôd kao root ako je administrator pokrenuo apacheclt sa nepoverljivog direktorijuma.	APPLE APPLE-SA-2013-09-12-1⁹⁴⁸² CVE CVE-2012-0883⁹⁴⁸³ SECUNIA 48849⁹⁴⁸⁴ URL1⁹⁴⁸⁵ URL2⁹⁴⁸⁶	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.23 Ažurirati na Apache HTTPD version 2.2.23 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz Apache HTTPD >= 2.4 and < 2.4.2 Ažurirati na Apache HTTPD version 2.4.2 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.2.tar.gz
16.	X.509 Server Certificate Is Invalid/Expired (tls-server-cert-expired)	Sertifikat X.509 na TLS/SSL serveru sadrži početni datum iz budućnosti ili je istekao. Proveriti proof za više detalja.		Ozbiljan	Nabaviti novi TLS/SSL serverov sertifikat i instalirati ga na server. Precizna uputstva za dobijanje novog sertifikata zavise od zahteva organizacije. Uopšteno, treba napraviti zahtev za sertifikat i taj zahtev sačuvati kao fajl. Ovaj fajl se zatim šalje Certificate Authority-ju (CA) na obradu. Proveriti da li su

⁹⁴⁷⁹ http://www.forensicswiki.org/wiki/TCP_timestamps⁹⁴⁸⁰ <http://www.ietf.org/rfc/rfc1323.txt>⁹⁴⁸¹ <http://uptime.netcraft.com/>⁹⁴⁸² <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁹⁴⁸³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0883>⁹⁴⁸⁴ <http://secunia.com/advisories/48849/>⁹⁴⁸⁵ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁴⁸⁶ http://httpd.apache.org/security/vulnerabilities_24.html

					početni i završni datumi na novom sertifikatu validni. Organizacija možda poseduje sopstveni interni Certificate Authority. U suprotnom, potrebno je platiti sertifikat iz spoljnog poverljivog Certificate Authority-ja. Nakon prijema novog sertifikata od Certificate Authority-ja, potrebno je instalirati ga na TLS/SSL server. Tačna uputstva za instaliranje su za svaki proizvod različita. Proveriti njihovu dokumentaciju.
17.	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368) (apache-httpd-cve-2011-3368)	172.23.202.198:80 172.23.202.198:443 172.23.202.223:80 172.23.202.223:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja prisustva mod_proxy modula. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy. Zlonamerni napadač bi mogao da iskoristi ovaj propust na takav način da primora proxy proces da se poveže sa proizvoljnim serverom i potencijalno objavi osetljive informacije sa internih web servera koje inače napadaču nisu direktno dostupne. Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/	APPLE APPLE-SA-2012-09-19-2 ⁹⁴⁸⁷ BID 49957 ⁹⁴⁸⁸ CVE CVE-2011-3368 ⁹⁴⁸⁹ IAVM 2012-A-0017 ⁹⁴⁹⁰ IAVM 2012-A-0152 ⁹⁴⁹¹ IAVM 2012-B-0056 ⁹⁴⁹² OSVDB 76079 ⁹⁴⁹³ REDHAT 2011:1391 ⁹⁴⁹⁴ RHSA-2011:1392 ⁹⁴⁹⁵ SECUNIA 46288 ⁹⁴⁹⁶ SECUNIA 46414 ⁹⁴⁹⁷ SECUNIA 48551 ⁹⁴⁹⁸ XF 70336 ⁹⁴⁹⁹ URL1 ⁹⁵⁰⁰ URL2 ⁹⁵⁰¹ URL3 ⁹⁵⁰²	Ozbiljan	Apache HTTPD >= 1.3 and < 2 Primeniti zakrpu za CVE-2011-3368 to 1.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
18.	Apache HTTPD: scoreboard parent DoS	172.23.202.198:80 172.23.202.198:443 172.23.202.223:80	APPLE APPLE-SA-2012-09-19-2 ⁹⁵⁰³ BID 51407 ⁹⁵⁰⁴	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache

⁹⁴⁸⁷ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁹⁴⁸⁸ <http://www.securityfocus.com/bid/49957>⁹⁴⁸⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3368>⁹⁴⁹⁰ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁴⁹¹ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁴⁹² <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁴⁹³ <http://www.osvdb.org/76079>⁹⁴⁹⁴ <http://rhn.redhat.com/errata/RHSA-2011-1391.html>⁹⁴⁹⁵ <http://rhn.redhat.com/errata/RHSA-2011-1392.html>⁹⁴⁹⁶ <http://secunia.com/advisories/46288/>⁹⁴⁹⁷ <http://secunia.com/advisories/46414/>⁹⁴⁹⁸ <http://secunia.com/advisories/48551/>⁹⁴⁹⁹ <http://xforce.iss.net/xforce/xfdb/70336>⁹⁵⁰⁰ http://httpd.apache.org/security/vulnerabilities_13.html⁹⁵⁰¹ http://httpd.apache.org/security/vulnerabilities_20.html⁹⁵⁰² http://httpd.apache.org/security/vulnerabilities_22.html⁹⁵⁰³ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>

	(CVE-2012-0031) (apache-httpd-cve-2012-0031)	172.23.202.223:443 Propust je otkriven u obradi scoreboard-a. Neprivilegovani child proces bi mogao da dovede do toga da parent proces krahira prilikom gašenja.	CVE CVE-2012-0031 ⁹⁵⁰⁵ IAVM 2012-A-0017 ⁹⁵⁰⁶ REDHAT RHSA-2012:0128 ⁹⁵⁰⁷ SECUNIA 47410 ⁹⁵⁰⁸ SECUNIA 48551 ⁹⁵⁰⁹ URL1 ⁹⁵¹⁰ URL2 ⁹⁵¹¹		HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
19.	Apache HTTPD: mod_proxy_ajp remote DoS (CVE-2012-4557) (apache-httpd-cve-2012-4557)	172.23.202.198:80 172.23.202.198:443 172.23.202.223:80 172.23.202.223:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ajp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Mod_proxy_ajp će vratiti pogrešan kôd statusa ako naiđe na grešku, prouzrokujući da backend server bude stavljen u status greške dok ne istekne vreme za ponovni pokušaj. Udaljeni napadač bi mogao da pošalje zlonameran zahtev da bi pokrenuo ovaj problem, što bi dovelo do privremenog odbijanja servisa.	CVE CVE-2012-4557 ⁹⁵¹² DEBIAN DSA-2579 ⁹⁵¹³ URL1 ⁹⁵¹⁴	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
20.	Apache HTTPD: mod_rewrite log escape filtering (CVE-2013-1862) (apache-httpd-cve-2013-1862)	172.23.202.198:80 172.23.202.198:443 172.23.202.223:80 172.23.202.223:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_rewrite. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Modul mod_rewrite ne filtrira završne izlazne sekvence iz logova, što zlonamenrom napadaču olakšava da ubace takve sekvence u završne emulatore koji sadrže ranjivosti koje se odnose na izlazne sekvence.	CVE CVE-2013-1862 ⁹⁵¹⁵ OVAL OVAL18790 ⁹⁵¹⁶ REDHAT RHSA-2013:0815 ⁹⁵¹⁷ REDHAT RHSA-2013:1207 ⁹⁵¹⁸ REDHAT RHSA-2013:1208 ⁹⁵¹⁹ REDHAT RHSA-2013:1209 ⁹⁵²⁰ SECUNIA 55032 ⁹⁵²¹ URL1 ⁹⁵²² URL2 ⁹⁵²³	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.25 Ažurirati na Apache HTTPD version 2.2.25 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.25.tar.gz

⁹⁵⁰⁴ <http://www.securityfocus.com/bid/51407>⁹⁵⁰⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0031>⁹⁵⁰⁶ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁵⁰⁷ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁹⁵⁰⁸ <http://secunia.com/advisories/47410/>⁹⁵⁰⁹ <http://secunia.com/advisories/48551/>⁹⁵¹⁰ http://httpd.apache.org/security/vulnerabilities_20.html⁹⁵¹¹ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁵¹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4557>⁹⁵¹³ <http://www.debian.org/security/2012/dsa-2579>⁹⁵¹⁴ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁵¹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1862>⁹⁵¹⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18790>⁹⁵¹⁷ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁹⁵¹⁸ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁹⁵¹⁹ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁹⁵²⁰ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁹⁵²¹ <http://secunia.com/advisories/55032/>⁹⁵²² http://httpd.apache.org/security/vulnerabilities_20.html⁹⁵²³ http://httpd.apache.org/security/vulnerabilities_22.html

21.	Apache HTTPD: mod_proxy_ajp remote DoS (CVE-2011-3348) (apache-httpd-cve-2011-3348)	172.23.202.198:80 172.23.202.198:443 172.23.202.223:80 172.23.202.223:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ajp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven kada se mod_proxy_ajp koristi zajedno sa mod_proxy_balancer. Sa specifičnom konfiguracijom, udaljeni napadač može da pošalje zlonameran HTTP zahtev, prouzrokujući da backend server bude stavljen u status greške dok ne istekne vreme za ponovni pokušaj. To bi dovelo do odbijanja servisa.	APPLE APPLE-SA-2012-02-01-1 ⁹⁵²⁴ BID 49616 ⁹⁵²⁵ CVE CVE-2011-3348 ⁹⁵²⁶ IAVM 2012-B-0056 ⁹⁵²⁷ OVAL OVAL14941 ⁹⁵²⁸ OVAL OVAL18154 ⁹⁵²⁹ REDHAT RHSA-2011:1391 ⁹⁵³⁰ SECUNIA 46013 ⁹⁵³¹ XF 69804 ⁹⁵³² URL1 ⁹⁵³³	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.21 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.21.tar.gz
22.	Apache HTTPD: mod_setenvif .htaccess privilege escalation (CVE-2011-3607) (apache-httpd-cve-2011-3607)	172.23.202.198:80 172.23.202.198:443 172.23.202.223:80 172.23.202.223:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_setenvif. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust preopterećenja je otkriven kada je omogućen modul mod_setenvif, što lokalnim korisnicima omogućava da dobiju privilegije preko fajla .htaccess.	APPLE APPLE-SA-2012-09-19-2 ⁹⁵³⁴ BID 50494 ⁹⁵³⁵ CVE CVE-2011-3607 ⁹⁵³⁶ IAVM 2012-A-0017 ⁹⁵³⁷ IAVM 2012-A-0152 ⁹⁵³⁸ OSVDB 76744 REDHAT RHSA-2012:0128 ⁹⁵³⁹ SECUNIA 45793 ⁹⁵⁴⁰ SECUNIA 48551 ⁹⁵⁴¹ XF 71093 ⁹⁵⁴² URL1 ⁹⁵⁴³ URL2 ⁹⁵⁴⁴	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
23.	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-4317) (apache-httpd-cve-2011-4317)	172.23.202.198:80 172.23.202.198:443 172.23.202.223:80 172.23.202.223:443 Skenirani servis je osetljiv na ovu ranjivost samo ako je pokrenut modul mod_proxy. Proveriti konfiguraciju	APPLE APPLE-SA-2012-09-19-2 ⁹⁵⁴⁵ CVE CVE-2011-4317 ⁹⁵⁴⁶ IAVM 2012-A-0017 ⁹⁵⁴⁷ IAVM 2012-A-0152 ⁹⁵⁴⁸ REDHAT RHSA-2012:0128 ⁹⁵⁴⁹	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.22 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz

