



OPERATIONS & INTELLIGENCE TECHNICAL CYBER SECURITY REPORT

Metrobank S.A.

July, 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
Description by Host	7
Vulnerabilities found by severity	10
Critical Risk Level Vulnerabilities.....	10
High Risk Level Vulnerabilities	10
Medium Risk Level Vulnerabilities	11
Low Risk Level Vulnerabilities	16
Threats.....	19

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.



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 Metrobank S.A., we have found a total of 12 hosts, of which 9 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, there was a decrease compared to last month. For this period, the critical vulnerability in Host 190.34.183.131 continues, which has been previously reported in your organization.

Total IP's Scanned		IP's Vulnerable		
12		9		
Risk Distribution				
Critical	High	Medium	Low	Total
1	3	30	13	47

According to the metrics:
RV= 0.311968085

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	0	0	24	6	30
Misc.	0	0	4	5	9
Service detection	0	3	0	1	4
Windows	1	0	2	0	3
Web Servers	0	0	0	1	1

- General (63%).
- Misc (19%).



- Services Detection (8%).
- Windows (6%)
- Web Server (2%).

Additional details about these vulnerabilities are presented in the Vulnerabilities found in Metrobank S.A by severity section of the MSS-VM on page 10.

Metrobank continues to present critical (2%), high (6%), medium (64%) and low (28%) vulnerabilities. For this month, the total number of vulnerabilities decreased to 47.

Critical vulnerability MS15-034 is presented again: a vulnerability in HTTP.sys could allow remote code execution (3042553) (unclassified verification) on host 190.34.183.131 through ports 443 and 80.

Among the main categories with the greatest number of vulnerabilities for this period, we can mention:

- General (64%) vulnerabilities that frequently occur in this category are: SSL Medium Strength Cipher Suites Supported and SSL Certificate Cannot Be Trusted both have an average severity level.
- Misc. (19%) the vulnerability that occur most frequently in this category are: SSH Weak Algorithms Supported represents a medium severity level.
- Service detection (8%) vulnerabilities that occur most frequently in this category are: SSL Version 2 and 3 Protocol Detection represents a high level of severity and SSL Anonymous Cipher Suites Supported represents a low level of severity.
- Windows (6%) its main vulnerability is MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (unauthenticated check) represents a level of critical severity; also presents the vulnerabilities with medium severity level of type Microsoft Exchange Client Access Server Information Disclosure and Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness.

Of the vulnerabilities mentioned above, the ones that occur most frequently are: SSL Certificate Cannot Be Trusted (26%), SSL Certificate Signed Using Weak Hashing



Algorithm (21%) and SSL Certificate Chain Contains RSA Keys Less Than 2048 bits (16%).

The 5 ports considered most vulnerable for this period were 443 (HTTPS), 3389 (RDP), 22 (SSH), 25 (SMTP) and port 80 (HTTP). This is due to the fact that many vulnerabilities related to them were found and the majority is classified at a medium severity level.

Ports 80 and 443 are considered critical, the most vulnerable host on these ports is 190.34.183.131. Port 25 has an average severity on host 190.34.183.148. The vulnerabilities found in this host are: SSL Certificate Cannot be trusted and SSL Media Strength Cipher Suites compatible. The port that appears most frequently as vulnerable is 443.

The 5 most vulnerable hosts are: 190.34.183.142, 190.34.183.154, 190.34.183.149, 190.34.183.190 and 190.34.183.132; most are of medium and low severity. We can mention that the most vulnerable protocol for this period is TCP.

There is a low percentage of vulnerability between the categories of Service Detection, Port Scanners and Firewalls (Chek Point) that present an "informational" level of severity, at ports 18264, 264 and 500 (hosts: 190.34.183.132, 190.34.183.91 and 190.34.183.90).



