OPERATIONS & INTELLIGENCE TECHNICAL CYBER SECURITY REPORT

Inspira Health Network

June 2018

Tel: +1 609-651-4246
Tel: +507-836-5355

Info@glesec.com
www.glesec.com

Table of Contents

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

About This Report

This report is a companion to the Monthly Operations & Intelligence Executive Report. The purpose of this document is to provide Technical and Tactical level information, detail and recommendations to the extent that can be summarized. GLESEC processes significant amount of data and not all can be presented in a detail report format. For more information you can review the dashboards of the GMP or if necessary contact us at the GLESEC Operation Centers (GOC).

Confidentiality

GLESEC considers the confidentiality of client's information as a trade secret. The information in this context is classified as:

- Client name and contact information
- System architecture, configuration, access methods and access control
- Security content

All the above information is kept secure to the extent in which GLESEC secures its own confidential information.

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

Managed Vulnerability Service (MSS-VM)

The Managed Vulnerability Service (MSS-VM) enables organizations to minimize the risk of vulnerabilities by quickly discovering weaknesses, measuring the potential risk and exposure, reporting, providing remediation information necessary to mitigate those risks on an on-going basis and facilitating reporting and compliance with regulations and best practices.

In the range of addresses provided by Inspira Health Network, we have found a total of 58 hosts, of which 8 are vulnerable. These vulnerabilities are divided into the following severities, as shown in the following table. In addition, you can observe the Risk Value score of your organization according to our metrics.

Total IP's Scanned	IP's Vulnerable
58	8

Risk Distribution				
Critical	High	Medium	Low	Total
0	9	17	10	36

According to the metrics:

RV= 0.062260536

The following values are to clarify RV:
RV=1 Points to every IP address in the infrastructure that are susceptible to attacks
RV=0 Points to no IP address in the infrastructure aret susceptible to attacks
RV=0.1 Point to 1/10 IP address in the infrastructure that are susceptible to attacks

All the vulnerabilities found in your organization belong to the following categories:

Category	Critical	High	Medium	Low	Total
General		0	16	5	21
Service detection		9	0	0	9
Misc.		0	0	3	3
Web Servers		0	0	2	2
Windows		0	1	0	1

- General (58.33 %).
- Service detection (25%).

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

- Misc. (8.33%).
- Web Servers (6%).
- Windows (2.8%).

Additional details about these vulnerabilities are presented in the Vulnerabilities found in Inspira Health Network by severity section of the MSS-VM **on page 8.**

TLS Version 1.0 Protocol Detection is the high risk vulnerability in your organization. We recommend implementing the recommendation that our GLESEC analyst team provides.

The vulnerability that occurs most frequently is SSL Medium Strength Cipher Suites Supported and belongs to the General category.

Next, the most vulnerable hosts will be displayed:

- Hosts 170.75.33.134 and 170.75.33.139 (19%) have vulnerabilities of the General category such as SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE), SSL Certificate Cannot Be Trusted and SSL / TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) of the category Misc.
- Host 170.75.49.35 (19%) has vulnerabilities of the Windows category such as Microsoft Exchange Client Access Server Information Disclosure and SSL Version 2 and 3 Protocol Detection of the Service Detection category.
- Host 170.75.32.15 (13%) has vulnerabilities of the General category such as Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key and SSL RC4 Cipher Suites Supported (Bar Mitzvah).

These vulnerabilities represent a medium risk which means that the attackers could take advantage of them and try to cause a negative impact on your organization. Many of these hosts have vulnerability in the TCP protocol.

Ports 443, 4443 and 500 are the most vulnerable ports for this period; this is because they found many vulnerabilities that are related to them and are classified as medium risk. Only host 170.75.32.15 is vulnerable by the UDP protocol and port 500, presents a medium risk level in the Internet Key Exchange (IKE) vulnerability Aggressive Mode with Pre-Shared Key.

Other ports and categories that are few vulnerable are: Ports 25, 53 and 80 in the Port Scanners category, port 53 in the DNS category and port 0 in the Settings category.