⁹⁵²⁴ <http://lists.apple.com/archives/security-announce/2012/Feb/msg00000.html>⁹⁵²⁵ <http://www.securityfocus.com/bid/49616>⁹⁵²⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3348>⁹⁵²⁷ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁵²⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14941>⁹⁵²⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18154>⁹⁵³⁰ <http://rhn.redhat.com/errata/RHSA-2011-1391.html>⁹⁵³¹ <http://secunia.com/advisories/46013/>⁹⁵³² <http://xforce.iss.net/xforce/xfdb/69804>⁹⁵³³ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁵³⁴ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁹⁵³⁵ <http://www.securityfocus.com/bid/50494>⁹⁵³⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3607>⁹⁵³⁷ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁵³⁸ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁵³⁹ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁹⁵⁴⁰ <http://secunia.com/advisories/45793/>⁹⁵⁴¹ <http://secunia.com/advisories/48551/>⁹⁵⁴² <http://xforce.iss.net/xforce/xfdb/71093>⁹⁵⁴³ http://httpd.apache.org/security/vulnerabilities_20.html⁹⁵⁴⁴ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁵⁴⁵ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁹⁵⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4317>⁹⁵⁴⁷ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁵⁴⁸ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁵⁴⁹ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>

		web servera radi utvrđivanja ove mogućnosti. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy U određenim konfiguracijama koje koriste RewriteRule sa proxy flag-om ili ProxyPassMatch, udaljeni napadač bi mogao da primora reverzni proksi da se poveže sa proizvoljnim serverom i potencijalno objavi osetljive informacije sa internih web servera koje inače napadaču nisu direktno dostupne.	SECUNIA 48551 ⁹⁵⁵⁰ URL1 ⁹⁵⁵¹		
24.	Apache HTTPD: error responses can expose cookies (CVE-2012-0053) (apache-httpd-cve-2012-0053)	172.23.202.198:80 172.23.202.198:443 172.23.202.223:80 172.23.202.223:443 Propust je otkriven u difoltnom pogrešnom odgovoru za statusni kôd 400. Zlonamerni napadač bi mogao da iskoristi ovaj propust da objavi "httpOnly" kolačiće ako nije određen dokument custom ErrorDocument.	APPLE APPLE-SA-2012-09-19-2 ⁹⁵⁵² BID 51706 ⁹⁵⁵³ CVE CVE-2012-0053 ⁹⁵⁵⁴ IAVM 2012-A-0017 ⁹⁵⁵⁵ REDHAT RHSA-2012:0128 ⁹⁵⁵⁶ SECUNIA 48551 ⁹⁵⁵⁷ URL1 ⁹⁵⁵⁸ URL2 ⁹⁵⁵⁹	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
25.	Apache HTTPD: XSS due to unescaped hostnames (CVE-2012-3499) (apache-httpd-cve-2012-3499)	172.23.202.198:80 172.23.202.198:443 172.23.202.223:80 172.23.202.223:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut jedan od sledećih modula: mod_imagemap, mod_info, mod_ldap, mod_proxy_ftp, mod_status. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Različiti XSS propusti usled nenapuštenih host imena i URI-ja HTML output-a u mod_info, mod_status, mod_imagemap, mod_ldap i mod_proxy_ftp.	APPLE APPLE-SA-2013-09-12-1 ⁹⁵⁶⁰ CVE CVE-2012-3499 ⁹⁵⁶¹ DEBIAN DSA-2637 ⁹⁵⁶² REDHAT RHSA-2013:0815 ⁹⁵⁶³ REDHAT RHSA-2013:1207 ⁹⁵⁶⁴ REDHAT RHSA-2013:1208 ⁹⁵⁶⁵ REDHAT RHSA-2013:1209 ⁹⁵⁶⁶ SECUNIA 55032 ⁹⁵⁶⁷ URL1 ⁹⁵⁶⁸ URL2 ⁹⁵⁶⁹	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.24 Ažurirati na Apache HTTPD version 2.2.24 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz Apache HTTPD >= 2.4 and < 2.4.4 Ažurirati na Apache HTTPD version 2.4.4 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz
26.	Apache HTTPD: XSS in mod_proxy_balancer (CVE-2012-4558)	172.23.202.198:80 172.23.202.198:443 172.23.202.223:80	APPLE APPLE-SA-2013-09-12-1 ⁹⁵⁷⁰ CVE CVE-2012-4558 ⁹⁵⁷¹	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.24 Ažurirati na Apache

⁹⁵⁵⁰ <http://secunia.com/advisories/48551/>⁹⁵⁵¹ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁵⁵² <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁹⁵⁵³ <http://www.securityfocus.com/bid/51706>⁹⁵⁵⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0053>⁹⁵⁵⁵ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁵⁵⁶ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁹⁵⁵⁷ <http://secunia.com/advisories/48551/>⁹⁵⁵⁸ http://httpd.apache.org/security/vulnerabilities_20.html⁹⁵⁵⁹ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁵⁶⁰ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁹⁵⁶¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3499>⁹⁵⁶² <http://www.debian.org/security/2013/dsa-2637>⁹⁵⁶³ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁹⁵⁶⁴ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁹⁵⁶⁵ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁹⁵⁶⁶ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁹⁵⁶⁷ <http://secunia.com/advisories/55032/>⁹⁵⁶⁸ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁵⁶⁹ http://httpd.apache.org/security/vulnerabilities_24.html⁹⁵⁷⁰ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>

	(apache-httpd-cve-2012-4558)	172.23.202.223:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy_balancer. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. XSS propust je uticao na manager interfejs mod_proxy_balancer-a.	DEBIAN DSA-2637 ⁹⁵⁷² REDHAT RHSA-2013:0815 ⁹⁵⁷³ REDHAT RHSA-2013:1207 ⁹⁵⁷⁴ REDHAT RHSA-2013:1208 ⁹⁵⁷⁵ REDHAT RHSA-2013:1209 ⁹⁵⁷⁶ URL1 ⁹⁵⁷⁷ URL2 ⁹⁵⁷⁸		HTTPD version 2.2.24 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz Apache HTTPD >= 2.4 and < 2.4.4 Ažurirati na Apache HTTPD version 2.4.4 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz
27.	Apache HTTPD: mod_dav crash (CVE-2013-1896) (apache-httpd-cve-2013-1896)	172.23.202.198:80 172.23.202.198:443 172.23.202.223:80 172.23.202.223:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_dav_svn. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Slanje MERGE zahteva URI-ju koji obrađuje mod_dav_svn sa izvorom href (poslato kao deo zahteva XML) ciljajući na URI koji nije konfigurisan za DAV prouzrokuje segmentation fault (segfault).	CVE CVE-2013-1896 ⁹⁵⁷⁹ OVAL OVAL18835 ⁹⁵⁸⁰ REDHAT RHSA-2013:1156 ⁹⁵⁸¹ REDHAT RHSA-2013:1207 ⁹⁵⁸² REDHAT RHSA-2013:1208 ⁹⁵⁸³ REDHAT RHSA-2013:1209 ⁹⁵⁸⁴ SECUNIA 55032 ⁹⁵⁸⁵ URL1 ⁹⁵⁸⁶ URL2 ⁹⁵⁸⁷	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.25 Ažurirati na Apache HTTPD version 2.2.25 Apache HTTPD >= 2.4 and < 2.4.6 Ažurirati na Apache HTTPD version 2.4.6 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.6.tar.gz
28.	Apache HTTPD: mod_log_config crash (CVE-2012-0021) (apache-httpd-cve-2012-0021)	172.23.202.198:80 172.23.202.198:443 172.23.202.223:80 172.23.202.223:443 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_log_config. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u modulu mod_log_config. Ako je u upotrebi '%{cookie}C' log format string, udaljeni napadač bi mogao da pošalje specifičan kolačić koji bi doveo do kraha. Krah bi se pokazao kao odbijanje servisa ako se koristi threaded MPM.	APPLE APPLE-SA-2012-09-19-2 ⁹⁵⁸⁸ CVE CVE-2012-0021 ⁹⁵⁸⁹ IAVM 2012-A-0017 ⁹⁵⁹⁰ SECUNIA 48551 ⁹⁵⁹¹ URL1 ⁹⁵⁹²	Umeren	Apache HTTPD >= 2.2 and < 2.2.22 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz

⁹⁵⁷¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4558>⁹⁵⁷² <http://www.debian.org/security/2013/dsa-2637>⁹⁵⁷³ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁹⁵⁷⁴ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁹⁵⁷⁵ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁹⁵⁷⁶ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁹⁵⁷⁷ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁵⁷⁸ http://httpd.apache.org/security/vulnerabilities_24.html⁹⁵⁷⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1896>⁹⁵⁸⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18835>⁹⁵⁸¹ <http://rhn.redhat.com/errata/RHSA-2013-1156.html>⁹⁵⁸² <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁹⁵⁸³ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁹⁵⁸⁴ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁹⁵⁸⁵ <http://secunia.com/advisories/55032/>⁹⁵⁸⁶ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁵⁸⁷ http://httpd.apache.org/security/vulnerabilities_24.html⁹⁵⁸⁸ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁹⁵⁸⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0021>⁹⁵⁹⁰ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁵⁹¹ <http://secunia.com/advisories/48551/>⁹⁵⁹² http://httpd.apache.org/security/vulnerabilities_22.html

29.	Apache HTTPD: XSS in mod_negotiation when untrusted uploads are supported (CVE-2012-2687) (apachehttpd-cve-2012-2687)	172.23.202.198:80 172.23.202.198:443 172.23.202.223:80 172.23.202.223:443 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_negotiation. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Moguće je ubaciti CRLF (Carriage Return and Line Feed) koji omogućava CRLF Injection napade (poznatih i kao HTTP Response Splitting) za sajtove koji koriste mod_negotiation, omogućavajući neproverene upload-ove na lokacije na kojima je omogućen MultiViews (višestruko pregledanje). Ovaj problem je poznat i kao CVE-2008-0455.	APPLE APPLE-SA-2013-09-12-1 ⁹⁵⁹³ BID 55131 ⁹⁵⁹⁴ CVE CVE-2012-2687 ⁹⁵⁹⁵ IAVM 2012-A-0139 ⁹⁵⁹⁶ REDHAT RHSA-2012:1591 ⁹⁵⁹⁷ REDHAT RHSA-2012:1592 ⁹⁵⁹⁸ REDHAT RHSA-2012:1594 ⁹⁵⁹⁹ REDHAT RHSA-2013:0130 ⁹⁶⁰⁰ SECUNIA 50894 ⁹⁶⁰¹ SECUNIA 51607 ⁹⁶⁰² URL1 ⁹⁶⁰³ URL2 ⁹⁶⁰⁴	Umeren	Apache HTTPD >= 2.2 and < 2.2.23 Ažurirati na Apache HTTPD version 2.2.23 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz Apache HTTPD >= 2.4 and < 2.4.3 Ažurirati na Apache HTTPD version 2.4.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.3.tar.gz
30.	Weak Cryptographic Key (weak-crypto-key)	172.23.202.198:443 172.23.202.223:443 Dužina RSA modula u sertifikatu X.509: 1024 bita (manje od 2047 bita). Dužina tajnog ključa koju koristi kriptografski algoritam određuje najviši mogući nivo bezbednosti. Nedavno otkriveni teoretski napadi i sve napredniji hardware stalno snižavaju nivo bezbednosti. Zbog ovoga, od 2011-te godine, vladine, akademske i privatne organizacije koje se bave kriptografskom bezbednošću, kao National Institute of Standards and Technology (NIST), European Network of Excellence in Cryptology II (ECRYPT II), daju sledeće preporuke da bi se obezbedila kratkoročna ili duža bezbednost čak i od najbolje opremljenih napadača (npr. agencije inteligencije): Dužine simetričnih tajnih ključeva od minimum 80-112 bitova. Dužine eliptičnih tajnih ključeva od minimum 160-224 bitova.	URL1 ⁹⁶⁰⁵ URL2 ⁹⁶⁰⁶ URL3 ⁹⁶⁰⁷ URL4 ⁹⁶⁰⁸ URL5 ⁹⁶⁰⁹ URL6 ⁹⁶¹⁰ URL7 ⁹⁶¹¹	Umeren	Slab tajni ključ se koristi u sertifikatu X.509 (npr. za HTTPS server), da generiše duži tajni ključ i osveži sertifikat. Pogledati NIST's preporuke za kriptografske algoritme i dužine tajnih ključeva. ⁹⁶¹²

⁹⁵⁹³ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁹⁵⁹⁴ <http://www.securityfocus.com/bid/55131>⁹⁵⁹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2687>⁹⁵⁹⁶ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁵⁹⁷ <http://rhn.redhat.com/errata/RHSA-2012-1591.html>⁹⁵⁹⁸ <http://rhn.redhat.com/errata/RHSA-2012-1592.html>⁹⁵⁹⁹ <http://rhn.redhat.com/errata/RHSA-2012-1594.html>⁹⁶⁰⁰ <http://rhn.redhat.com/errata/RHSA-2013-0130.html>⁹⁶⁰¹ <http://secunia.com/advisories/50894/>⁹⁶⁰² <http://secunia.com/advisories/51607/>⁹⁶⁰³ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁶⁰⁴ http://httpd.apache.org/security/vulnerabilities_24.html⁹⁶⁰⁵ <http://www.symantec.com/page.jsp?id=1024-bit-certificate-support>⁹⁶⁰⁶ <http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf>⁹⁶⁰⁷ http://csrc.nist.gov/groups/ST/toolkit/key_management.html⁹⁶⁰⁸www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2011_2_AlgoKatpdf.pdf⁹⁶⁰⁹ <http://www.ecrypt.eu.org/documents/D.SPA.17.pdf>⁹⁶¹⁰ <http://www.keylength.com/>⁹⁶¹¹ http://www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf⁹⁶¹² <http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf>

		Dužine RSA tajnih ključeva od minimum 1248-2048 bitova. CA/Browser Forum Extended Validation (EV) Guidelines izričito zahteva da dužina tajnog ključa bude minimum 2048 bitova. Ispitivanja pokazuju da je izrada 1024-bitnog RSA modula praktično dostupna. Dužine DSA tajnih ključeva od minimum 2048 bitova. Dodatno, od 2014-te, Certificate Authority/Browser Forum zahteva da SSL sertifikati i kôd potpisivanje više ne podržavaju 1024-bitne RSA tajne ključeve.			

