



OPERATIONS & INTELLIGENCE TECHNICAL  
CYBER SECURITY REPORT

Inspira Health Network

May 2018

Tel: +1 609-651-4246

Tel: +507-836-5355

Info@glesec.com

www.glesec.com

CONFIDENTIAL

## Table of Contents

Table of Contents.....	2
About This Report .....	3
Confidentiality .....	3
Managed Vulnerability Service .....	4
Descriptions by hosts .....	5
Vulnerabilities found by severity .....	8
Medium Risk Level Vulnerabilities .....	8
Low Risk Level Vulnerabilities .....	14
Threats.....	18

CONFIDENTIAL



## 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.

CONFIDENTIAL



## 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 address range given by Inspira Health Network, we have found a total of 57 hosts, of which 10 are vulnerable. These vulnerabilities are divided in the following severities as shown in the following table. Additionally you can notice the Risk Value score of your organization according to our metrics.

Total IP's Scanned		IP's Vulnerable		
57		10		
Risk Distribution				
Critical	High	Medium	Low	Total
0	0	30	9	39

According to the metrics:  
 RV= 0.071524966

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

CONFIDENTIAL

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

Category	Critical	High	Medium	Low	Total
General			25	5	30
Service detection			4	0	4
Misc.			0	3	3
Web Servers			0	1	1
Windows			1	0	1

- General
- Services detection
- Misc.



- Web Server
- Windows

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**.

Overall the vulnerabilities for Inspira Health Network this period have been 30 medium and 9 low-risk. Please refer to MSS-VM intelligence section for more detail about specific vulnerabilities. Among the medium risk vulnerabilities found are: SSL Medium Strength Cipher Suites Supported, SSL Certificate Cannot Be Trusted, SSL Certificate Expiry, SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability (POODLE), SSL Certificate Signed Using Weak Hashing Algorithm and Internet Key Exchanged. Medium risk vulnerabilities found were classified as, this means that attackers could take advantage of any of those and attempt to cause and negative impact to your Organization.

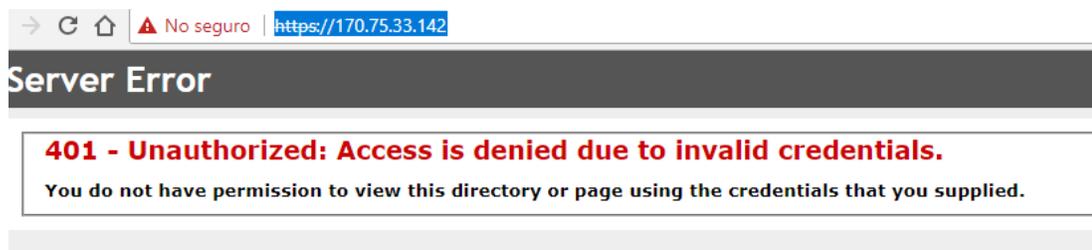
Ports 443, 4443 and 500 are the most vulnerable ports for this period; this is because many vulnerabilities were found which are related to them and categorized as medium risk.

## Descriptions by Host

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.

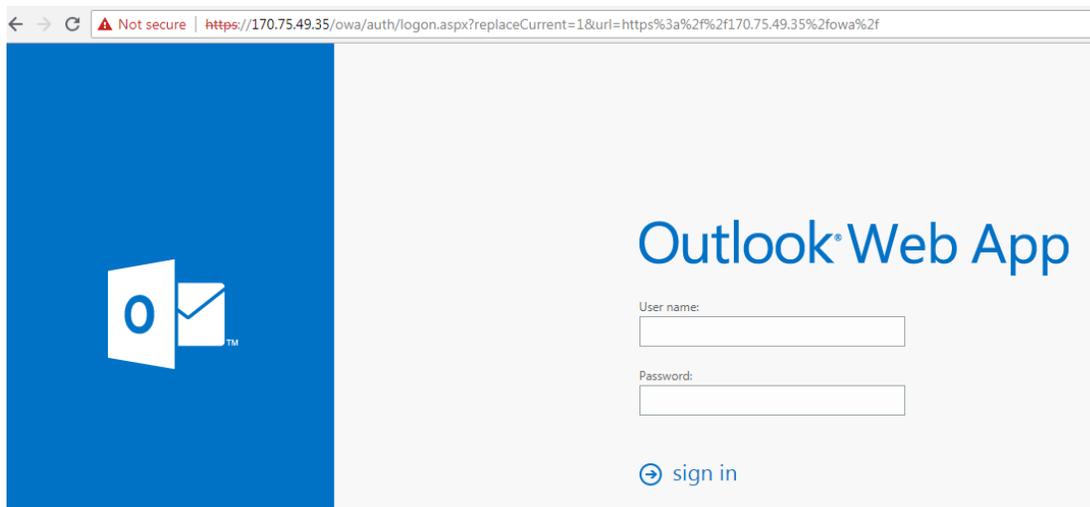


## REPORT FOR:

Inspira Health Network

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://170.75.33.171/> indicates an SSL Certified Expired vulnerability, which indicates that your SSL certificate has passed the validity date. You must request and upload a new valid certificate that is issued to the destination domain.