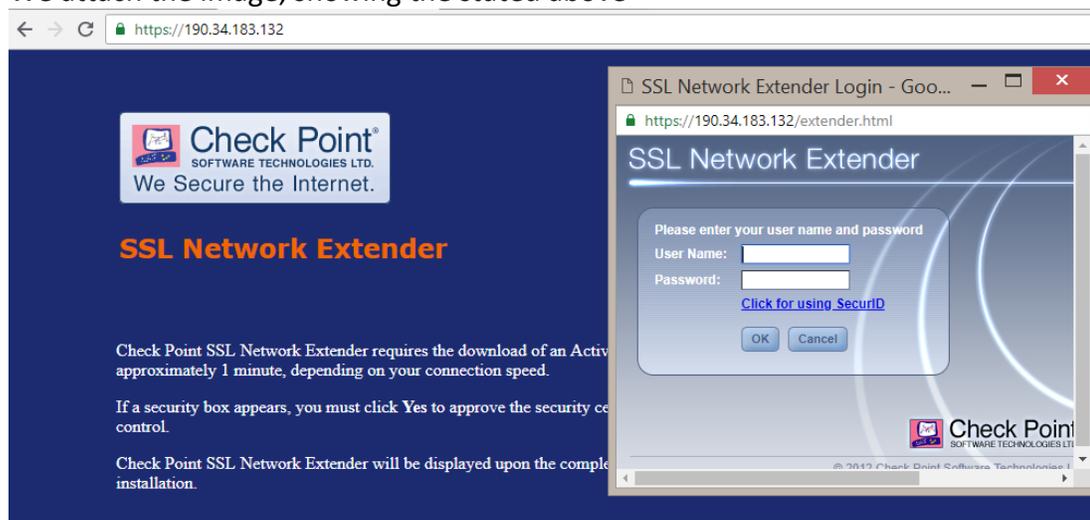
Descriptions by Host

The host remote <https://190.34.183.132/> presents a pop-up window with the following message: The SSL Network Extender authentication pop-up window was blocked. You can click on the button to open it or permanently set your pop-up blocker to allow pop-up from this site. It is recommended to add this site to the Trusted Sites. Other hosts that exhibit this same vulnerability are: <https://190.34.183.90/> and <https://190.34.183.91/>

Some of the vulnerabilities that it presents are: SSH Server CBC Mode Ciphers Enabled y SSH Weak Algorithms Supported.

The previous month this vulnerability was presented.

We attach the image, showing the stated above



The host remote <https://190.34.183.149> the remote mail server is affected by an information disclosure vulnerability. A remote, unauthenticated attacker can exploit this vulnerability to learn the server's internal IP address.

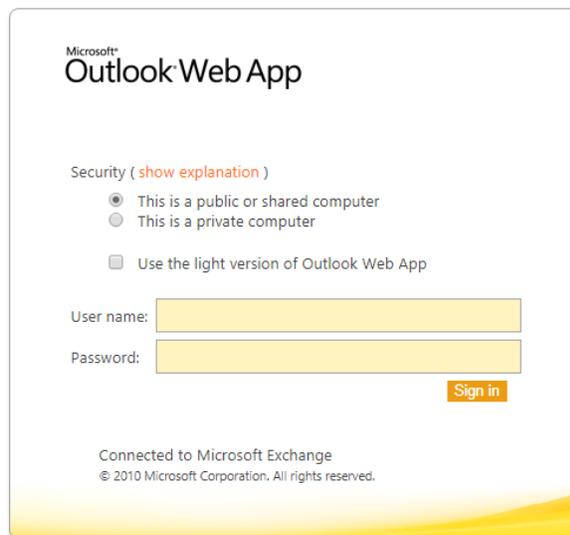
We attach the image, showing the stated above

CONFIDENTIAL

REPORT FOR:

Metrobank S.A.

