GLESEC INCIDENT REPORT

TLP-AMBER

Organization	Inspira Health Network.
Date	10/26/2018
Service	MSS-VM
Severity Level	High
Impact Level	High
Vulnerability Level	High

INCIDENT DESCRIPTION

GLESEC Operation's Center discovered 1 high severity vulnerability on five different hosts, it was detected that SSL Version 2 and/or 3 Protocol was enabled on hosts: 170.75.49.35, 170.75.33.139, 170.75.33.136, 170.75.33.166 and 170.75.33.55.

ACTIONS TO BE TAKEN

SSL Version 2 and 3 should be disabled, these versions of the protocol are known to be vulnerable to many types of attacks, TLS v1.2 or higher should be enabled instead. This should be done following the change control policy of the company.

COMMENTS AND RECOMMENDATIONS

GLESEC recommends mitigating this vulnerability as soon as possible.

An attacker can exploit these vulnerabilities and conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients. Although SSL/TLS has a secure means for only using these versions of the protocol if the client or server do not support something more secure. many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE attack). Therefore, it is recommended that these protocols be disabled entirely.

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).