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

Descriptions by Host

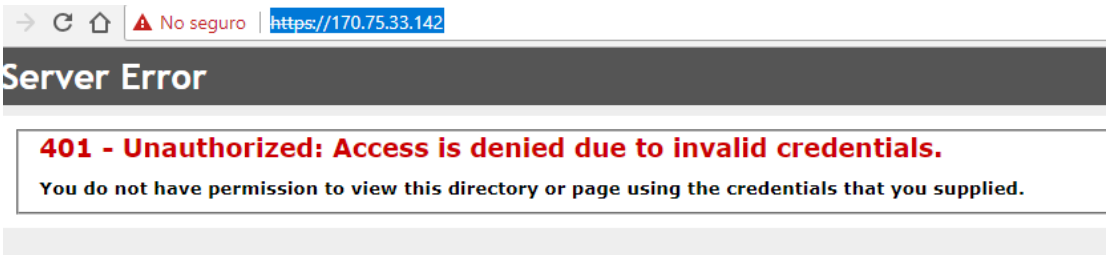
The remote host https://170.75.33.134/ is vulnerable to SSL / TLS Diffie-Hellman Modulus <= 1024 bits (Logjam) that is, it allows SSL/TLS connections with one or more Diffie-Hellman modules less than or equal to 1024 bits. It is a popular cryptographic algorithm that allows Internet protocols to agree on a shared key and negotiate a secure connection. The Logjam attack allows a male attacker in the middle to degrade vulnerable TLS connections to a 512-bit export-grade cryptography. This allows the attacker to read and modify any data passed through the connection.

The remote host https://170.75.33.139/ is vulnerable to SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) this is a weakness in version 3 of the SSL protocol that allows an attacker in a context of man in the middle to decrypt the plain text content of an SSLv3 encrypted message.
This vulnerability affects all software components that may be forced to communicate with SSLv3.

The following vulnerabilities have been reported previously:

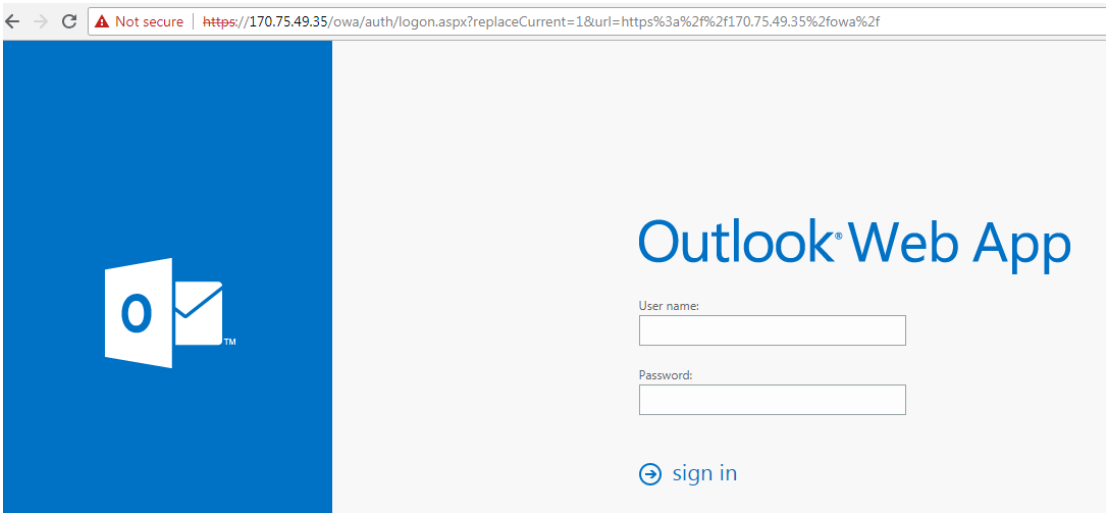
The remote host https://170.75.33.142/ is affected by an integer overflow condition in the HTTP protocol stack (HTTP.sys) due to improper parsing of crafted HTTP requests. An unauthenticated; remote attacker can exploit this to execute arbitrary code with System privileges.
This vulnerability is known as **integer overflows**, where version of Windows running. Microsoft has released a set of patches for Windows 7, 2008 R2, 8, 8.1, 2012, and 2012 R2.

We attach the image, showing the stated above.

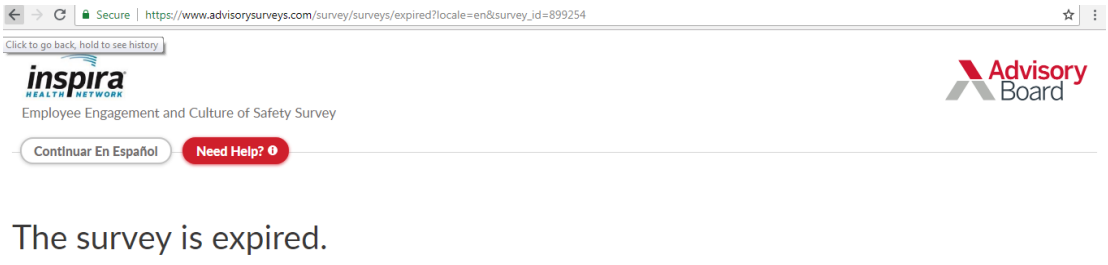


The remote host https://170.75.49.35/ is affected by an information disclosure vulnerability condition called The Microsoft Exchange Client Access Server (CAS). A remote unauthenticated attacker can exploit this vulnerability to know the internal IP address of the server.