Tabela 133. Linux OS sa IP adresom 172.23.202.131 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.131		OS: Slackware 13.37 x86, slackware1337			26
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Browsable web directory (http-generic-browsable-dir)	172.23.202.131:80 Otkriven je direktorijum na web serveru koji može biti pretraživan, što znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice - spajdering (prateći hiperlinkove), ili -kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute force napadom na liste uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skriven“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice.		Ozbiljan	Za Apache: onemogućiti pretraživanje direktorijuma mreže za sve direktorijume i poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume. Za Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote: Onemogućiti pretraživanje direktorijuma za sve direktorijume i poddirektorijume. Uključiti Tomcat-ov web.xml file. U odeljku „default“, promeniti parametar „listings“ iz „true“ u „false“. Restartovati server. Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim

					fajlovima i direktorijumima na web root-u (uključujući CGI skripta i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume.
2.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	TCP reset with incorrect sequence number triggered this fault on 172.23.202.131:113: Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hедера i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije) tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	BID: 10183 ⁹⁶¹³ CERT-VN: 415294 ⁹⁶¹⁴ CVE CVE-2004-0230 ⁹⁶¹⁵ MS: MS05-019 ⁹⁶¹⁶ MS: MS06-064 ⁹⁶¹⁷ NETBSD: SA2004-006 ⁹⁶¹⁸ NetBSD- OVAL: OVAL2689 ⁹⁶¹⁹ OVAL: OVAL270 ⁹⁶²⁰ OVAL OVAL3508 ⁹⁶²¹ OVAL OVAL4791 ⁹⁶²² OVAL OVAL5711 ⁹⁶²³ SECUNIA: 11440 ⁹⁶²⁴ SECUNIA 11458 ⁹⁶²⁵ SECUNIA: 22341 ⁹⁶²⁶ SGI 20040403-01-A ⁹⁶²⁷ XF tcp-rst-dos(15886) ⁹⁶²⁸ URL1 ⁹⁶²⁹ URL2 ⁹⁶³⁰	Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC 2385 ⁹⁶³¹ . Ono je napravljeno da smanji opasnost od određenih napada na BGP, kao što su TCP reseti.
3.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podesi na jedinstvenu vrednost i da se koristi u rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da fingerprint-uje operativni sistem.	BID 4314 ⁹⁶³² CVE CVE-2002-0510 ⁹⁶³³ XF linux-udp-fingerprint(8588) ⁹⁶³⁴	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili pak ranjivost koju treba popravljati, tako da ne postoje rešenja koja se mogu kupiti. Jedino se može postaviti fajervol ili neka druga sprava za filtriranje između napadnutog i neprijateljskog napada koji je u mogućnosti da randomizuje IP ID-jeve.

⁹⁶¹³ <http://www.securityfocus.com/bid/10183>⁹⁶¹⁴ <http://www.kb.cert.org/vuls/id/415294>⁹⁶¹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁹⁶¹⁶ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁹⁶¹⁷ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁹⁶¹⁸ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁹⁶¹⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>⁹⁶²⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>⁹⁶²¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>⁹⁶²² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>⁹⁶²³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>⁹⁶²⁴ <http://secunia.com/advisories/11440/>⁹⁶²⁵ <http://secunia.com/advisories/11458/>⁹⁶²⁶ <http://secunia.com/advisories/22341/>⁹⁶²⁷ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>⁹⁶²⁸ <http://xforce.iss.net/xforce/xfdb/15886>⁹⁶²⁹ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁹⁶³⁰ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>⁹⁶³¹ <http://www.ietf.org/rfc/rfc2385.txt>⁹⁶³² <http://www.securityfocus.com/bid/4314>⁹⁶³³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>⁹⁶³⁴ <http://xforce.iss.net/xforce/xfdb/8588>

4.	Apache HTTPD: apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpdcve-2011-0419)	172.23.202.131:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_autoindex. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_fnmatch() u sklopu APR biblioteke. Ako je omogućen mod_autoindex, a indeksi direktorijuma mod_autoindex su sadržavali fajlove sa dovoljno dugim nazivima, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do preterane upotrebe CPU-a. Ovo bi moglo da bude iskorišćeno u napadu odbijanja servisa. Zahvaljujući Maksymilian Arciemowicz prijavljen je ovaj propust.	CVE CVE-2011-0419 ⁹⁶³⁵ DEBIAN DSA-2237 ⁹⁶³⁶ IAVM 2012-B-0056 ⁹⁶³⁷ OVAL OVAL14638 ⁹⁶³⁸ OVAL OVAL14804 ⁹⁶³⁹ REDHAT RHSA-2011:0896 ⁹⁶⁴⁰ REDHAT RHSA-2011:0897 ⁹⁶⁴¹ REDHAT RHSA-2011:0507 ⁹⁶⁴² SECUNIA 44490 ⁹⁶⁴³ SECUNIA 44564 ⁹⁶⁴⁴ SECUNIA 44574 ⁹⁶⁴⁵ URL1 ⁹⁶⁴⁶	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.19 Ažurirati na Apache HTTPD version 2.2.19 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.19.tar.gz
5.	Apache HTTPD: ETag Inode Information Leakage (CVE-2003-1418) (apache-httpdcve-2003-1418)	172.23.202.131:80 U određenim konfiguracijama, Apache HTTP server dozvoljava udaljenim napadačima da dobiju poverljive informacije preko (1) Etag heder-a, koji otkriva broj inoda ili (2) razdvajanje višedelnih MIME-a, koja ukazuje na ID child procesa (PID). Određene verzije Apache-a koriste zahtevani broj čvorova fajla da bi konstruisali 'Etag' heder za odgovor. Iako sama po sebi nije ranjivost, ova informacija olakšava sprovođenje određenih NFS napada. „Running vulnerable HTTP service: Apache 2.2.17. <a 27231-2c-3e9564c23b600\""="" href="http://172.23.202.131/1: \">http://172.23.202.131/1: \"27231-2c-3e9564c23b600\" “	BID 6939 ⁹⁶⁴⁷ BID 6943 ⁹⁶⁴⁸ CVE CVE-2003-1418 ⁹⁶⁴⁹ XF apache-mime-information-disclosure(11438) ⁹⁶⁵⁰	Ozbiljan	Onemogućiti Etag mehanizam tipa "inod-based" konfiguraciji Apache-a. Takođe, inod informacije je moguće ukloniti iz Etag heder-a tako što će se dodati direktiva u Apache konfiguraciju: <i>FileETag Mtime Size</i>
6.	Apache default installation/welcome page installed (http://apache-default-install-page)	172.23.202.131:80 Apache difoltna instalacija ili „Welcome“ stranica je instalirana na serveru. To obično ukazuje na novoinstalirani server. U mnogim slučajevima, Apache se instalira zajedno sa drugim aplikacijama i korisnik možda nije svestan da je web server pokrenut. Ovakvi serveri se retko patch-uju i još ređe nadgledaju, što zlonamernim napadačima postaje pogodna meta koja najverovatnije neće pokrenuti nikakvo upozorenje.		Umeren	Ako se od servera zahteva da obezbedi neophodnu funkcionalnost, onda difoltnu stranicu treba zameniti odgovarajućim sadržajem. U suprotnom, ovakav server treba ukloniti sa mreže, prateći bezbednosni princip minimalne složenosti (više složenosti = manja bezbednost). Ako server nije potreban, treba ga ukloniti iz svih

⁹⁶³⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419>⁹⁶³⁶ <http://www.debian.org/security/2011/dsa-2237>⁹⁶³⁷ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁶³⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14638>⁹⁶³⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14804>⁹⁶⁴⁰ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁹⁶⁴¹ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>⁹⁶⁴² <http://rhn.redhat.com/errata/RHSA-2011-0507.html>⁹⁶⁴³ <http://secunia.com/advisories/44490/>⁹⁶⁴⁴ <http://secunia.com/advisories/44564/>⁹⁶⁴⁵ <http://secunia.com/advisories/44574/>⁹⁶⁴⁶ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁶⁴⁷ <http://www.securityfocus.com/bid/6939>⁹⁶⁴⁸ <http://www.securityfocus.com/bid/6943>⁹⁶⁴⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-1418>⁹⁶⁵⁰ <http://xforce.iss.net/xforce/xfdb/11438>

		Primer : Running vulnerable HTTP service: Apache 2.2.17. http://172.23.202.131/ 1: <code><html><body><h1>It works!</h1></body></html></code>			startup fajlova (npr. /etc/rc*) ili skripti, a zatim prekinuti servis. Proveriti da li se on ponovo pokreće kada se mašina reboot-uje. Apache se uglavnom instalira kao /usr/sbin/httpd na UNIX mašinama ili kao C:\Program Files\Apache Group na Windows mašinama. Razmotriti uklanjanje binara i svih srodnih biblioteka iz sistema.
7.	HTTP TRACE Method Enabled (http-trace-method-enabled)	172.23.202.131:80 HTTP TRACE metoda se obično koristi da uzvрати potpuni HTTP zahtev klijentu koji ga zahteva, u cilju debugovanja proxy servera. Napadač bi mogao da kreira web stranicu koristeći XMLHTTP, ActiveX ili XMLDOM da natera klijenta da pošalje TRACE zahtev i da sačuva klijenove kolačiće. Kao posledica može da se javi XSS napad. Primer: 172.23.202.193:80 Running vulnerable HTTP service. http://172.23.202.131/ 1: TRACE / HTTP/1.1 2: Host: 172.23.202.209 3: Cookie: <code>vulnerable=yes</code>	CERT-VN 867593 ⁹⁶⁵¹ OSVDB 35511 ⁹⁶⁵² OSVDB 3726 ⁹⁶⁵³ SECUNIA 10726 ⁹⁶⁵⁴ SECUNIA 17334 ⁹⁶⁵⁵ SECUNIA 21802 ⁹⁶⁵⁶ SECUNIA 25636 ⁹⁶⁵⁷ CVE CVE-2004-2320 ⁹⁶⁵⁸ CVE CVE-2004-2763 ⁹⁶⁵⁹ CVE CVE-2005-3398 ⁹⁶⁶⁰ CVE CVE-2006-4683 ⁹⁶⁶¹ CVE CVE-2007-3008 ⁹⁶⁶² CVE CVE-2008-7253 ⁹⁶⁶³ CVE CVE-2009-2823 ⁹⁶⁶⁴ CVE CVE-2010-0386 ⁹⁶⁶⁵ OSVDB 877 ⁹⁶⁶⁶ SUN 50603 ⁹⁶⁶⁷ BID 9561 ⁹⁶⁶⁸ URL1 9669 URL2 9670	Ozbiljan	Apache Onemogućiti HTTP TRACE metodu za Apache. Novije verzije Apache-a (1.3.34 i 2.0.55 i novije) omogućuju konfiguracionu direktivu koja se zove TraceEnable. Da bi se odbili TRACE zahtevi, dodaje se sledeći red u konfiguraciju servera: TraceEnable off Za starije verzije Apache web servera, koristiti modul mod_rewrite da bi se odbili TRACE zahteve: RewriteEngine On RewriteCond %{REQUEST_METHOD} ^TRACE RewriteRule .* - [F]
8.	Database Open Access (database-open-access)	172.23.202.131:3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim	URL1 9671	Umeren	Konfigurisati server baze podataka tako da dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.

⁹⁶⁵¹ <http://www.kb.cert.org/vuls/id/867593>⁹⁶⁵² <http://www.osvdb.org/35511>⁹⁶⁵³ <http://www.osvdb.org/3726>⁹⁶⁵⁴ <http://secunia.com/advisories/10726/>⁹⁶⁵⁵ <http://secunia.com/advisories/17334/>⁹⁶⁵⁶ <http://secunia.com/advisories/21802/>⁹⁶⁵⁷ <http://secunia.com/advisories/25636/>⁹⁶⁵⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2320>⁹⁶⁵⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2763>⁹⁶⁶⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-3398>⁹⁶⁶¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-4683>⁹⁶⁶² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3008>⁹⁶⁶³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-7253>⁹⁶⁶⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2823>⁹⁶⁶⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0386>⁹⁶⁶⁶ <http://osvdb.org/887>⁹⁶⁶⁷ <https://sunsolve.sun.com/search/document.do?assetkey=1-22-50603-1> pristupljeno 18.12.2011⁹⁶⁶⁸ <http://www.securityfocus.com/bid/9561>⁹⁶⁶⁹ <http://www.apacheweek.com/issues/03-01-24#news>⁹⁶⁷⁰ <http://www.kb.cert.org/vuls/id/867593>⁹⁶⁷¹ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf

		mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7.			
9.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	CVE CVE-1999-0524 ⁹⁶⁷² OSVDB 95 ⁹⁶⁷³ XF icmp-netmask(306) ⁹⁶⁷⁴ XF icmp-timestamp(322) ⁹⁶⁷⁵	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
10.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1 ⁹⁶⁷⁶ URL2 ⁹⁶⁷⁷ URL3 ⁹⁶⁷⁸	Umeren	Onemogućavanje TCP timestamp odgovora na Linux OS. Podesiti <code>net.ipv4.tcp_timestamps</code> vrednost na sledećem ključu na 0 pokretanjem sledeće komande: <code>sysctl -w net.ipv4.tcp_timestamps=0</code> Dodatno, sledeću vrednost u difoltnom <code>sysctl</code> konfiguracionom fajlu, <code>generally sysctl.conf</code> : <code>net.ipv4.tcp_timestamps=0</code>
11.	WebDAV Extensions are Enabled (http-generic-webdav-enabled)	172.23.202.131:80 WebDAV je skup ekstenzija za HTTP protokol koji omogućava korisnicima da zajednički edituju i obrađuju fajlove na udaljenim web serverima. Mnogi web serveri po difoltu omogućavaju WebDAV ekstenzije, čak i kada nisu potrebne. S obzirom na dodatnu složenost, dosadašnja praksa je pokazala da treba onemogućiti WebDAV ukoliko se trenutno ne koristi.		Umeren	Apache: Potrebno je onemogućiti WebDAV (eng. Web-based Distributed Authoring and Versioning) za Apache. Proveriti da li je <code>mod_dav</code> modul isključen ili utvrditi da li postoji zahtevana autentifikacija na direktorijumima nad kojima se zahteva DAV.
12.	Apache HTTPD: Range header remote DoS (CVE-2011-3192) (apache-httpd-cve-2011-3192)	172.23.202.131:80 Propust je otkriven u načinu na koji Apache HTTP Server obrađuje Range HTTP hedere. Zlonamerni napadač bi mogao da iskoristi ovaj propust i dovede do toga da http koristi veliku količinu memorije i CPU vremena preko HTTP zahteva sa posebno	APPLE APPLE-SA-2011-10-12-3 ⁹⁶⁷⁹ BID 49303 ⁹⁶⁸⁰ CERT-VN 405811 ⁹⁶⁸¹ CVE CVE-2011-3192 ⁹⁶⁸² IAVM 2012-B-0056 ⁹⁶⁸³ OSVDB 74721 ⁹⁶⁸⁴ OVAL OVAL14762 ⁹⁶⁸⁵ OVAL OVAL14824 ⁹⁶⁸⁶	Kritičan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and

