GLESEC INCIDENT REPORT

TLP-AMBER

Organization	Inspira Health Network
Date	11/27/2018
Service	MSS-VME
Severity Level	Medium
Impact Level	Medium
Vulnerability Level	Medium

INCIDENT DESCRIPTION

Our GOC presents you a summary of the vulnerabilities present in your systems.

- SSL vulnerabilities including: SSL Medium Strength Cipher Suites, SSL RC4 Cipher suite supported (Bar Mitzvah), SSLv3 POODLE vulnerability, SSL with Diffie-Hellman module less than 1024 bits LOGJAM, SSLv2 and v3 detection, SSL Null cipher suites. These vulnerabilities affect the following hosts: 170.75.33.137, 170.75.33.139, 170.75.49.35, 170.75.33.186, 170.75.32.15, 170.75.33.169, 170.75.33.167, 170.75.33.152, 170.75.33.141, 170.75.33.133, 170.75.33.125, 170.75.33.124, 170.75.33.123, 170.75.33.122, 170.75.33.119, 170.75.33.112.

- Disclosure of Internal IP of the Web Server affecting hosts: 170.75.33.142, 170.75.33.169, 170.75.49.35.

- Internet Key Exchange (IKE) Aggressive mode with Pre-Shared Key affecting hosts: 170.75.32.1, 170.75.48.100.

- Microsoft Exchange CAS Server information Disclosure affecting host 170.75.49.35.

- A Critical vulnerability MS15-034: Vulnerability in HTTP.sys could allow remote code execution (uncredentialled check) affecting host 170.75.33.152

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

GLESEC INCIDENT REPORT

TLP-AMBER

for POS POI terminals that are verified as not being susceptible to known exploits.

The Internal IP disclosure is a known issue with different versions of IIS in their default configuration.

The CAS vulnerability was fixed in a security patch, Microsoft recommends keeping software up to date to fix any vulnerabilities.

The critical vulnerability in HTTP.sys could allow a remote attacker obtain complete control over the affected system when exploiting this vulnerability by executing remote code.

Using pre-shared keys in aggresive mode for IKE protocol could allow an attacker to capture a packet of the transmission and attempt to crack the pre-shared key of the VPN Gateway.

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

For the internal IP disclosure, Microsoft corrected this issue for IIS 6.0 in Service Pack 1 for Windows Server 2003, for other versions of IIS Microsoft suggests reconfiguring certain files as

GLESEC INCIDENT REPORT

TLP-AMBER

specified in the article: https://support.microsoft.com/en-us/help/834141/fix-ip-address-is-revealed-in-the-content-location-field-in-the-tcp-he

For the IKE protocol is recommended to disable the aggressive mode if pre-shared keys are used, if aggressive mode must be used then strong pre-shared keys are recommended.

The critical vulnerability in HTTP.sys was patched by Microsoft with additional information regarding the patch and vulnerability information in: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2015/ms15-034

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).

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355