

GLESEC INCIDENT REPORT

TLP-AMBAR

Organization	Institute of Electrical and Electronics Engineers
Date	9/08/2018
Service	MSS-VME
Severity Level	Critical
Impact Level	Critical
Vulnerability Level	Critical

INCIDENT DESCRIPTION

In recent days, our Operations Center (GOC) detected an "irregular" situation with the results obtained from our MSS-VME service for the IEEE client.

We have seen a very noticeable reduction of 357 hosts inspected in the June report to 291 hosts the last week of the month of July. Following up, on August 6 we conducted a new inspection with further decrease from 291 hosts to 261 reachable systems.

It is very important to determine if the loss of visibility of these systems is due to the fact that they have been shutdown or made unavailable to our testing.

The following is the list most recent of the unreachable systems for our service, many of these IPs present vulnerabilities regarding missing updates or old versions: "Microsoft IIS 6.0 Unsupported Version Detection" and "Microsoft IIS 6.0 Unsupported Version Detection"

This list is based on the 357 hosts inspected during the month of June, of which we do not have access to 96 systems.

CONFIDENTIAL

GLESEC INCIDENT REPORT

TLP-AMBAR

- | | | |
|-------------------|--------------------|--------------------|
| 1. 140.98.193.127 | 17. 140.98.194.65 | 33. 140.98.194.160 |
| 2. 140.98.194.50 | 18. 140.98.194.79 | 34. 140.98.194.161 |
| 3. 140.98.194.51 | 19. 140.98.194.81 | 35. 140.98.194.162 |
| 4. 140.98.194.52 | 20. 140.98.194.82 | 36. 140.98.194.163 |
| 5. 140.98.194.53 | 21. 140.98.194.83 | 37. 140.98.194.164 |
| 6. 140.98.194.54 | 22. 140.98.194.85 | 38. 140.98.194.165 |
| 7. 140.98.194.55 | 23. 140.98.194.86 | 39. 140.98.194.166 |
| 8. 140.98.194.56 | 24. 140.98.194.87 | 40. 140.98.194.167 |
| 9. 140.98.194.57 | 25. 140.98.194.88 | 41. 140.98.194.168 |
| 10. 140.98.194.58 | 26. 140.98.194.89 | 42. 140.98.194.169 |
| 11. 140.98.194.59 | 27. 140.98.194.90 | 43. 140.98.194.170 |
| 12. 140.98.194.60 | 28. 140.98.194.95 | 44. 140.98.194.171 |
| 13. 140.98.194.61 | 29. 140.98.194.113 | 45. 140.98.194.172 |
| 14. 140.98.194.62 | 30. 140.98.194.157 | 46. 140.98.194.173 |
| 15. 140.98.194.63 | 31. 140.98.194.158 | 47. 140.98.194.174 |
| 16. 140.98.194.64 | 32. 140.98.194.159 | 48. 140.98.194.175 |

CONFIDENTIAL

GLESEC INCIDENT REPORT

TLP-AMBAR

49. 140.98.194.176	65. 140.98.202.12	81. 140.198.196.173
50. 140.98.194.177	66. 140.98.202.55	82. 140.198.196.181
51. 140.98.194.178	67. 140.98.202.62	83. 140.198.196.183
52. 140.98.194.179	68. 140.98.202.173	84. 140.198.196.191
53. 140.98.194.185	69. 140.98.202.176	85. 140.198.196.192
54. 140.98.194.189	70. 140.98.202.187	86. 140.198.196.193
55. 140.98.194.192	71. 140.98.202.240	87. 140.198.196.194
56. 140.98.194.196	72. 140.98.202.246	88. 140.198.196.196
57. 140.98.194.197	73. 140.98.202.252	89. 140.198.196.197
58. 140.98.194.200	74. 208.99.166.233	90. 140.198.196.198
59. 140.98.194.202	75. 208.99.166.243	91. 140.98.200.131
60. 140.98.194.203	76. 140.98.194.96	92. 140.98.202.200
61. 140.98.194.206	77. 140.98.194.99	93. 140.98.200.27
62. 140.98.194.218	78. 140.98.196.162	94. 140.98.194.204
63. 140.98.196.182	79. 140.198.196.164	95. 140.98.202.33
64. 140.98.200.75	80. 140.198.196.165	96. 140.98.202.189

CONFIDENTIAL



www.glesec.com

GLESEC INCIDENT REPORT

TLP-AMBAR

PROTOCOLO DE COMPARTICION DE INFORMACION DE GLESEC

LOS REPORTES DE INCIDENCIAS DE CYBERSEGURIDAD DE GLESEC están en cumplimiento con el protocolo de Semáforo (TLP) del Departamento de Seguridad de Estado de Estados Unidos (DHS): TLP -Blanco (Divulgación no limitada), TLP-Verde (Divulgación Limitada, Restringida, solo para la comunidad), TLP-Ámbar (Divulgación Limitada, Restringida, Para los participantes de la Organización) y TLP-Rojo (No Divulgación, Restringida/Confidencial – Solo compartida con el US DHS).

CONFIDENTIAL



Page 4