⁹⁶⁷² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁹⁶⁷³ <http://www.osvdb.org/95>⁹⁶⁷⁴ <http://xforce.iss.net/xforce/xfdb/306>⁹⁶⁷⁵ <http://xforce.iss.net/xforce/xfdb/322>⁹⁶⁷⁶ http://www.forensicswiki.org/wiki/TCP_timestamps⁹⁶⁷⁷ <http://www.ietf.org/rfc/rfc1323.txt>⁹⁶⁷⁸ <http://uptime.netcraft.com/>⁹⁶⁷⁹ <http://lists.apple.com/archives/Security-announce/2011/Oct/msg00003.html>⁹⁶⁸⁰ <http://www.securityfocus.com/bid/49303>⁹⁶⁸¹ <http://www.kb.cert.org/vuls/id/405811>⁹⁶⁸² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3192>⁹⁶⁸³ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁶⁸⁴ <http://www.osvdb.org/74721>⁹⁶⁸⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14762>⁹⁶⁸⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14824>

		kreiranim Range hederom. Ovo bi moglo dovesti do napada odbijanja servisa. Advisory: CVE-2011-3192.txt	OVAL OVAL18827 ⁹⁶⁸⁷ REDHAT RHSA-2011:1245 ⁹⁶⁸⁸ REDHAT RHSA-2011:1294 ⁹⁶⁸⁹ REDHAT RHSA-2011:1300 ⁹⁶⁹⁰ REDHAT RHSA-2011:1329 ⁹⁶⁹¹ REDHAT RHSA-2011:1330 ⁹⁶⁹² REDHAT RHSA-2011:1369 ⁹⁶⁹³ SECUNIA 45606 ⁹⁶⁹⁴ SECUNIA 45937 ⁹⁶⁹⁵ SECUNIA 46000 ⁹⁶⁹⁶ SECUNIA 46125 ⁹⁶⁹⁷ SECUNIA 46126 ⁹⁶⁹⁸ XF 69396 ⁹⁶⁹⁹ URL1 ⁹⁷⁰⁰ URL2 ⁹⁷⁰¹		< 2.2.20 Ažurirati na Apache HTTPD version 2.2.20 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.20.tar.gz
13.	Apache HTTPD: insecure LD_LIBRARY_PATH handling (CVE-2012-0883) (apache-httpd-cve-2012-0883)	172.23.202.131:80 Otkrivena je nebezbedna obrada rute LD_LIBRARY_PATH koja bi mogla da dovede do toga da direktorijum koji trenutno radi traži DSO-ove. Ovo bi lokalnom korisniku omogućilo da izvrši kôd kao root ako je administrator pokrenuo apachectl sa nepoverljivog direktorijuma.	APPLE APPLE-SA-2013-09-12-1 ⁹⁷⁰² CVE CVE-2012-0883 ⁹⁷⁰³ SECUNIA 48849 ⁹⁷⁰⁴ URL1 ⁹⁷⁰⁵ URL2 ⁹⁷⁰⁶	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.23 Ažurirati na Apache HTTPD version 2.2.23 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz Apache HTTPD >= 2.4 and < 2.4.2 Ažurirati na Apache HTTPD version 2.4.2 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.2.tar.gz
14.	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368) (apache-httpd-cve-2011-3368)	172.23.202.131:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja prisustva mod_proxy modula. Ranjivost na	APPLE APPLE-SA-2012-09-19-2 ⁹⁷⁰⁷ BID 49957 ⁹⁷⁰⁸ CVE CVE-2011-3368 ⁹⁷⁰⁹ IAVM 2012-A-0017 ⁹⁷¹⁰ IAVM 2012-A-0152 ⁹⁷¹¹ IAVM 2012-B-0056 ⁹⁷¹²	Ozbiljan	Apache HTTPD >= 1.3 and < 2 Primeniti zakrpu za CVE-2011-3368 to 1.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.2.tar.gz

⁹⁶⁸⁷ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18827>⁹⁶⁸⁸ <http://rhn.redhat.com/errata/RHSA-2011-1245.html>⁹⁶⁸⁹ <http://rhn.redhat.com/errata/RHSA-2011-1294.html>⁹⁶⁹⁰ <http://rhn.redhat.com/errata/RHSA-2011-1300.html>⁹⁶⁹¹ <http://rhn.redhat.com/errata/RHSA-2011-1329.html>⁹⁶⁹² <http://rhn.redhat.com/errata/RHSA-2011-1330.html>⁹⁶⁹³ <http://rhn.redhat.com/errata/RHSA-2011-1369.html>⁹⁶⁹⁴ <http://secunia.com/advisories/45606/>⁹⁶⁹⁵ <http://secunia.com/advisories/45937/>⁹⁶⁹⁶ <http://secunia.com/advisories/46000/>⁹⁶⁹⁷ <http://secunia.com/advisories/46125/>⁹⁶⁹⁸ <http://secunia.com/advisories/46126/>⁹⁶⁹⁹ <http://xforce.iss.net/xforce/xfdb/69396>⁹⁷⁰⁰ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁷⁰¹ http://httpd.apache.org/security/vulnerabilities_20.html⁹⁷⁰² <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁹⁷⁰³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0883>⁹⁷⁰⁴ <http://secunia.com/advisories/48849/>⁹⁷⁰⁵ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁷⁰⁶ http://httpd.apache.org/security/vulnerabilities_24.html⁹⁷⁰⁷ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁹⁷⁰⁸ <http://www.securityfocus.com/bid/49957>⁹⁷⁰⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3368>⁹⁷¹⁰ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁷¹¹ <http://iase.disa.mil/stigs/iavm-cve.html>

		DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy. Zlonamerni napadač bi mogao da iskoristi ovaj propust na takav način da primora proxy proces da se poveže sa proizvoljnim serverom i potencijalno objavi osjetljive informacije sa internih web servera koje inače napadaču nisu direktno dostupne. Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/	OSVDB 76079 ⁹⁷¹³ REDHAT RHSA-2011:1391 ⁹⁷¹⁴ REDHAT RHSA-2011:1392 ⁹⁷¹⁵ SECUNIA 46288 ⁹⁷¹⁶ SECUNIA 46414 ⁹⁷¹⁷ SECUNIA 48551 ⁹⁷¹⁸ XF 70336 ⁹⁷¹⁹ URL1 ⁹⁷²⁰ URL2 ⁹⁷²¹ URL3 ⁹⁷²²		t/httpd/patches/apply_to_1.3.42/ Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
15.	Apache HTTPD: scoreboard parent DoS (CVE-2012-0031) (apache-httpd-cve-2012-0031)	172.23.202.131:80 Propust je otkriven u obradi scoreboard-a. Neprivilegovani child proces bi mogao da dovede do toga da parent proces krahira prilikom gašenja.	APPLE APPLE-SA-2012-09-19-2 ⁹⁷²³ BID 51407 ⁹⁷²⁴ CVE CVE-2012-0031 ⁹⁷²⁵ IAVM 2012-A-0017 ⁹⁷²⁶ REDHAT RHSA-2012:0128 ⁹⁷²⁷ SECUNIA 47410 ⁹⁷²⁸ SECUNIA 48551 ⁹⁷²⁹ URL1 ⁹⁷³⁰ URL2 ⁹⁷³¹	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
16.	Apache HTTPD: mod_proxy_ajp remote DoS (CVE-2012-4557) (apache-httpd-cve-2012-4557)	172.23.202.131:80 Skenirani servis je osjetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ajp. Proveriti konfiguraciju web servera	CVE CVE-2012-4557 ⁹⁷³² DEBIAN DSA-2579 ⁹⁷³³ URL1 ⁹⁷³⁴	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz

⁹⁷¹² <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁷¹³ <http://www.osvdb.org/76079>⁹⁷¹⁴ <http://rhn.redhat.com/errata/RHSA-2011-1391.html>⁹⁷¹⁵ <http://rhn.redhat.com/errata/RHSA-2011-1392.html>⁹⁷¹⁶ <http://secunia.com/advisories/46288/>⁹⁷¹⁷ <http://secunia.com/advisories/46414/>⁹⁷¹⁸ <http://secunia.com/advisories/48551/>⁹⁷¹⁹ <http://xforce.iss.net/xforce/xfdb/70336>⁹⁷²⁰ http://httpd.apache.org/security/vulnerabilities_13.html⁹⁷²¹ http://httpd.apache.org/security/vulnerabilities_20.html⁹⁷²² http://httpd.apache.org/security/vulnerabilities_22.html⁹⁷²³ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁹⁷²⁴ <http://www.securityfocus.com/bid/51407>⁹⁷²⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0031>⁹⁷²⁶ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁷²⁷ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁹⁷²⁸ <http://secunia.com/advisories/47410/>⁹⁷²⁹ <http://secunia.com/advisories/48551/>⁹⁷³⁰ http://httpd.apache.org/security/vulnerabilities_20.html⁹⁷³¹ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁷³² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4557>⁹⁷³³ <http://www.debian.org/security/2012/dsa-2579>⁹⁷³⁴ http://httpd.apache.org/security/vulnerabilities_22.html

		radi utvrđivanja ove mogućnosti. Propust je otkriven kada se mod_proxy_ajp koristi zajedno sa mod_proxy_balancer. Sa specifičnom konfiguracijom, udaljeni napadač može da pošalje zlonameran HTTP zahtev, prouzrokujući da backend server bude stavljen u status greške dok ne istekne vreme za ponovni pokušaj. To bi dovelo do odbijanja servisa.			
17.	Apache HTTPD: mod_rewrite log escape filtering (CVE-2013-1862) (apache-httpd-cve-2013-1862)	172.23.202.131:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_rewrite. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Modul mod_rewrite ne filtrira završne izlazne sekvence iz logova, što zlonamenom napadaču olakšava da ubace takve sekvence u završne emulatore koji sadrže ranjivosti koje se odnose na izlazne sekvence.	CVE CVE-2013-1862 ⁹⁷³⁵ OVAL OVAL18790 ⁹⁷³⁶ REDHAT RHSA-2013:0815 ⁹⁷³⁷ REDHAT RHSA-2013:1207 ⁹⁷³⁸ REDHAT RHSA-2013:1208 ⁹⁷³⁹ REDHAT RHSA-2013:1209 ⁹⁷⁴⁰ SECUNIA 55032 ⁹⁷⁴¹ URL1 ⁹⁷⁴² URL2 ⁹⁷⁴³	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.25 Ažurirati na Apache HTTPD version 2.2.25 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.25.tar.gz
18.	Apache HTTPD: mod_proxy_ajp remote DoS (CVE-2011-3348) (apache-httpd-cve-2011-3348)	172.23.202.131:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ajp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven kada se mod_proxy_ajp koristi zajedno sa mod_proxy_balancer. Sa specifičnom konfiguracijom, udaljeni napadač može da pošalje zlonameran HTTP zahtev, prouzrokujući da backend server bude stavljen u status greške dok ne istekne vreme za ponovni pokušaj. To bi dovelo do odbijanja servisa.	APPLE APPLE-SA-2012-02-01-1 ⁹⁷⁴⁴ BID 49616 ⁹⁷⁴⁵ CVE CVE-2011-3348 ⁹⁷⁴⁶ IAVM 2012-B-0056 ⁹⁷⁴⁷ OVAL OVAL14941 ⁹⁷⁴⁸ OVAL OVAL18154 ⁹⁷⁴⁹ REDHAT RHSA-2011:1391 ⁹⁷⁵⁰ SECUNIA 46013 ⁹⁷⁵¹ XF 69804 ⁹⁷⁵² URL1 ⁹⁷⁵³	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.21 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.21.tar.gz
19.	Apache HTTPD: mod_setenvif.htaccess privilege escalation (CVE-2011-3607)	172.23.202.131:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul:	APPLE APPLE-SA-2012-09-19-2 ⁹⁷⁵⁴ BID 50494 ⁹⁷⁵⁵ CVE CVE-2011-3607 ⁹⁷⁵⁶	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65