← → ↻ No seguro <https://190.34.183.149/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2f190.34.183.149%2fowa%2f>



The remote host <http://190.34.183.139/> is affected the action of Fingerprinting. This vulnerability is known OS Fingerprinting is a technique that involves analyzing the footprints left by an operating system in its network connections. It is based on the response times to the different packages, to establish a connection in the TCP / IP protocol, which is used by the different operating systems. We recommend applying more security to your servers.

Another vulnerability that it presents is: Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness. This is based on the fact that a remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle attack (MiTM). The RDP client does not endeavor to validate the identity of the server when configuring the encryption. An attacker with the ability to intercept RDP server traffic can establish encryption with the client and the server without being detected.

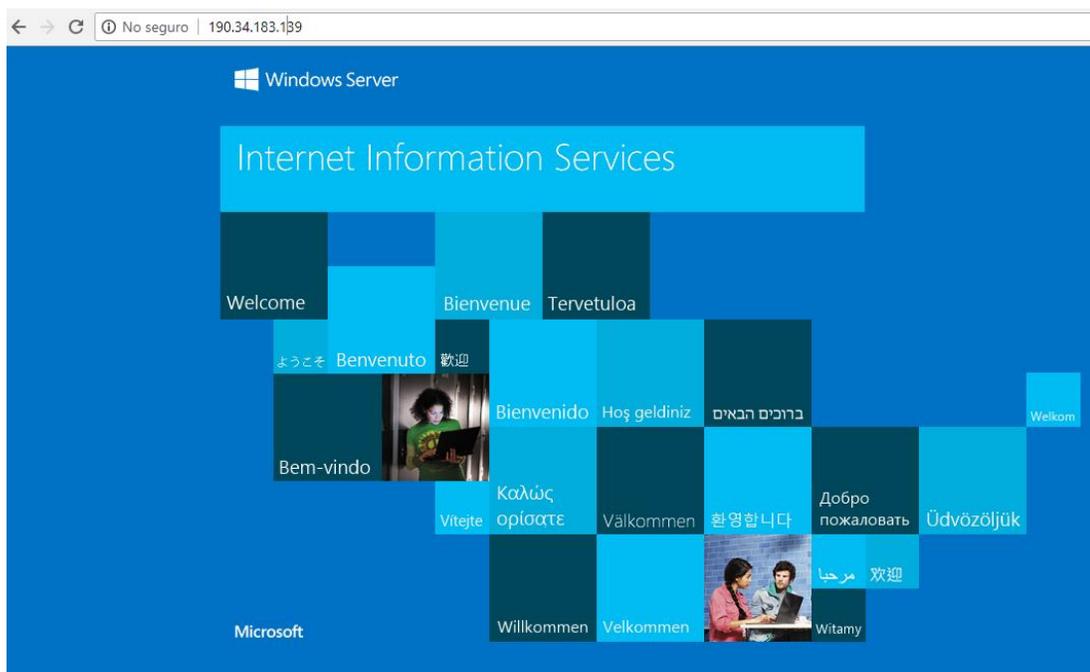
We attach the image, showing the stated above.

CONFIDENTIAL



REPORT FOR:

Metrobank S.A.



The remote host 190.34.183.131 (<https://www.govimar.com.pa/>) is affected vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553), which affects Windows systems (ports 80/443); We recommend to apply all the security updates suggested by Windows, especially MS15-034 (KB 3042553), since they all solve the vulnerabilities found in this type of system. The previous month this vulnerability was presented.

Other vulnerabilities were SSL Anonymous Cipher Suites Supported, SSL RC4 Cipher Suites Supported (Bar Mitzvah) and SSL Version 2 and 3 Protocol Detection are presented on the host:

190.34.183.152, (<https://www.metrobanksa.com/metrobank/en>).

CONFIDENTIAL



Vulnerabilities by severity

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

Critical Risk Level Vulnerabilities

MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution

Description

The version of Windows running on the remote host 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.