We attach the image, showing the stated above.

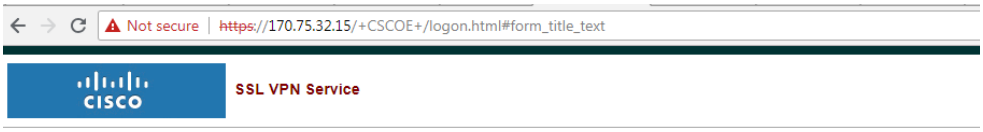


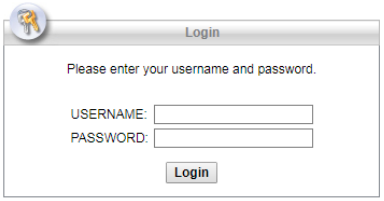
The remote host https://170.75.33.133/ by affected SSL Certificate Signed Using Weak Hashing Algorithm. The SSL certificate that has been signed uses a weak cryptographic algorithm (for example, MD2, MD4, MD5 or SHA1). It is known that these signature algorithms are vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, which allows an attacker to be masqueraded as the affected service.



The remote host https://170.75.32.15 is affected by the IKE version 1 service (Internet Key Exchange) seems to be compatible with aggressive mode with pre-

shared key authentication (PSK). Such a configuration could allow an attacker to capture and crack the PSK of a VPN gateway and gain unauthorized access to private networks.





Vulnerabilities by severity

The following section will describe in detail each vulnerability found according to their severity.

High Risk Level Vulnerabilities

TLS Version 1.0 Protocol Detection

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Affected Systems
443 / tcp / cisco-ssl-vpn-svr 170.75.32.15
5061 / tcp 170.75.33.134
4443 / tcp / possible_wls 170.75.33.134170.75.33.139
443 / tcp 170.75.33.134170.75.33.217
443 / tcp / possible_wls 170.75.33.55170.75.49.35

SSL Version 2 and 3 Protocol Detection

Description
The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

1. An insecure padding scheme with CBC ciphers.

2. Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution
Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.1 (with approved cipher suites) or higher instead.

Affected Systems

4443 / tcp / possible_wls	170.75.33.136, 170.75.33.139
443 / tcp / possible_wls	170.75.33.55, 170.75.49.35

Output

```
- SSLv3 is enabled and the server supports at least one cipher.
```

Medium Risk Level Vulnerabilities

SSL Medium Strength Cipher Suites Supported

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. GLESEC regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note: Reconfigure the affected application if possible to avoid use of medium strength ciphers

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Affected Systems

443 / tcp / cisco-ssl-vpn-svr	170.75.32.15
4443 / tcp / possible_wls	170.75.33.136, 170.75.33.139
443 / tcp / possible_wls	170.75.33.55,170.75.33.131,170.75.33.133, 170.75.33.167, 170.75.33.168, 170.75.33.171, 170.75.49.35

Output

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

```
Here is the list of medium strength SSL ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    DES-CBC3-SHA                Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

SSL Certificate Cannot Be Trusted

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below:

1. First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

2. Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

3. Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

4. If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper certificate for this service.

Affected Systems

443 / tcp / possible_wls 170.75.33.131

Output

```
The following certificate was part of the certificate chain
sent by the remote host, but it has expired :

|-Subject   : C=US/2.5.4.17=08302/ST=NJ/L=Bridgeton/2.5.4.9=333 Irving Ave/O=Inspira Health
Network/OU=IS/OU=Secure Link SSL Wildcard/CN=*.sjhs.com
|-Not After : Dec 17 23:59:59 2016 GMT
```

Affected Systems

443 / tcp / possible_wls 170.75.33.133

Output

```
The following certificate was part of the certificate chain
sent by the remote host, but it has expired :

|-Subject   : C=US/2.5.4.17=08302/ST=NJ/L=Bridgeton/2.5.4.9=333 Irving Ave/O=Inspira Health
Network/OU=Information Systems/OU=Secure Link SSL Wildcard/CN=*.ihn.org
|-Not After : Jun 20 23:59:59 2017 GMT