⁹⁷³⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1862>
⁹⁷³⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18790>
⁹⁷³⁷ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>
⁹⁷³⁸ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>
⁹⁷³⁹ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>
⁹⁷⁴⁰ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>
⁹⁷⁴¹ <http://secunia.com/advisories/55032/>
⁹⁷⁴² http://httpd.apache.org/security/vulnerabilities_20.html
⁹⁷⁴³ http://httpd.apache.org/security/vulnerabilities_22.html
⁹⁷⁴⁴ <http://lists.apple.com/archives/security-announce/2012/Feb/msg00000.html>
⁹⁷⁴⁵ <http://www.securityfocus.com/bid/49616>
⁹⁷⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3348>
⁹⁷⁴⁷ <http://iase.disa.mil/stigs/iavm-cve.html>
⁹⁷⁴⁸ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14941>
⁹⁷⁴⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18154>
⁹⁷⁵⁰ <http://rhn.redhat.com/errata/RHSA-2011-1391.html>
⁹⁷⁵¹ <http://secunia.com/advisories/46013/>
⁹⁷⁵² <http://xforce.iss.net/xforce/xfdb/69804>
⁹⁷⁵³ http://httpd.apache.org/security/vulnerabilities_22.html
⁹⁷⁵⁴ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>
⁹⁷⁵⁵ <http://www.securityfocus.com/bid/50494>

	(apache-httpd-cve-2011-3607)	mod_setenvif. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust preopterećenja je otkriven kada je omogućen modul mod_setenvif, što lokalnim korisnicima omogućava da dobiju privilegije preko fajla .htaccess.	IAVM 2012-A-0017 ⁹⁷⁵⁷ IAVM 2012-A-0152 ⁹⁷⁵⁸ OSVDB 76744 REDHAT ⁹⁷⁵⁹ RHSA-2012:0128 SECUNIA 45793 ⁹⁷⁶⁰ SECUNIA 48551 ⁹⁷⁶¹ XF 71093 ⁹⁷⁶² URL1 ⁹⁷⁶³ URL2 ⁹⁷⁶⁴		Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
20.	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-4317) (apache-httpd-cve-2011-4317)	172.23.202.131:80 Skenirani servis je osetljiv na ovu ranjivost samo ako je pokrenut modul mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy U određenim konfiguracijama koje koriste RewriteRule sa proxy flag-om ili ProxyPassMatch, udaljeni napadač bi mogao da primora reverzni proksi da se poveže sa proizvoljnim serverom i potencijalno objavi osetljive informacije sa internih web servera koje inače napadaču nisu direktno dostupne.	APPLE ⁹⁷⁶⁵ APPLE-SA-2012-09-19-2 CVE CVE-2011-4317 ⁹⁷⁶⁶ IAVM 2012-A-0017 ⁹⁷⁶⁷ IAVM 2012-A-0152 ⁹⁷⁶⁸ REDHAT ⁹⁷⁶⁹ RHSA-2012:0128 SECUNIA 48551 ⁹⁷⁷⁰ URL1 ⁹⁷⁷¹	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
21.	Apache HTTPD: error responses can expose cookies (CVE-2012-0053) (apache-httpd-cve-2012-0053)	172.23.202.131:80 Propust je otkriven u difoltnom pogrešnom odgovoru za statusni kôd 400. Zlonamerni napadač bi mogao da iskoristi ovaj propust da objavi "httpOnly" kolačiće ako nije određen dokument custom ErrorDocument.	APPLE ⁹⁷⁷² APPLE-SA-2012-09-19-2 BID 51706 ⁹⁷⁷³ CVE CVE-2012-0053 ⁹⁷⁷⁴ IAVM 2012-A-0017 ⁹⁷⁷⁵ REDHAT ⁹⁷⁷⁶ RHSA-2012:0128 SECUNIA 48551 ⁹⁷⁷⁷ URL1 ⁹⁷⁷⁸ URL2 ⁹⁷⁷⁹	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz

⁹⁷⁵⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3607>⁹⁷⁵⁷ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁷⁵⁸ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁷⁵⁹ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁹⁷⁶⁰ <http://secunia.com/advisories/45793/>⁹⁷⁶¹ <http://secunia.com/advisories/48551/>⁹⁷⁶² <http://xforce.iss.net/xforce/xfdb/71093>⁹⁷⁶³ http://httpd.apache.org/security/vulnerabilities_20.html⁹⁷⁶⁴ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁷⁶⁵ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁹⁷⁶⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4317>⁹⁷⁶⁷ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁷⁶⁸ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁷⁶⁹ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁹⁷⁷⁰ <http://secunia.com/advisories/48551/>⁹⁷⁷¹ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁷⁷² <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁹⁷⁷³ <http://www.securityfocus.com/bid/51706>⁹⁷⁷⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0053>⁹⁷⁷⁵ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁷⁷⁶ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁹⁷⁷⁷ <http://secunia.com/advisories/48551/>⁹⁷⁷⁸ http://httpd.apache.org/security/vulnerabilities_20.html⁹⁷⁷⁹ http://httpd.apache.org/security/vulnerabilities_22.html

22.	Apache HTTPD: XSS due to unescaped hostnames (CVE-2012-3499) (apache-httpd-cve-2012-3499)	172.23.202.131:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut jedan od sledećih modula: mod_imagemap, mod_info, mod_ldap, mod_proxy_ftp, mod_status. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Različiti XSS propusti usled nenapuštenih host imena i URI-ja HTML output-a u mod_info, mod_status, mod_imagemap, mod_ldap i mod_proxy_ftp.	APPLE APPLE-SA-2013-09-12-1 ⁹⁷⁸⁰ CVE CVE-2012-3499 ⁹⁷⁸¹ DEBIAN DSA-2637 ⁹⁷⁸² REDHAT RHSA-2013:0815 ⁹⁷⁸³ REDHAT RHSA-2013:1207 ⁹⁷⁸⁴ REDHAT RHSA-2013:1208 ⁹⁷⁸⁵ REDHAT RHSA-2013:1209 ⁹⁷⁸⁶ SECUNIA 55032 ⁹⁷⁸⁷ URL1 ⁹⁷⁸⁸ URL2 ⁹⁷⁸⁹	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.24 Ažurirati na Apache HTTPD version 2.2.24 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz Apache HTTPD >= 2.4 and < 2.4.4 Ažurirati na Apache HTTPD version 2.4.4 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz
23.	Apache HTTPD: XSS in mod_proxy_balancer (CVE-2012-4558) (apache-httpd-cve-2012-4558)	172.23.202.131:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy_balancer. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. XSS propust je uticao na manager interfejs mod_proxy_balancer-a.	APPLE APPLE-SA-2013-09-12-1 ⁹⁷⁹⁰ CVE CVE-2012-4558 ⁹⁷⁹¹ DEBIAN DSA-2637 ⁹⁷⁹² REDHAT RHSA-2013:0815 ⁹⁷⁹³ REDHAT RHSA-2013:1207 ⁹⁷⁹⁴ REDHAT RHSA-2013:1208 ⁹⁷⁹⁵ REDHAT RHSA-2013:1209 ⁹⁷⁹⁶ URL1 ⁹⁷⁹⁷ URL2 ⁹⁷⁹⁸	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.24 Ažurirati na Apache HTTPD version 2.2.24 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz Apache HTTPD >= 2.4 and < 2.4.4 Ažurirati na Apache HTTPD version 2.4.4 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz
24.	Apache HTTPD: mod_dav crash (CVE-2013-1896) (apache-httpd-cve-2013-1896)	172.23.202.131:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_dav_svn. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Slanje MERGE zahteva URI-ju koji obrađuje mod_dav_svn sa izvorom href (poslato kao deo zahteva XML) ciljajući na URI koji nije konfigurisan za DAV	CVE CVE-2013-1896 ⁹⁷⁹⁹ OVAL OVAL18835 ⁹⁸⁰⁰ REDHAT RHSA-2013:1156 ⁹⁸⁰¹ REDHAT RHSA-2013:1207 ⁹⁸⁰² REDHAT RHSA-2013:1208 ⁹⁸⁰³ REDHAT RHSA-2013:1209 ⁹⁸⁰⁴ SECUNIA 55032 ⁹⁸⁰⁵	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.25 Ažurirati na Apache HTTPD version 2.2.25 Apache HTTPD >= 2.4 and < 2.4.6 Ažurirati na Apache HTTPD version 2.4.6 Uraditi download a zatim instalirati: http://archive.apache.org/dist

⁹⁷⁸⁰ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁹⁷⁸¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3499>⁹⁷⁸² <http://www.debian.org/security/2013/dsa-2637>⁹⁷⁸³ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁹⁷⁸⁴ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁹⁷⁸⁵ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁹⁷⁸⁶ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁹⁷⁸⁷ <http://secunia.com/advisories/55032/>⁹⁷⁸⁸ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁷⁸⁹ http://httpd.apache.org/security/vulnerabilities_24.html⁹⁷⁹⁰ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁹⁷⁹¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4558>⁹⁷⁹² <http://www.debian.org/security/2013/dsa-2637>⁹⁷⁹³ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁹⁷⁹⁴ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁹⁷⁹⁵ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁹⁷⁹⁶ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁹⁷⁹⁷ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁷⁹⁸ http://httpd.apache.org/security/vulnerabilities_24.html⁹⁷⁹⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1896>⁹⁸⁰⁰ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18835>⁹⁸⁰¹ <http://rhn.redhat.com/errata/RHSA-2013-1156.html>⁹⁸⁰² <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁹⁸⁰³ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁹⁸⁰⁴ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁹⁸⁰⁵ <http://secunia.com/advisories/55032/>

		prouzrokuje segmentation fault (segfault).	URL1⁹⁸⁰⁶ URL2⁹⁸⁰⁷		t/httpd/httpd-2.4.6.tar.gz
25.	Apache HTTPD: mod_log_config crash (CVE-2012-0021) (apache-httpd-cve-2012-0021)	172.23.202.131:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_log_config. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u modulu mod_log_config. Ako je u upotrebi "%{cookienam}C" log format string, udaljeni napadač bi mogao da pošalje specifičan kolačić koji bi doveo do kraha. Krah bi se pokazao kao odbijanje servisa ako se koristi threaded MPM.	APPLE APPLE-SA-2012-09-19-2⁹⁸⁰⁸ CVE CVE-2012-0021⁹⁸⁰⁹ IAVM 2012-A-0017⁹⁸¹⁰ SECUNIA 48551⁹⁸¹¹ URL1⁹⁸¹²	Umeren	Apache HTTPD >= 2.2 and < 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
26.	Apache HTTPD: XSS in mod_negotiation when untrusted uploads are supported (CVE-2012-2687) (apachehttpd-cve-2012-2687)	172.23.202.131:80 Skenirani servis je osjetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_negotiation. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Moguće je ubaciti CRLF (Carriage Return and Line Feed) koji omogućava CRLF Injection napade (poznatih i kao HTTP Response Splitting) za sajtove koji koriste mod_negotiation, omogućavajući neproverene upload-ove na lokacije na kojima je omogućen MultiViews (višestruko pregledanje). Ovaj problem je poznat i kao CVE-2008-0455.	APPLE APPLE-SA-2013-09-12-1⁹⁸¹³ BID 55131⁹⁸¹⁴ CVE CVE-2012-2687⁹⁸¹⁵ IAVM 2012-A-0139⁹⁸¹⁶ REDHAT RHSA-2012:1591⁹⁸¹⁷ REDHAT RHSA-2012:1592⁹⁸¹⁸ REDHAT RHSA-2012:1594⁹⁸¹⁹ REDHAT RHSA-2013:0130⁹⁸²⁰ SECUNIA 50894⁹⁸²¹ SECUNIA 51607⁹⁸²² URL1⁹⁸²³ URL2⁹⁸²⁴	Umeren	Apache HTTPD >= 2.2 and < 2.2.23 Ažurirati na Apache HTTPD version 2.2.23 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz Apache HTTPD >= 2.4 and < 2.4.3 Ažurirati na Apache HTTPD version 2.4.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.3.tar.gz

Tabela 134. Linux OS sa IP adresom 172.23.202.125 (2013. godina)

Datum: 16.11.2013		Operativni sistem i ime računara			Broj ranjivosti
IP adresa: 172.23.202.125		OS: Opensuse 11.4 x86, opensuse1104x86			22
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešenje ranjivosti
1.	Browsable web directory (http-generic-	172.23.202.125:80 Otkriven je direktorijum na web serveru koji može biti pretraživan, što		Ozbiljan	Za Apache: onemogućiti pretraživanje direktorijuma mreže za sve direktorijume i