Solution

Microsoft has released a set of patches for Windows 7, 2008 R2, 8, 8.1, 2012, and 2012 R2

Affected Systems

80 / tcp / possible_wls	190.34.183.131
443 / tcp / possible_wls	190.34.183.131

Output

```
HTTP response status: HTTP/1.1 301 Moved Permanently
```

```
HTTP response status: HTTP/1.1 200 OK
```

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

443 / tcp / possible_wls 190.34.183.139, 190.34.183.142, 190.34.183.149,
190.34.183.154

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

9443 / tcp / possible_wls 190.34.183.139
 25 / tcp / smtp 190.34.183.148
 8089 / tcp / possible_wls 190.34.183.139
 443 / tcp / possible_wls 190.34.183.90,190.34.183.91,190.34.183.132,
 190.34.183.139, 190.34.183.142, 190.34.183.149.

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

25 / tcp / smtp 190.34.183.148

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=PA/ST=Panama/L=Panama/OU=Metrobank/O=Metrobank, S.A./CN=correo.metrobanksa.com
|-Issuer : C=BE/O=GlobalSign nv-sa/CN=GlobalSign Organization Validation CA - SHA256 - G2
```

Affected Systems

443 / tcp / possible_wls 190.34.183.154

Output



REPORT FOR:

Metrobank S.A.

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 : 2.5.4.15=Private  
Organization/2.5.4.5=1991/1.3.6.1.4.1.311.60.2.1.3=PA/C=PA/ST=Panama/L=Panama/2.5.4.9=Ground  
Floor, Metrobank Tower/OU=Metrobank/O=Metrobank, S.A./CN=metronet.metrobanksa.com  
|-Issuer : C=BE/O=GlobalSign nv-sa/CN=GlobalSign Extended Validation CA - SHA256 - G3
```

Affected Systems

443 / tcp / possible_wls 190.34.183.142

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=PA/CN=190.34.183.142/O=Glesec Panama, S.A./OU=Radware Web Management  
|-Issuer : C=PA/CN=190.34.183.142/O=Glesec Panama, S.A./OU=Radware Web Management
```

Affected Systems

443 / tcp / possible_wls 190.34.183.90 190.34.183.91, 190.34.183.132

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 : O=fwmetro..5afb7i  
|-Issuer : O=fwmetro..5afb7i
```

Affected Systems

3389 / tcp / msrdp 190.34.183.139
8443 / tcp / possible_wls 190.34.183.139

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 : CN=AppServer.metrobank.local  
|-Issuer : CN=AppServer.metrobank.local
```

CONFIDENTIAL



```
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=PA/ST=Panama/L=Panama/OU=Metrobank/O=Metrobank, S.A./CN=appserver.metrobanksa.com
|-Issuer : C=BE/O=GlobalSign nv-sa/CN=GlobalSign Organization Validation CA - SHA256 - G2
```

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

443 / tcp / possible_wls 190.34.183.142,190.34.183.149



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 190.34.183.149

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: Keep-Alive
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 :

10.1.1.235
```

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 / possible_wls 190.34.183.139,190.34.183.142,190.34.183.149

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}
```

SSH Server CBC Mode Ciphers Enabled

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Affected Systems

190.34.183.142

Output

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :
```

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
```

```
The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :
```

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
```

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 / possible_wls 190.34.183.154