The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=US/O=Network Solutions L.L.C./CN=Network Solutions Certificate Authority
|-Issuer  : C=US/ST=UT/L=Salt Lake City/O=The USERTRUST
Network/OU=http://www.usertrust.com/CN=UTN-USERFirst-Hardware
```

Affected Systems

443 / tcp / possible_wls 170.75.33.171

Output

```
The following certificate was part of the certificate chain
sent by the remote host, but it has expired :

|-Subject   : C=US/2.5.4.17=08302/ST=NJ/L=Bridgeton/2.5.4.9=333 Irving Ave/O=Inspira Health
Network/OU=Information Systems/OU=Secure Link SSL Wildcard/CN=*.sjhs.com
|-Not After : Dec 06 23:59:59 2015 GMT
```

Affected Systems

4443 / tcp / possible_wls 170.75.33.136,170.75.33.139

Output

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

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=US/ST=New Jersey/L=Bridgeton/O=Inspira Health Network/OU=Information
Systems/CN=ucedgepool.corporate.lan
|-Issuer  : DC=lan/DC=corporate/CN=IHN-CA
```

SSL Certificate Signed Using Weak Hashing Algorithm

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Solution

Contact the Certificate Authority to have the certificate reissued.

Affected Systems

443 / tcp / possible_wls 170.75.33.133

Output

```
The following certificates were part of the certificate chain sent by
the remote host, but contain hashes that are considered to be weak.

|-Subject             : C=US/2.5.4.17=08302/ST=NJ/L=Bridgeton/2.5.4.9=333 Irving Ave/O=Inspira
Health Network/OU=Information Systems/OU=Secure Link SSL Wildcard/CN=*.ihn.org
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Jun 09 00:00:00 2014 GMT
|-Valid To            : Jun 20 23:59:59 2017 GMT
```

SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability(POODLE)

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles

padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.
MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

Note: Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Solution
Disable SSLv3.

Affected Systems

4443 / tcp / possible_wls	170.75.33.136, 170.75.33.139.
443 / tcp / possible_wls	170.75.33.55, 170.75.49.35.

Output

```
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

Microsoft Exchange Client Access Server Information Disclosure

Description
The Microsoft Exchange Client Access Server (CAS) is affected by an information

disclosure vulnerability. A remote, unauthenticated attacker can exploit this vulnerability to learn the server's internal IP address.

Affected Systems

443 / tcp / possible_wls 170.75.49.35

Output

```
GET /autodiscover/autodiscover.xml HTTP/1.0
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

Which returned the following IP address :

10.103.190.210
```

Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key

Description

The remote Internet Key Exchange (IKE) version 1 service seems to support Aggressive Mode with Pre-Shared key (PSK) authentication. Such a configuration could allow an attacker to capture and crack the PSK of a VPN gateway and gain unauthorized access to private networks.

Solution

1. Disable Aggressive Mode if supported.
2. Do not use Pre-Shared key for authentication if it's possible.
3. If using Pre-Shared key cannot be avoided, use very strong keys.
4. If possible, do not allow VPN connections from any IP addresses.

Note that this plugin does not run over IPv6.

Affected Systems

500 / udp / ike 170.75.32.15

Low Risk Level Vulnerabilities

SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Affected Systems

443 / tcp / cisco-ssl-vpn-svr 170.75.32.15

Output

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    RC4-SHA                     Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

Affected Systems

4443 / tcp / possible_wls 170.75.33.136170.75.33.139
443 / tcp / possible_wls 170.75.33.55170.75.49.35

Output

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    RC4-MD5                    Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=MD5
    RC4-SHA                    Kx=RSA         Au=RSA      Enc=RC4(128)            Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Affected Systems

443 / tcp / cisco-ssl-vpn-svr 170.75.32.15

Output

```
Vulnerable connection combinations :

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)
```

Affected Systems

4443 / tcp / possible_wls 170.75.33.136

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

Output

```
Vulnerable connection combinations :