⁹⁸⁰⁶ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁸⁰⁷ http://httpd.apache.org/security/vulnerabilities_24.html⁹⁸⁰⁸ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁹⁸⁰⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0021>⁹⁸¹⁰ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁸¹¹ <http://secunia.com/advisories/48551/>⁹⁸¹² http://httpd.apache.org/security/vulnerabilities_22.html⁹⁸¹³ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁹⁸¹⁴ <http://www.securityfocus.com/bid/55131>⁹⁸¹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2687>⁹⁸¹⁶ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁸¹⁷ <http://rhn.redhat.com/errata/RHSA-2012-1591.html>⁹⁸¹⁸ <http://rhn.redhat.com/errata/RHSA-2012-1592.html>⁹⁸¹⁹ <http://rhn.redhat.com/errata/RHSA-2012-1594.html>⁹⁸²⁰ <http://rhn.redhat.com/errata/RHSA-2013-0130.html>⁹⁸²¹ <http://secunia.com/advisories/50894/>⁹⁸²² <http://secunia.com/advisories/51607/>⁹⁸²³ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁸²⁴ http://httpd.apache.org/security/vulnerabilities_24.html

	browsable-dir)	znači da bilo ko može da ima uvid u sadržaje ovog direktorijuma. Ovi direktorijumi se mogu naći: -preko pregledanja stranice - spajdering (prateći hiperlinkove), ili -kao deo glavne (eng. parent) putanje (kada se proverava svaki direktorijum na putanji kada se traži „Directory Listing“ ili slični stringovi), ili -brute force napadom na liste uobičajenih direktorijuma. Pretraživi direktorijumi mogu omogućiti napadaču da pregleda „skriven“ fajlove u root-u web servera, uključujući CGI skripte, fajlove podataka ili backup stranice.			poddirektorijume. U httpd.conf fajlu, potrebno je isključiti opciju „Indexes“ za odgovarajući <Directory> tako što će se ukloniti sa liste opcija (Options). Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skripte i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume. Za Apache Tomcat, Tomcat, Tomcat Web Server, Apache Coyote, Apache-Coyote: Onemogućiti pretraživanje direktorijuma za sve direktorijume i poddirektorijume. Uključiti Tomcat-ov web.xml file. U odeljku „default“, promeniti parametar „listings“ iz „true“ u „false“. Restartovati server. Uz to, uvek treba proveriti jesu li određena odobrenja postavljena na svim fajlovima i direktorijumima na web root-u (uključujući CGI skriptu i backup fajlove). Ne kopirati fajlove u web root, osim u slučaju da je potrebno da ovi fajlovi budu dostupni preko web-a. Povremeno kontrolisati web direktorijume i obrisati svaki koji nije u upotrebi, koji je zastareo, kao i nepoznate fajlove i direktorijume.
2.	TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation)	TCP reset with incorrect sequence number triggered this fault on 172.23.202.125:80: Kada se kod TCP paketa koristi Large Window Size, olakšava se spoljnom napadaču da otkrije sekvencijalni broj hedera i prouzrokuje DOS napad (prekid uspostavljene TCP konekcije)	OSVDB 4030⁹⁸²⁵ BID: 10183⁹⁸²⁶ CERT-VN: 415294⁹⁸²⁷ CVE CVE-2004-0230⁹⁸²⁸ MS: MS05-019⁹⁸²⁹ MS: MS06-064⁹⁸³⁰ NETBSD: NetBSD-SA2004-006⁹⁸³¹	Ozbiljan	Omogućiti opciju TCP MD5 potpisivanja, kako je dokumentovano u RFC 2385⁹⁸⁴⁴. Ono je napravljeno da smanji opasnost od određenih napada na BGP, kao što su TCP reseti.

⁹⁸²⁵ <http://www.osvdb.org/4030>⁹⁸²⁶ <http://www.securityfocus.com/bid/10183>⁹⁸²⁷ <http://www.kb.cert.org/vuls/id/415294>⁹⁸²⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-0230>⁹⁸²⁹ <http://technet.microsoft.com/en-us/security/bulletin/ms05-019>⁹⁸³⁰ <http://technet.microsoft.com/en-us/security/bulletin/ms06-064>⁹⁸³¹ <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>

		tako što neprekidno ubacuje TCP RST paket, naročito u protokole koji koriste dugotrajne veze, kao npr. BGP.	OVAL: OVAL2689⁹⁸³² OVAL: OVAL270⁹⁸³³ OVAL OVAL3508⁹⁸³⁴ OVAL OVAL4791⁹⁸³⁵ OVAL OVAL5711⁹⁸³⁶ SECUNIA: 11440⁹⁸³⁷ SECUNIA 11458⁹⁸³⁸ SECUNIA: 22341⁹⁸³⁹ SGI 20040403-01-A⁹⁸⁴⁰ XF tcp-rst-dos(15886)⁹⁸⁴¹ URL1⁹⁸⁴² URL2⁹⁸⁴³		
3.	UDP IP ID Zero (udp-ipid-zero)	Udaljeni host je odgovorio UDP paketom čiji je IP ID bio nula. Uobičajeno je da se IP ID podesi na jedinstvenu vrednost i da se koristi u rekonstrukciji fragmentovanih paketa. Uopšteno, ovakav postupak je vidljiv sistemima koji potiču iz Linux kernel-a, a koji mogu omogućiti napadaču da fingerprint-uje operativni sistem.	BID 4314⁹⁸⁴⁵ CVE CVE-2002-0510⁹⁸⁴⁶ XF linux-udp-fingerprint(8588)⁹⁸⁴⁷	Ozbiljan	Mnogi prodavci ne smatraju da je ovo ranjivost ili pak ranjivost koju treba popravljati, tako da ne postoje rešenja koja se mogu kupiti. Jedino se može postaviti fajervol ili neka druga sprava za filtriranje između napadnutog i neprijateljskog napada koji je u mogućnosti da randomizuje IP ID-jeve.
4.	Apache HTTPD: apr_fnmatch flaw leads to mod_autoindex remote DoS (CVE-2011-0419) (apache-httpdcve-2011-0419)	172.23.202.125:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_autoindex. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u funkciji apr_fnmatch() u sklopu APR biblioteke. Ako je omogućen mod_autoindex, a indeksi direktorijuma mod_autoindex su sadržavali fajlove sa dovoljno dugim nazivima, udaljeni napadač bi mogao da pošalje pažljivo kreiran zahtev koji bi doveo do preterane upotrebe CPU-a. Ovo bi moglo da bude iskorišćeno u napadu odbijanja servisa.	CVE CVE-2011-0419⁹⁸⁴⁸ DEBIAN DSA-2237⁹⁸⁴⁹ IAVM 2012-B-0056⁹⁸⁵⁰ OVAL OVAL14638⁹⁸⁵¹ OVAL OVAL14804⁹⁸⁵² REDHAT RHSA-2011:0896⁹⁸⁵³ REDHAT RHSA-2011:0897⁹⁸⁵⁴ REDHAT RHSA-2011:0507⁹⁸⁵⁵ SECUNIA 44490⁹⁸⁵⁶ SECUNIA 44564⁹⁸⁵⁷ SECUNIA 44574⁹⁸⁵⁸ URL1⁹⁸⁵⁹	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.19 Ažurirati na Apache HTTPD version 2.2.19 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.19.tar.gz

⁹⁸⁴⁴ <http://www.ietf.org/rfc/rfc2385.txt>⁹⁸³² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:2689>⁹⁸³³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:270>⁹⁸³⁴ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3508>⁹⁸³⁵ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4791>⁹⁸³⁶ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:5711>⁹⁸³⁷ <http://secunia.com/advisories/11440/>⁹⁸³⁸ <http://secunia.com/advisories/11458/>⁹⁸³⁹ <http://secunia.com/advisories/22341/>⁹⁸⁴⁰ <ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc>⁹⁸⁴¹ <http://xforce.iss.net/xforce/xfdb/15886>⁹⁸⁴² <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc>⁹⁸⁴³ <http://tools.ietf.org/html/draft-ietf-tcpm-tcpsecure-12>⁹⁸⁴⁵ <http://www.securityfocus.com/bid/4314>⁹⁸⁴⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0510>⁹⁸⁴⁷ <http://xforce.iss.net/xforce/xfdb/8588>⁹⁸⁴⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0419>⁹⁸⁴⁹ <http://www.debian.org/security/2011/dsa-2237>⁹⁸⁵⁰ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁸⁵¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14638>⁹⁸⁵² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14804>⁹⁸⁵³ <http://rhn.redhat.com/errata/RHSA-2011-0896.html>⁹⁸⁵⁴ <http://rhn.redhat.com/errata/RHSA-2011-0897.html>⁹⁸⁵⁵ <http://rhn.redhat.com/errata/RHSA-2011-0507.html>⁹⁸⁵⁶ <http://secunia.com/advisories/44490/>⁹⁸⁵⁷ <http://secunia.com/advisories/44564/>⁹⁸⁵⁸ <http://secunia.com/advisories/44574/>⁹⁸⁵⁹ http://httpd.apache.org/security/vulnerabilities_22.html

		Zahvaljujući Maksymilian Arciemowicz prijavljen je ovaj propust.			
5.	HTTP TRACE Method Enabled (http-trace-method-enabled)	172.23.202.125:80 HTTP TRACE metoda se obično koristi da uzvati potpuni HTTP zahtev klijentu koji ga zahteva, u cilju debugovanja proxy servera. Napadač bi mogao da kreira web stranicu koristeći XMLHTTP, ActiveX ili XMLDOM da natera klijenta da pošalje TRACE zahtev i da sačuva klijenove kolačiće. Kao posledica može da se javi XSS napad. Primer: 172.23.202.193:80 Running vulnerable HTTP service. http://172.23.202.125/ 1: TRACE / HTTP/1.1 2: Host: 172.23.202.125 3: Cookie: vulnerable=yes	CERT-VN 867593 ⁹⁸⁶⁰ OSVDB 35511 ⁹⁸⁶¹ OSVDB 3726 ⁹⁸⁶² SECUNIA 10726 ⁹⁸⁶³ SECUNIA 17334 ⁹⁸⁶⁴ SECUNIA 21802 ⁹⁸⁶⁵ SECUNIA 25636 ⁹⁸⁶⁶ CVE CVE-2004-2320 ⁹⁸⁶⁷ CVE CVE-2004-2763 ⁹⁸⁶⁸ CVE CVE-2005-3398 ⁹⁸⁶⁹ CVE CVE-2006-4683 ⁹⁸⁷⁰ CVE CVE-2007-3008 ⁹⁸⁷¹ CVE CVE-2008-7253 ⁹⁸⁷² CVE CVE-2009-2823 ⁹⁸⁷³ CVE CVE-2010-0386 ⁹⁸⁷⁴ OSVDB 877 ⁹⁸⁷⁵ SUN 50603 ⁹⁸⁷⁶ BID 9561 ⁹⁸⁷⁷ URL1 9878 URL2 9879	Ozbiljan	Apache Onemogućiti HTTP TRACE metodu za Apache. Novije verzije Apache-a (1.3.34 i 2.0.55 i novije) omogućuju konfiguracionu direktivu koja se zove TraceEnable. Da bi se odbili TRACE zahtevi, dodaje se sledeći red u konfiguraciju servera: TraceEnable off Za starije verzije Apache web servera, koristiti modul mod_rewrite da bi se odbili TRACE zahteve: RewriteEngine On RewriteCond %{REQUEST_METHOD} ^TRACE RewriteRule .* - [F]
6.	Database Open Access (database-open-access)	172.23.202.125:3306 Pronađena baza podataka daje mogućnost bilo kom udaljenom sistemu da se poveže sa njom. Preporučuje se da se ograniči direktan pristup sistemima od poverenja jer baze podataka mogu da sadrže osetljive podatke, a nove ranjivosti i novi eksploati se vrlo često pojavljuju. Iz ovog razloga, posedovanje baza podataka na portovima kojima se može prići preko Interneta, čak i ako su zaštićene sigurnosnim mehanizmima autorizacije, predstavlja povredu standarda PCI DSS sekcija 1.3.7.	URL1 9880	Umeren	Konfigurisati server baze podataka tako da dozvoljava pristup samo sistemima od poverenja. Na primer, PCI DSS standard zahteva da se baza podataka postavi na internu mrežnu zonu, odvojenu od DMZ.
7.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova	CVE CVE-1999-0524 ⁹⁸⁸¹ OSVDB 95 ⁹⁸⁸² XF icmp-netmask(306) ⁹⁸⁸³ XF icmp-	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru

