OPERATIONS & INTELLIGENCE TECHNICAL CYBER SECURITY REPORT

Inspira Health Network

October, 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 56 hosts, of which 10 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
56	10

Risk Distribution				
Critical	High	Medium	Low	Total
0	3	16	12	31

According to the metrics:

RV= 0.065956221

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	0	15	7	22
Service detection	0	3	0	1	4
Misc.	0	0	0	2	2
Web Servers	0	0	0	2	2
CISCO	1	0	0	0	1
Windows	0	0	1	0	1

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

- General (68.75 %).
- Service detection (12.5%).
- Misc. (6.25%).
- Web Servers (6.25%).
- Windows (3.125%).
- Cisco (3.125%).

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

Detection of SSL version 2 and 3 is the high severity vulnerability found during this period. The remediation for this vulnerability is the implementation of the TLS protocol v1.1 or 1.2. TLS 1.0 was declared insecure in June of the present year.
This vulnerability affects the following hosts: 170.75.33.166, 170.75.33.139 and 170.75.49.35.

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

The most vulnerable hosts will be summarized:

- Host 170.75.33.166 has 6 vulnerabilities of the General category: SSL Certificate Cannot Be Trusted , SSL Certificate Signed Using Weak Hashing Algorithm, SSL Medium Strength Cipher Suites Supported, SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability, SSL Certificate Chain Contains RSA Keys Less Than 2048 bits and SSL RC4 Cipher Suites Supported; 2 of Service Detection category: SSL Anonymous Cipher Suites Supported and SSL Version 2 and 3 Protocol.

- Host 170.75.49.35 has 3 vulnerabilities of General category: SSL Medium Strength Cipher Suites Supported, SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability and SSL RC4 Cipher Suites Supported; 1 Service Detection category: SSL Version 2 and 3 Protocol supported ; 1 Web Server category: Web Server HTTP Header Internal IP Disclosure and 1 Windows Category: Microsoft Exchange Client Access Server Information Disclosure.

- Host 170.75.32.15 has 4 vulnerabilities of the General category: Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key and SSL RC4 Cipher

Suites Supported (Bar Mitzvah).

These vulnerabilities represent a medium risk. An attacker could exploit the vulnerabilities to act as a man-in-the-middle, usurping the legitimate source connection and intercepting client's information.

The ports considered most vulnerable for this period were 4443 (Used as an alternative port to the HTTPS) and 443 (HTTPS). These ports present the most activity because the vulnerabilities found target those ports.

Descriptions by Host

The following vulnerabilities have been reported previously:

The remote hosts https://170.75.33.136/ is vulnerable to SSL / TLS Diffie-Hellman Modulus <= 1024 bits (Logjam), it allows SSL/TLS connections with one or more Diffie-Hellman modulus's 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.

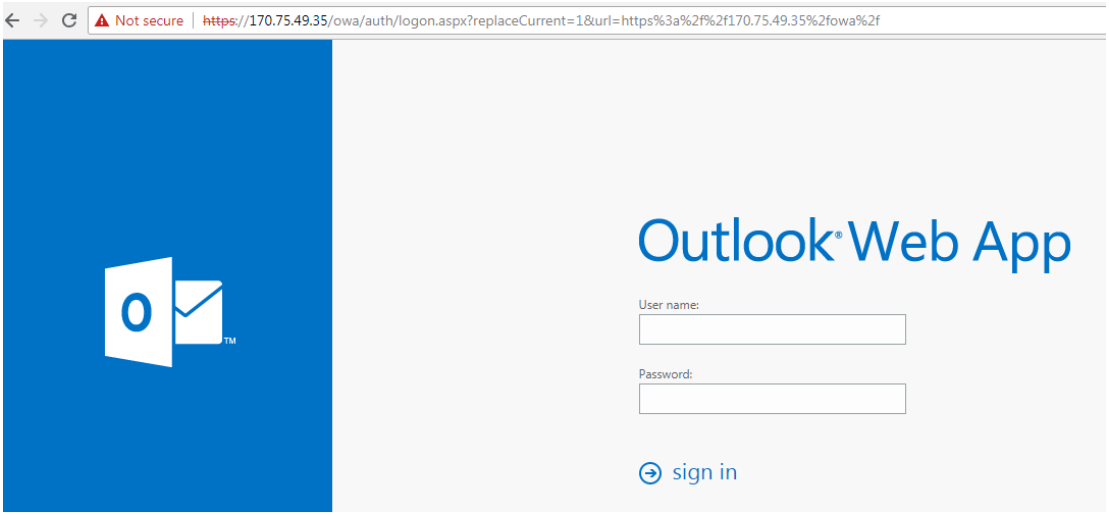
The remote host https://170.75.33.139/ is vulnerable to SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) this is a weakness in version 3 of the SSL protocol that allows an attacker in a context of man in the middle to decrypt the plain text content of an SSLv3 encrypted message.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

Remediation: For all the SSL vulnerabilities, the recommended solution is implementing TLS 1.1 or higher as the security layer for the connections. SSL v2 and v3 have many well documented vulnerabilities and is considered a deprecated protocol. In case the devices do not support TLS, the best approach would be to check with the device/software vendors if there are updates that patch the flaws present in the implementation of SSL.