  SSL/TLS version   : TLSv1.1
  Cipher suite      : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version   : TLSv1.1
  Cipher suite      : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version   : TLSv1.0
  Cipher suite      : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version   : TLSv1.0
  Cipher suite      : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)
```

Affected Systems

4443 / tcp / possible_wls 170.75.33.139

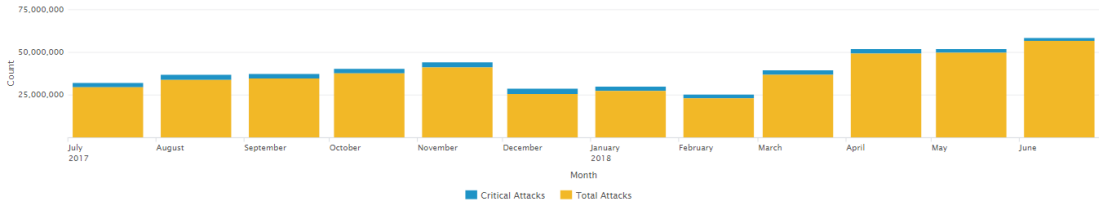
Output

```
Vulnerable connection combinations :

  SSL/TLS version   : TLSv1.1
  Cipher suite      : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version   : TLSv1.1
  Cipher suite      : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version   : TLSv1.0
  Cipher suite      : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version   : TLSv1.0
  Cipher suite      : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)
```

THREATS

GLESEC uses its MSS-APS, MSS-EPS, MSS-SIEM, MSS-EIR and MSS-UTM to determine threat intelligence activity.

The Threats as reported by the MSS-APS, MSS-EPS, MSS-SIEM, MSS-EIR and MSS-UTM for this month are Scanning, Access and Behavorial-DoS. All these threats were identified and dropped.



For this period we observed a 13.62% decrease in critical attacks compared to the previous month and a 16.28% increase in total attacks compared to the previous month.
Most of the attacks that were presented came from the Scanning category, representing 89%, followed by Access with 6% and Behavorial-DoS with 3%.

The following are the countries with the highest percentage of attacks:

- The Russian Federation represents 43%, some of the attacks carried out are TCP Scan, TCP Scan (Horizontal) of the Anti-Scannig category; and Network flood IPv4 TCP-SYN of the Behavorial-DoS category.
- The United States represents 19%, some of the attacks carried out are Ping Sweep of the Anti-Scannig category; and BlackList and Threat List in the Access category.
- Chile represents 11%, some of the attacks carried out are TCP Scan, UDP and Scan (Horizontal) of the Anti-Scanning category.
- China represents 7%, some of the attacks carried out are TCP Scan (Horizontal) of the Anti-Scanning category; network flood IPv4 TCP-SYN-ACK and network flood IPv4 UDP of the Behavorial-DoS category.

Anti-Scannig generally performs polling techniques such as TCP Scan, Ping Sweep and UDP Scan that attackers use to discover entry points to the target system. While Behavorial-DoS performs attacks such as Network Flood, IPv4, TCP-SYN UDP and

Network Flood, IPv4 TCP-SYN (ACK) are used to saturate the network.

Attacks for this period that last more than one hour belong to the Anti-Scanning category, followed by Anomalies and one to five minutes belong to the Behavorial-DoS category. We can mention that the Access category is the one that consumes the most bandwidth.

The TCP and UDP protocols are the most used to perform the attacks, through port 8545 is targeted for scans very frequently, if it is not a necessity to leave it open it would be advisable to close or filter it from traffic from the outside. Ports 1433 and 3389 are also targets for scanners, this ports correspond to SQL Server and IANA registered for Microsoft WBT Server, used for Windows Remote Desktop and Remote Assistance connections (RDP - Remote Desktop Protocol) respectively. All these examples should only be open to the internet if strictly necessary.

Based on the information gathered from the security countermeasures during this period 56,774,059 attacks on Inspira Health Network; 1,939,762 of which were considered critical were all stopped by the GLESEC managed security countermeasures.

Inspira Health Network receives an average of 34,864,448 total attacks and 2,487,505 critical attacks on a monthly basis. This equates to an average of 1,231,265 total daily attacks and 84,875 critical daily attacks.

Top Source IPs (Local or public).

- 46.161.27.30 (Reino Unido)
- 5.188.86.36, 77.72.82.146, 77.72.85.8, 92.63.193.150, 31.192.108.68 (Rusia)
- 181.214.87.14 (Estados Unidos)
- 78.128.112.2 (Bulgaria)

Top Destination IPs (Local or public) targeted
In this section we present the Destination IPs from denied or dropped connections that were most recurrent during this period.

- 170.75.32.5
- 170.75.33.21
- 170.75.62.161

USA-ARGENTINA-PANAMA
México-Perú-Brasil- Chile

Tel: +1 609-651-4246
Tel: +507-836-5355

Info@glesec.com

www.glesec.com