⁹⁸⁶⁰ <http://www.kb.cert.org/vuls/id/867593>⁹⁸⁶¹ <http://www.osvdb.org/35511>⁹⁸⁶² <http://www.osvdb.org/3726>⁹⁸⁶³ <http://secunia.com/advisories/10726/>⁹⁸⁶⁴ <http://secunia.com/advisories/17334/>⁹⁸⁶⁵ <http://secunia.com/advisories/21802/>⁹⁸⁶⁶ <http://secunia.com/advisories/25636/>⁹⁸⁶⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2320>⁹⁸⁶⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2763>⁹⁸⁶⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-3398>⁹⁸⁷⁰ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-4683>⁹⁸⁷¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3008>⁹⁸⁷² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-7253>⁹⁸⁷³ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2823>⁹⁸⁷⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0386>⁹⁸⁷⁵ <http://osvdb.org/877>⁹⁸⁷⁶ <https://sunsolve.sun.com/search/document.do?assetkey=1-22-50603-1> pristupljeno 18.12.2011⁹⁸⁷⁷ <http://www.securityfocus.com/bid/9561>⁹⁸⁷⁸ <http://www.apacheweek.com/issues/03-01-24#news>⁹⁸⁷⁹ <http://www.kb.cert.org/vuls/id/867593>⁹⁸⁸⁰ https://www.pcisecuritystandards.org/security_standards/index.php?id=pci_dss_v1-2.pdf⁹⁸⁸¹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524>⁹⁸⁸² <http://www.osvdb.org/95>⁹⁸⁸³ <http://xforce.iss.net/xforce/xfdb/306>

		informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	timestamp(322) ⁹⁸⁸⁴		ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost.
8.	Apache HTTPD: insecure LD_LIBRARY_PATH handling (CVE-2012-0883) (apache-httpd-cve-2012-0883)	172.23.202.125:80 Otkrivena je nebezbedna obrada rute LD_LIBRARY_PATH koja bi mogla da dovede do toga da direktorijum koji trenutno radi traži DSO-ove. Ovo bi lokalnom korisniku omogućilo da izvrši kôd kao root ako je administrator pokrenuo apachectl sa nepoverljivog direktorijuma.	APPLE APPLE-SA-2013-09-12-1 ⁹⁸⁸⁵ CVE CVE-2012-0883 ⁹⁸⁸⁶ SECUNIA 48849 ⁹⁸⁸⁷ URL1 ⁹⁸⁸⁸ URL2 ⁹⁸⁸⁹	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.23 Ažurirati na Apache HTTPD version 2.2.23 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz Apache HTTPD >= 2.4 and < 2.4.2 Ažurirati na Apache HTTPD version 2.4.2 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.2.tar.gz
9.	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-2011-3368) (apache-httpd-cve-2011-3368)	172.23.202.125:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja prisustva mod_proxy modula. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy. Zlonamerni napadač bi mogao da iskoristi ovaj propust na takav način da primora proxy proces da se poveže sa proizvoljnim serverom i potencijalno objavi osetljive informacije sa internih web servera koje inače napadaču nisu direktno dostupne. Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/	APPLE APPLE-SA-2012-09-19-2 ⁹⁸⁹⁰ BID 49957 ⁹⁸⁹¹ CVE CVE-2011-3368 ⁹⁸⁹² IAVM 2012-A-0017 ⁹⁸⁹³ IAVM 2012-A-0152 ⁹⁸⁹⁴ IAVM 2012-B-0056 ⁹⁸⁹⁵ OSVDB 76079 ⁹⁸⁹⁶ REDHAT RHSA-2011:1391 ⁹⁸⁹⁷ REDHAT RHSA-2011:1392 ⁹⁸⁹⁸ SECUNIA 46288 ⁹⁸⁹⁹ SECUNIA 46414 ⁹⁹⁰⁰ SECUNIA 48551 ⁹⁹⁰¹ XF 70336 ⁹⁹⁰² URL1 ⁹⁹⁰³ URL2 ⁹⁹⁰⁴ URL3 ⁹⁹⁰⁵	Ozbiljan	Apache HTTPD >= 1.3 and < 2 Primeniti zakrpu za CVE-2011-3368 to 1.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ Update za 1.3 neće biti pušten u opticaj. Zakrpe će biti objavljene na http://archive.apache.org/dist/httpd/patches/apply_to_1.3.42/ Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dis

⁹⁸⁸⁴ <http://xforce.iss.net/xforce/xfdb/322>⁹⁸⁸⁵ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁹⁸⁸⁶ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0883>⁹⁸⁸⁷ <http://secunia.com/advisories/48849/>⁹⁸⁸⁸ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁸⁸⁹ http://httpd.apache.org/security/vulnerabilities_24.html⁹⁸⁹⁰ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁹⁸⁹¹ <http://www.securityfocus.com/bid/49957>⁹⁸⁹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3368>⁹⁸⁹³ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁸⁹⁴ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁸⁹⁵ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁸⁹⁶ <http://www.osvdb.org/76079>⁹⁸⁹⁷ <http://rhn.redhat.com/errata/RHSA-2011-1391.html>⁹⁸⁹⁸ <http://rhn.redhat.com/errata/RHSA-2011-1392.html>⁹⁸⁹⁹ <http://secunia.com/advisories/46288/>⁹⁹⁰⁰ <http://secunia.com/advisories/46414/>⁹⁹⁰¹ <http://secunia.com/advisories/48551/>⁹⁹⁰² <http://xforce.iss.net/xforce/xfdb/70336>⁹⁹⁰³ http://httpd.apache.org/security/vulnerabilities_13.html⁹⁹⁰⁴ http://httpd.apache.org/security/vulnerabilities_20.html⁹⁹⁰⁵ http://httpd.apache.org/security/vulnerabilities_22.html

					t/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
10.	Apache HTTPD: scoreboard parent DoS (CVE-2012-0031) (apache-httpd-cve-2012-0031)	172.23.202.125:80 Propust je otkriven u obradi scoreboard-a. Neprivilegovani child proces bi mogao da dovede do toga da parent proces krahira prilikom gašenja.	APPLE APPLE-SA-2012-09-19-2 ⁹⁹⁰⁶ BID 51407 ⁹⁹⁰⁷ CVE CVE-2012-0031 ⁹⁹⁰⁸ IAVM 2012-A-0017 ⁹⁹⁰⁹ REDHAT RHSA-2012:0128 ⁹⁹¹⁰ SECUNIA 47410 ⁹⁹¹¹ SECUNIA 48551 ⁹⁹¹² URL1 ⁹⁹¹³ URL2 ⁹⁹¹⁴	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
11.	Apache HTTPD: mod_proxy_ajp remote DoS (CVE-2012-4557) (apache-httpd-cve-2012-4557)	172.23.202.125:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ajp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven kada se mod_proxy_ajp koristi zajedno sa mod_proxy_balancer. Sa specifičnom konfiguracijom, udaljeni napadač može da pošalje zlonameran HTTP zahtev, prouzrokujući da backend server bude stavljen u status greške dok ne istekne vreme za ponovni pokušaj. To bi dovelo do odbijanja servisa.	CVE CVE-2012-4557 ⁹⁹¹⁵ DEBIAN DSA-2579 ⁹⁹¹⁶ URL1 ⁹⁹¹⁷	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
12.	Apache HTTPD: mod_rewrite log escape filtering (CVE-2013-1862) (apache-httpd-cve-2013-1862)	172.23.202.125:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_rewrite. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Modul mod_rewrite ne filtrira završne izlazne sekvence iz logova, što zlonamenom napadaču olakšava da	CVE CVE-2013-1862 ⁹⁹¹⁸ OVAL OVAL18790 ⁹⁹¹⁹ REDHAT RHSA-2013:0815 ⁹⁹²⁰ REDHAT RHSA-2013:1207 ⁹⁹²¹ REDHAT RHSA-2013:1208 ⁹⁹²² REDHAT RHSA-	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and

⁹⁹⁰⁶ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁹⁹⁰⁷ <http://www.securityfocus.com/bid/51407>⁹⁹⁰⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0031>⁹⁹⁰⁹ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁹¹⁰ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>⁹⁹¹¹ <http://secunia.com/advisories/47410/>⁹⁹¹² <http://secunia.com/advisories/48551/>⁹⁹¹³ http://httpd.apache.org/security/vulnerabilities_20.html⁹⁹¹⁴ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁹¹⁵ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4557>⁹⁹¹⁶ <http://www.debian.org/security/2012/dsa-2579>⁹⁹¹⁷ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁹¹⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1862>⁹⁹¹⁹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18790>⁹⁹²⁰ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁹⁹²¹ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁹⁹²² <http://rhn.redhat.com/errata/RHSA-2013-1208.html>

		ubace takve sekvence u završne emulatore koji sadrže ranjivosti koje se odnose na izlazne sekvence.	2013:1209 ⁹⁹²³ SECUNIA 55032 ⁹⁹²⁴ URL1 ⁹⁹²⁵ URL2 ⁹⁹²⁶		< 2.2.25 Ažurirati na Apache HTTPD version 2.2.25 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.25.tar.gz
13.	Apache HTTPD: mod_proxy_ajp remote DoS (CVE-2011-3348) (apache-httpd-cve-2011-3348)	172.23.202.125:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_proxy_ajp. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven kada se mod_proxy_ajp koristi zajedno sa mod_proxy_balancer. Sa specifičnom konfiguracijom, udaljeni napadač može da pošalje zlonameran HTTP zahtev, prouzrokujući da backend server bude stavljen u status greške dok ne istekne vreme za ponovni pokušaj. To bi dovelo do odbijanja servisa.	APPLE APPLE-SA-2012-02-01-1 ⁹⁹²⁷ BID 49616 ⁹⁹²⁸ CVE CVE-2011-3348 ⁹⁹²⁹ IAVM 2012-B-0056 ⁹⁹³⁰ OVAL OVAL14941 ⁹⁹³¹ OVAL OVAL18154 ⁹⁹³² REDHAT RHSA-2011:1391 ⁹⁹³³ SECUNIA 46013 ⁹⁹³⁴ XF 69804 ⁹⁹³⁵ URL1 ⁹⁹³⁶	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.21 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.21.tar.gz
14.	Apache HTTPD: mod_setenvif.htaccess privilege escalation (CVE-2011-3607) (apache-httpd-cve-2011-3607)	172.23.202.125:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_setenvif. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust preopterećenja je otkriven kada je omogućen modul mod_setenvif, što lokalnim korisnicima omogućava da dobiju privilegije preko fajla .htaccess.	APPLE APPLE-SA-2012-09-19-2 ⁹⁹³⁷ BID 50494 ⁹⁹³⁸ CVE CVE-2011-3607 ⁹⁹³⁹ IAVM 2012-A-0017 ⁹⁹⁴⁰ IAVM 2012-A-0152 ⁹⁹⁴¹ OSVDB 76744 REDHAT RHSA-2012:0128 ⁹⁹⁴² SECUNIA 45793 ⁹⁹⁴³ SECUNIA 48551 ⁹⁹⁴⁴ XF 71093 ⁹⁹⁴⁵ URL1 ⁹⁹⁴⁶ URL2 ⁹⁹⁴⁷	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
15.	Apache HTTPD: mod_proxy reverse proxy exposure (CVE-	172.23.202.125:80 Skenirani servis je osetljiv na ovu ranjivost samo ako je pokrenut modul	APPLE APPLE-SA-2012-09-19-2 ⁹⁹⁴⁸ CVE CVE-2011-4317 ⁹⁹⁴⁹	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.22 Uradi download a zatim

⁹⁹²³ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>
⁹⁹²⁴ <http://secunia.com/advisories/55032/>
⁹⁹²⁵ http://httpd.apache.org/security/vulnerabilities_20.html
⁹⁹²⁶ http://httpd.apache.org/security/vulnerabilities_22.html
⁹⁹²⁷ <http://lists.apple.com/archives/security-announce/2012/Feb/msg00000.html>
⁹⁹²⁸ <http://www.securityfocus.com/bid/49616>
⁹⁹²⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3348>
⁹⁹³⁰ <http://iase.disa.mil/stigs/iavm-cve.html>
⁹⁹³¹ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:14941>
⁹⁹³² <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18154>
⁹⁹³³ <http://rhn.redhat.com/errata/RHSA-2011-1391.html>
⁹⁹³⁴ <http://secunia.com/advisories/46013/>
⁹⁹³⁵ <http://xforce.iss.net/xforce/xfdb/69804>
⁹⁹³⁶ http://httpd.apache.org/security/vulnerabilities_22.html
⁹⁹³⁷ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>
⁹⁹³⁸ <http://www.securityfocus.com/bid/50494>
⁹⁹³⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3607>
⁹⁹⁴⁰ <http://iase.disa.mil/stigs/iavm-cve.html>
⁹⁹⁴¹ <http://iase.disa.mil/stigs/iavm-cve.html>
⁹⁹⁴² <http://rhn.redhat.com/errata/RHSA-2012-0128.html>
⁹⁹⁴³ <http://secunia.com/advisories/45793/>
⁹⁹⁴⁴ <http://secunia.com/advisories/48551/>
⁹⁹⁴⁵ <http://xforce.iss.net/xforce/xfdb/71093>
⁹⁹⁴⁶ http://httpd.apache.org/security/vulnerabilities_20.html
⁹⁹⁴⁷ http://httpd.apache.org/security/vulnerabilities_22.html
⁹⁹⁴⁸ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>
⁹⁹⁴⁹ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4317>