The remote host https://170.75.49.35/ is affected by an information disclosure

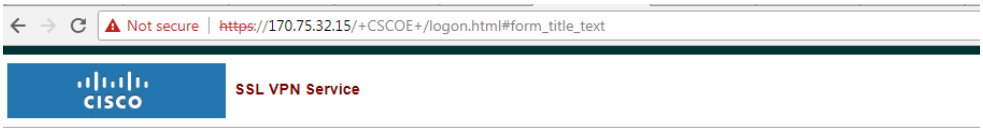
vulnerability condition called The Microsoft Exchange Client Access Server (CAS). A remote unauthenticated attacker can exploit this vulnerability to know the internal IP address of the server.

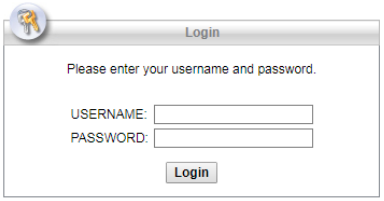
We attach the image, showing the stated above.



Remediation: Microsoft released a patch to fix this vulnerability, apply the relevant update to mitigate the vulnerability, the update is *Security Update for Microsoft Exchange Server (3185883)*.

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

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 and 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	170.75.49.35,170.75.33.122

Output

```
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 170.75.33.58, 170.75.33.136 and 170.75.33.139

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
```

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, 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 and 170.75.49.35

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 170.75.33.136 and 170.75.33.139

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

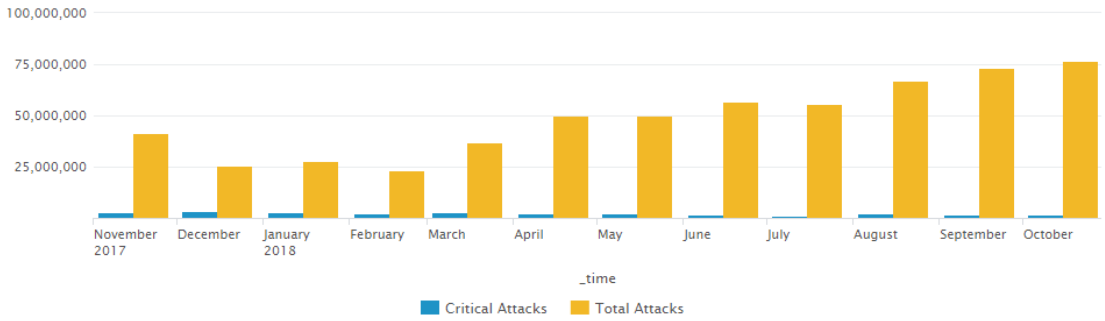
4443 / tcp / possible_wls 170.75.33.136, 170.75.33.139

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

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 the month we observed an increase in the activity of attacks from the previous month of approximately 5% and decrease in the critical attacks of the previous month of approximately 2%.

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

- The Russian Federation represents 37.77 % of the attacks, 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.
- Ukraine represents 19.30%, some of the attacks carried out are TCP Scan, UDP and Scan (Horizontal) of the Anti-Scanning category; and Network flood IPv4 TCP-SYN of the Behavorial-DoS category.
- The United States represents 12.38%, some of the attacks carried out are Ping Sweep of the Anti-Scannig category; and BlackList and Threat List in the Access category.

Here are some of the blocked attacks and the level of severity they represent:

- TCP Scan (horizontal), TCP Scan, UDP Scan (horizontal), UDP Scan, Ping Sweep and TCP Scan (vertical), are considered with a medium severity level.
- Network flood IPv4 UDP, Pattern flood Detected, SIP-Scanner-SIPVicious and Access

denied due to malicious request are considered with a high level of severity.

