GLESEC INCIDENT REPORT

TLP-AMBER

Organization	Inspira Health Network
Date	June 5th 2018
Service	MSS-VME
Severity Level	High
Impact Level	High
Vulnerability Level	High

INCIDENT DESCRIPTION

Our GOC detected the implementation of TLS 1.0 protocol on some of your systems. TLS 1.0 has a number of cryptographic flaws (in its design) that makes this protocol more susceptible to certain attacks. The newer versions of TLS, TLS 1.1 and TLS 1.2 are designed against these flaws. GLESEC recommends to enable TLS 1.2, and if possible and does not represent an availability flaw, enable the recently approved TLS 1.3.

The affected systems are the following:

- 170.75.32.15
- 170.75.33.134
- 170.75.33.139
- 170.75.33.55
- 170.75.49.35

The standard PCI-DSS v3.2.1, published on May 17th, 2018, established that TLS 1.0 and SSL (this category is called SSL and Early TLS) should be disabled entirely by June 30, 2018 except for POS POI terminals that are verified as not being susceptible to known exploits.

COMMENTS AND RECOMMENDATIONS

TLS Implementations should be upgraded to version 1.2 at least and only enable TLS connections with version 1.2 (or 1.3 if applicable). This should be done in external servers; and in endpoints, it should be verified that the web browsers are kept up to date and if they are using TLS 1.2. For additional reference, the following blog by the PCI Security Standards Council has additional information: https://blog.pcisecuritystandards.org/what-happens-after-30-june-2018-new-guidance-on-use-of-ssl/early-tls-.

- SSL Labs has a site to test which TLS implementations are currently in use in your systems https://www.ssllabs.com/ssltest/viewMyClient.html

GLESEC INCIDENT REPORT

TLP-AMBER

GLESEC INFORMATION SHARING PROTOCOL

GLESEC CYBER SECURITY INCIDENTE REPORTS are in compliance with the U.S. Department of Homeland Security (DHS) Traffic-Light Protocol (TLP): TLP-White (Disclosure is Not Limited), TLP-Green (Limited Disclosure, Restricted Only to the Community), TLP-Amber (Limited Disclosure, Restricted to the Participant's Organization), and TLP-Red (Not for Disclosure, Restricted/ Classified - Only Shared with US DHS).