	2011-4317) (apache-httpd-cve-2011-4317)	mod_proxy. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Ranjivost na DOS napad otkrivena je u modulu mod_proxy ukoliko se on koristi kao reverzni proxy U određenim konfiguracijama koje koriste RewriteRule sa proxy flag-om ili ProxyPassMatch, udaljeni napadač bi mogao da primora reverzni proksi da se poveže sa proizvoljnim serverom i potencijalno objavi osetljive informacije sa internih web servera koje inače napadaču nisu direktno dostupne.	IAVM 2012-A-0017 ⁹⁹⁵⁰ IAVM 2012-A-0152 ⁹⁹⁵¹ REDHAT RHSA-2012:0128 ⁹⁹⁵² SECUNIA 48551 ⁹⁹⁵³ URL1 ⁹⁹⁵⁴		instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
16.	Apache HTTPD: error responses can expose cookies (CVE-2012-0053) (apache-httpd-cve-2012-0053)	172.23.202.125:80 Propust je otkriven u difoltnom pogrešnom odgovoru za statusni kôd 400. Zlonamerni napadač bi mogao da iskoristi ovaj propust da objavi "httpOnly" kolačiće ako nije određen dokument custom ErrorDocument.	APPLE APPLE-SA-2012-09-19-2 ⁹⁹⁵⁵ BID 51706 ⁹⁹⁵⁶ CVE CVE-2012-0053 ⁹⁹⁵⁷ IAVM 2012-A-0017 ⁹⁹⁵⁸ REDHAT RHSA-2012:0128 ⁹⁹⁵⁹ SECUNIA 48551 ⁹⁹⁶⁰ URL1 ⁹⁹⁶¹ URL2 ⁹⁹⁶²	Ozbiljan	Apache HTTPD >= 2.0 and < 2.0.65 Ažurirati na Apache HTTPD version 2.0.65 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.0.65.tar.gz Apache HTTPD >= 2.2 and < 2.2.22 Ažurirati na Apache HTTPD version 2.2.22 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz
17.	Apache HTTPD: XSS due to unescaped hostnames (CVE-2012-3499) (apache-httpd-cve-2012-3499)	172.23.202.125:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut jedan od sledećih modula: mod_imagemap, mod_info, mod_ldap, mod_proxy_ftp, mod_status. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Različiti XSS propusti usled nenapuštenih host imena i URI-ja HTML output-a u mod_info, mod_status, mod_imagemap, mod_ldap i mod_proxy_ftp.	APPLE APPLE-SA-2013-09-12-1 ⁹⁹⁶³ CVE CVE-2012-3499 ⁹⁹⁶⁴ DEBIAN DSA-2637 ⁹⁹⁶⁵ REDHAT RHSA-2013:0815 ⁹⁹⁶⁶ REDHAT RHSA-2013:1207 ⁹⁹⁶⁷ REDHAT RHSA-2013:1208 ⁹⁹⁶⁸ REDHAT RHSA-2013:1209 ⁹⁹⁶⁹ SECUNIA 55032 ⁹⁹⁷⁰ URL1 ⁹⁹⁷¹ URL2 ⁹⁹⁷²	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.24 Ažurirati na Apache HTTPD version 2.2.24 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz Apache HTTPD >= 2.4 and < 2.4.4 Ažurirati na Apache HTTPD version 2.4.4 Uradi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz

⁹⁹⁵⁰ <http://iase.disa.mil/stigs/iavm-cve.html>
⁹⁹⁵¹ <http://iase.disa.mil/stigs/iavm-cve.html>
⁹⁹⁵² <http://rhn.redhat.com/errata/RHSA-2012-0128.html>
⁹⁹⁵³ <http://secunia.com/advisories/48551/>
⁹⁹⁵⁴ http://httpd.apache.org/security/vulnerabilities_22.html
⁹⁹⁵⁵ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>
⁹⁹⁵⁶ <http://www.securityfocus.com/bid/51706>
⁹⁹⁵⁷ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0053>
⁹⁹⁵⁸ <http://iase.disa.mil/stigs/iavm-cve.html>
⁹⁹⁵⁹ <http://rhn.redhat.com/errata/RHSA-2012-0128.html>
⁹⁹⁶⁰ <http://secunia.com/advisories/48551/>
⁹⁹⁶¹ http://httpd.apache.org/security/vulnerabilities_20.html
⁹⁹⁶² http://httpd.apache.org/security/vulnerabilities_22.html
⁹⁹⁶³ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>
⁹⁹⁶⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3499>
⁹⁹⁶⁵ <http://www.debian.org/security/2013/dsa-2637>
⁹⁹⁶⁶ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>
⁹⁹⁶⁷ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>
⁹⁹⁶⁸ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>
⁹⁹⁶⁹ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>
⁹⁹⁷⁰ <http://secunia.com/advisories/55032/>
⁹⁹⁷¹ http://httpd.apache.org/security/vulnerabilities_22.html
⁹⁹⁷² http://httpd.apache.org/security/vulnerabilities_24.html

18.	Apache HTTPD: XSS in mod_proxy_balancer (CVE-2012-4558) (apache-httpd-cve-2012-4558)	172.23.202.125:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_proxy_balancer. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. XSS propust je uticao na manager interfejs mod_proxy_balancer-a.	APPLE APPLE-SA-2013-09-12-1 ⁹⁹⁷³ CVE CVE-2012-4558 ⁹⁹⁷⁴ DEBIAN DSA-2637 ⁹⁹⁷⁵ REDHAT RHSA-2013:0815 ⁹⁹⁷⁶ REDHAT RHSA-2013:1207 ⁹⁹⁷⁷ REDHAT RHSA-2013:1208 ⁹⁹⁷⁸ REDHAT RHSA-2013:1209 ⁹⁹⁷⁹ URL1 ⁹⁹⁸⁰ URL2 ⁹⁹⁸¹	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.24 Ažurirati na Apache HTTPD version 2.2.24 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.24.tar.gz Apache HTTPD >= 2.4 and < 2.4.4 Ažurirati na Apache HTTPD version 2.4.4 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.4.tar.gz
19.	Apache HTTPD: mod_dav crash (CVE-2013-1896) (apache-httpd-cve-2013-1896)	172.23.202.125:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_dav_svn. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Slanje MERGE zahteva URI-ju koji obrađuje mod_dav_svn sa izvorom href (poslato kao deo zahteva XML) ciljajući na URI koji nije konfigurisan za DAV prouzrokuje segmentation fault (segfault).	CVE CVE-2013-1896 ⁹⁹⁸² OVAL OVAL18835 ⁹⁹⁸³ REDHAT RHSA-2013:1156 ⁹⁹⁸⁴ REDHAT RHSA-2013:1207 ⁹⁹⁸⁵ REDHAT RHSA-2013:1208 ⁹⁹⁸⁶ REDHAT RHSA-2013:1209 ⁹⁹⁸⁷ SECUNIA 55032 ⁹⁹⁸⁸ URL1 ⁹⁹⁸⁹ URL2 ⁹⁹⁹⁰	Ozbiljan	Apache HTTPD >= 2.2 and < 2.2.25 Ažurirati na Apache HTTPD version 2.2.25 Apache HTTPD >= 2.4 and < 2.4.6 Ažurirati na Apache HTTPD version 2.4.6 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.6.tar.gz
20.	Apache HTTPD: mod_log_config crash (CVE-2012-0021) (apache-httpd-cve-2012-0021)	172.23.202.125:80 Skenirani servis je ranjiv ukoliko je na njemu pokrenut modul: mod_log_config. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Propust je otkriven u modulu mod_log_config. Ako je u upotrebi '%{cookienam}C' log format string, udaljeni napadač bi mogao da pošalje specifičan kolačić koji bi doveo do kraha. Krah bi se pokazao kao odbijanje servisa ako se koristi threaded MPM.	APPLE APPLE-SA-2012-09-19-2 ⁹⁹⁹¹ CVE CVE-2012-0021 ⁹⁹⁹² IAVM 2012-A-0017 ⁹⁹⁹³ SECUNIA 48551 ⁹⁹⁹⁴ URL1 ⁹⁹⁹⁵	Umeren	Apache HTTPD >= 2.2 and < 2.2.22 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.22.tar.gz

⁹⁹⁷³ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁹⁹⁷⁴ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4558>⁹⁹⁷⁵ <http://www.debian.org/security/2013/dsa-2637>⁹⁹⁷⁶ <http://rhn.redhat.com/errata/RHSA-2013-0815.html>⁹⁹⁷⁷ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁹⁹⁷⁸ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁹⁹⁷⁹ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁹⁹⁸⁰ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁹⁸¹ http://httpd.apache.org/security/vulnerabilities_24.html⁹⁹⁸² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1896>⁹⁹⁸³ <http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:18835>⁹⁹⁸⁴ <http://rhn.redhat.com/errata/RHSA-2013-1156.html>⁹⁹⁸⁵ <http://rhn.redhat.com/errata/RHSA-2013-1207.html>⁹⁹⁸⁶ <http://rhn.redhat.com/errata/RHSA-2013-1208.html>⁹⁹⁸⁷ <http://rhn.redhat.com/errata/RHSA-2013-1209.html>⁹⁹⁸⁸ <http://secunia.com/advisories/55032/>⁹⁹⁸⁹ http://httpd.apache.org/security/vulnerabilities_22.html⁹⁹⁹⁰ http://httpd.apache.org/security/vulnerabilities_24.html⁹⁹⁹¹ <http://lists.apple.com/archives/security-announce/2012/Sep/msg00004.html>⁹⁹⁹² <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0021>⁹⁹⁹³ <http://iase.disa.mil/stigs/iavm-cve.html>⁹⁹⁹⁴ <http://secunia.com/advisories/48551/>⁹⁹⁹⁵ http://httpd.apache.org/security/vulnerabilities_22.html

21.	Apache HTTPD: XSS in mod_negotiation when untrusted uploads are supported (CVE-2012-2687) (apachehttpd-cve-2012-2687)	172.23.202.125:80 Skenirani servis je osetljiv na ovu ranjivost SAMO ako izvršava jedan od sledećih modula: mod_negotiation. Proveriti konfiguraciju web servera radi utvrđivanja ove mogućnosti. Moguće je ubaciti CRLF (Carriage Return and Line Feed) koji omogućava CRLF Injection napade (poznatih i kao HTTP Response Splitting) za sajtove koji koriste mod_negotiation, omogućavajući neproverene upload-ove na lokacije na kojima je omogućen MultiViews (višestruko pregledanje). Ovaj problem je poznat i kao CVE-2008-0455.	APPLE APPLE-SA-2013-09-12-1 ⁹⁹⁹⁶ BID 55131 ⁹⁹⁹⁷ CVE CVE-2012-2687 ⁹⁹⁹⁸ IAVM 2012-A-0139 ⁹⁹⁹⁹ REDHAT RHSA-2012:1591 ¹⁰⁰⁰⁰ REDHAT RHSA-2012:1592 ¹⁰⁰⁰¹ REDHAT RHSA-2012:1594 ¹⁰⁰⁰² REDHAT RHSA-2013:0130 ¹⁰⁰⁰³ SECUNIA 50894 ¹⁰⁰⁰⁴ SECUNIA 51607 ¹⁰⁰⁰⁵ URL1 ¹⁰⁰⁰⁶ URL2 ¹⁰⁰⁰⁷	Umeren	Apache HTTPD >= 2.2 and < 2.2.23 Ažurirati na Apache HTTPD version 2.2.23 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.2.23.tar.gz Apache HTTPD >= 2.4 and < 2.4.3 Ažurirati na Apache HTTPD version 2.4.3 Uraditi download a zatim instalirati: http://archive.apache.org/dist/httpd/httpd-2.4.3.tar.gz
22.	TCP timestamp response (generic-tcp-timestamp)	Udaljeni host je odgovorio sa TCP vremenskim pečatom. TCP odgovor sa vremenskim pečatom koristi se za procenu vremena neprekidnog rada udaljenog hosta, što zlonamerni napadač može iskoristiti pri planiranju daljih napada. Određeni operativni sistemi mogu biti prepoznati na osnovu osobina njihovih TCP vremenskih pečata.	URL1 ¹⁰⁰⁰⁸ URL2 ¹⁰⁰⁰⁹ URL3 ¹⁰⁰¹⁰	Umeren	Onemogućavanje TCP timestamp odgovora na Linux OS. Podesiti net.ipv4.tcp_timestamps vrednost na sledećem ključu na 0 pokretanjem sledeće komande: sysctl -w net.ipv4.tcp_timestamps=0 Dodatno, sledeću vrednost u difoltnom sysctl konfiguracionom fajlu, generally sysctl.conf: net.ipv4.tcp_timestamps=0

⁹⁹⁹⁶ <http://lists.apple.com/archives/security-announce/2013/Sep/msg00002.html>⁹⁹⁹⁷ <http://www.securityfocus.com/bid/55131>⁹⁹⁹⁸ <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2687>⁹⁹⁹⁹ <http://iase.disa.mil/stigs/iavm-cve.html>¹⁰⁰⁰⁰ <http://rhn.redhat.com/errata/RHSA-2012-1591.html>¹⁰⁰⁰¹ <http://rhn.redhat.com/errata/RHSA-2012-1592.html>¹⁰⁰⁰² <http://rhn.redhat.com/errata/RHSA-2012-1594.html>¹⁰⁰⁰³ <http://rhn.redhat.com/errata/RHSA-2013-0130.html>¹⁰⁰⁰⁴ <http://secunia.com/advisories/50894/>¹⁰⁰⁰⁵ <http://secunia.com/advisories/51607/>¹⁰⁰⁰⁶ http://httpd.apache.org/security/vulnerabilities_22.html¹⁰⁰⁰⁷ http://httpd.apache.org/security/vulnerabilities_24.html¹⁰⁰⁰⁸ http://www.forensicswiki.org/wiki/TCP_timestamps¹⁰⁰⁰⁹ <http://www.ietf.org/rfc/rfc1323.txt>¹⁰⁰¹⁰ <http://uptime.netcraft.com/>