Most of the attacks Inspira Health Network receives are aimed at Bridgeton

The duration that presents the most attacks are:

- More than one hour ones were categorized as Access, Anomalies and Anti-Scanning.
- Less than one minute ones were categorized as Anti-Scanning, Behavioral-DoS, DoS and Intrusions.
- Ten to thirty minutes ones were categorized as Access, Anomalies, DNS protection and Anti-Scanning

These categories are comprised by different types of attacks.

Top 5 Source IPs (Local or public).

- 5.188.207.7
- 122.228.10.50
- 78.128.112.10
- 77.72.85.8
- 78.128.112.54

Correlation between the MSS-APS and MSS-VME

In the following table we will describe which hosts are the most frequent targets if these attacks target specific vulnerabilities on these hosts. 170.75.33.167, 170.75.49.35, 170.75.33.166, 170.75.33.160, 170.75.33.159

Attack destination (MSS-APS)	Number of attacks	Vulnerabilities that are present (MSS-VME)
170.75.33.159	1,128	✓ SSL Medium Strength Cipher Suites Supported ✓ SSL RC4 Cipher Suites Supported

170.75.33.166	907	✓ SSL Medium Strength Cipher Suites Supported ✓ SSL Version 2 and 3 Protocol Supported ✓ SSL Certificate Cannot Be Trusted ✓ SSL Certificate Signed Using Weak Hashing Algorithm ✓ SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability ✓ SSL Certificate Chain Contains RSA Keys Less Than 2048 bits ✓ SSL RC4 Cipher Suites Supported
170.75.33.160	862	✓ SSL Medium Strength Cipher Suites Supported ✓ SSL RC4 Cipher Suites Supported
170.75.33.167	798	✓ SSL Medium Strength Cipher Suites Supported
170.75.49.35	706	✓ SSL Version 2 and 3 Protocol Supported. ✓ SSL RC4 Cipher Suites Supported. ✓ SSL Medium Strength Cipher Suites Supported ✓ SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability

Types of attacks received from hosts that have vulnerabilities

170.75.33.159

Black List 83.599%
network flood IPv4 TCP-SYN 9.574%
TCP Scan (vertical) 6.117%
L4 Source or Dest Port Zero 0.532%
SIP-Scanner-SIPVicious 0.177%
Host IP 170.75.33.159 received 5 different types of attacks which are: Black List, network flood IPv4 TCP-SYN, TCP Scan (vertical), L4 Source or Dest Port Zero and SIP-Scanner-SIPVicious.

170.75.33.166

Black List 83.462%
network flood IPv4 TCP-SYN 10.033%
Anomaly-SSL-renegotiation-Cli 5.513%
Invalid TCP Flags 0.331%
L4 Source or Dest Port Zero 0.331%
SIP-Scanner-SIPVicious 0.22%
SIP-Sipcli18 0.11%
Host IP 170.75.33.166 received 7 different types of attacks which are: Black List, network flood IPv4 TCP-SYN, Anomaly-SSL-renegotiation-Cli, Invalid TCP Flags, L4 Source or Dest Port Zero, SIP-Scanner-SIPVicious and SIP-Sipcli18.

170.75.33.160

Black List 86.659%
network flood IPv4 TCP-SYN 12.645%
L4 Source or Dest Port Zero 0.464%
SIP-Scanner-SIPVicious 0.232%
Host IP 170.75.33.160 received 4 different types of attacks which are: Black List, network flood IPv4 TCP-SYN, L4 Source or Dest Port Zero and SIP-Scanner-SIPVicious.

170.75.33.167

Black List 84.712%
network flood IPv4 TCP-SYN 14.662%
L4 Source or Dest Port Zero 0.251%
SIP-Scanner-SIPVicious 0.251%
SIP-Sipcli18 0.125%
Host IP 170.75.33.167 received 5 different types of attacks which are: Black List, network flood IPv4 TCP-SYN, L4 Source or Dest Port Zero, SIP-Scanner-SIPVicious and SIP-Sipcli18.

170.75.49.35

Black List 56.091%
network flood IPv4 TCP-SYN 40.935%
Invalid TCP Flags 0.85%

L4 Source or Dest Port Zero 0.85%
Anomaly-SSL-renegotiation-Cli 0.708%
SIP-Scanner-SIPVicious 0.425%
network flood IPv4 UDP 0.142%
Host IP 170.75.49.35 received 7 different types of attacks which are: Black List, network flood IPv4 TCP-SYN, Invalid TCP Flags, L4 Source or Dest Port Zero, Anomaly-SSL-renegotiation-Cli, SIP-Scanner-SIPVicious and network flood IPv4 UDP.

We recommend applying the remediation of the vulnerabilities present in your systems for greater security.

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

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

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

Info@glesec.com

www.glesec.com