The remote host <https://170.75.33.133/> is affected by an 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.

CONFIDENTIAL

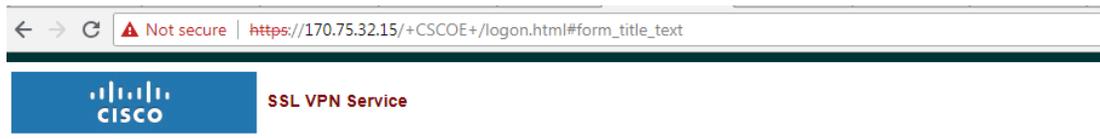


REPORT FOR:  
Inspira Health Network



The survey is expired.

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.

A screenshot of a login form titled "Login". The form contains the text "Please enter your username and password." followed by two input fields: "USERNAME:" and "PASSWORD:". Below the input fields is a "Login" button.

CONFIDENTIAL



## Vulnerabilities by severity

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

### 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

```
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**



## REPORT FOR:

Inspira Health Network

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

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 Version 2 and 3 Protocol Detection

### Description

CONFIDENTIAL



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.
```

### 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**

CONFIDENTIAL



```
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 170.75.33.136 170.75.33.139

443 / tcp / possible\_wls 170.75.33.55 170.75.49.35

### 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

**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)

```

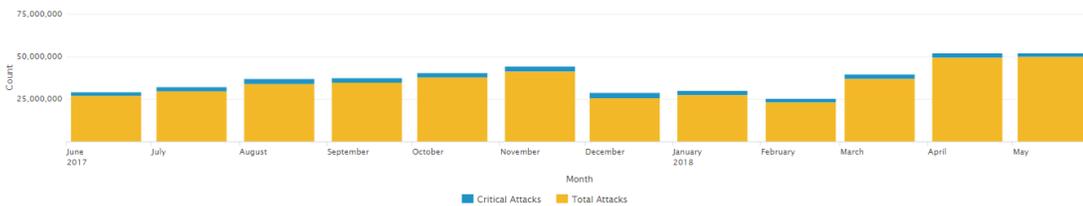
CONFIDENTIAL



## 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 Behavioral-DoS. All these threats were identified and dropped.



This month we are seeing a decrease in attack activity from prior month of about 0.50% and an increase in critical attacks from prior month of about 4.83%.

Most of the attacks are more than an hour and less than a minute and they target multiple ports. The 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.

Most of the attacks seem to be of reconnaissance (scanning). About 88.704% of the attacks for this month came from scanning which can be considered reconnaissance and it is what precedes further attacks. Other categories with a lower percentage of attacks were Access with 5.05% and Behavioral-DoS with 3.94%.

The attacks are, for the most part, from the Russian Federation (36%), United States (22%) and the Chile (12%) as the three main sources. Within these attacks, we were able to recognize TCP Scan, Ping Sweep, Network flood IPv4 TCP-SYN, Network flood IPv4 TCP-SYN-ACK and Network flood IPv4 UDP; all the mentioned before are typical probing techniques which means attackers are always searching for new opportunities.

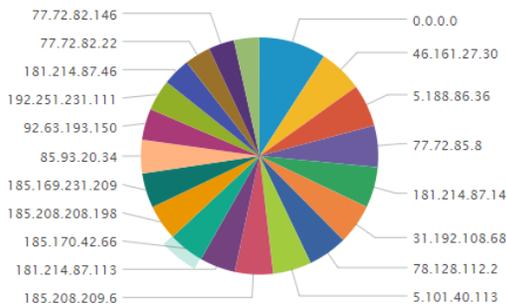
CONFIDENTIAL



Based on the information gathered from the security countermeasures during this period 49,967,647 attacks on Inspira Health Network; 2,317,017 of which were considered critical were all stopped by the GLESEC managed security countermeasures.

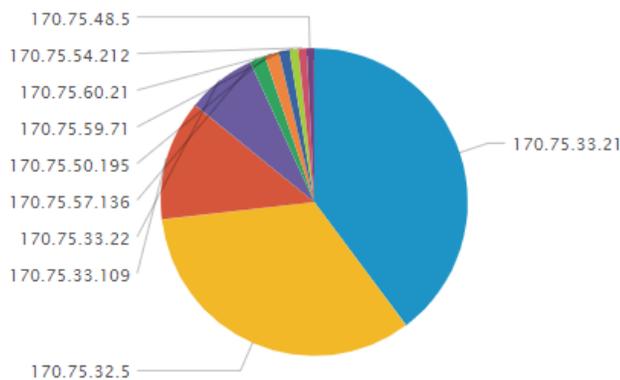
Inspira Health Network receives an average of 37,552,819 total attacks and 2,446,879 critical attacks on a monthly basis. This equates to an average of 1,243,471 total daily attacks and 81,022 critical daily attacks.

Top Source IPs (Local or public).



Top 10 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.



CONFIDENTIAL





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

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

Info@glesec.com  
www.glesec.com