Output

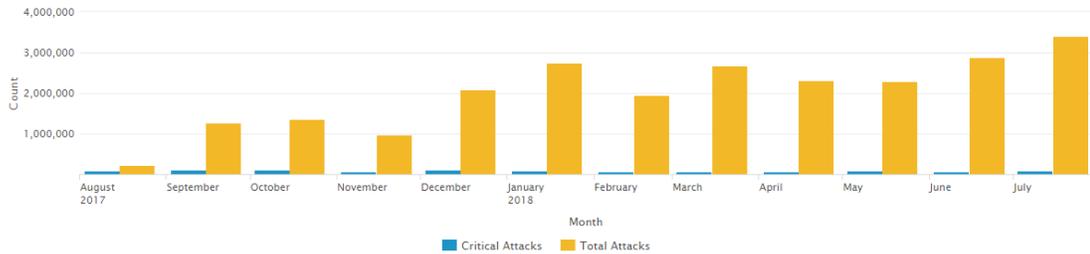
```
Vulnerable connection combinations :
```

```
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 reported by MSS-APS for this month are Anti-Scan, Access, DoS Behavior and Anomalies. All these threats were identified and discarded.



Based on the information collected from the security measures during this period, Metrobank SA received a total of: 3,410,589 attacks, of which 91,286 are critical, there was an increase of 18% in the number of attacks received in this period compared to the month of June (Total attacks: 2,878,997), and a 27% increase in critical attacks for this month. The critical attack that occurs most frequently for this month was Network Flood IPv4 UDP (72%) and belongs to the Behavioral-DoS category.

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

- Network flood IPv4 UDP and SIP-Scanner-SIPVicious, are considered with a high level of severity.
- TCP Scan, TCP Scan (Horizontal), UDP Scan, UDP Scan (Horizontal) and Ping Sweep, are considered with a medium severity level.
- Threat List and TCP handshake violation, first packet not SYN, they are considered with a low level of severity

Between frequent and blocked attacks per week we have: Invalid IP Header or Total Length, Ping Sweep, SIP-Scanner-SIPVicious, TCP Scan, TCP Scan (Horizontal), TCP handshake violation, first packet not syn, Threat List, UDP Scan, UDP Scan

CONFIDENTIAL



(horizontal) and Network flood IPv4 UDP.

All this was stopped by the security countermeasures administered by GLESEC. Most attacks last less than a minute and are in the categories of Anti-scanning, Behavior-DoS, Cracking-Protection and HttpFlood; Attacks that last more than an hour include: Access, Anti-Scanning and Anomalies.

Most of the attacks are carried out from the following countries: Russian Federation (48%), Panama (20%), United States (11%), Netherlands (5%) and China (4.6%); These are mainly destined to the ports: 8545 is destined to explorations with a lot of frequency; if it is not necessary to leave it open, it would be advisable to close it or filter it from traffic from outside, 3389 (RDP: Microsoft Terminal Server), the web access port (8080) and the SSH connection port (22).

Most attacks seem to be recognition (scanning) lasting less than a minute and up to more than an hour. Approximately 93% of the attacks are scanning, which can be considered recognition and is what you prefer for future attacks. The attacks that consume the most amount of bandwidth are the attacks of Behavioral-DoS, Access, Anti-Scanning, Anomalies and Intrusions.

In this period there was a low percentage of attacks in the categories:

- HttpFlood (HTTP page flood attack) and Cracking-Protection (web browsing, SMTP scanning) to the IP addresses 190.34.183.152 and 190.34.183.154.
- Cracking Protection (Web Scan, SMTP Scan) to IPs 190.34.183.149 and 190.34.183.153.

The DefensePro helped prevent targeted attacks at the network and server level that were directed to known port numbers: 3389 (RDP), 8545 (JSON-RPC), 8080 and 81 (HTTP-Alternative), 22 (SSH), 5060 (SIP), 3390 (DSC), 1433 (MS-SQL-S), 445 (Microsoft-ds), in order of frequency for this reporting period.

Top 5 Source IPs (Local or public).

- 190.34.192.31
- 190.34.192.34



- 195.43.95.90
- 5.188.40.100
- 5.188.40.99

The most frequent types of attacks were the horizontal scan mode TCP.

The first two IPs remain as attackers just like the previous month and come from Panama; and the last three IPs come from Russia.

Top 5 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.

- 190.34.183.135
- 190.34.183.158
- 190.34.183.137
- 190.34.183.132
- 190.34.183.152

The DefensePro system has operated properly with 100.00% up time and good performance.





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

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

Info@glesec.com
www.glesec.com