OPERATIONS & INTELLIGENCE TECHNICAL CYBER SECURITY REPORT

BANVIVIENDA

September, 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.

According the address range given by BANVIVIENDA, we have found a total of 15 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
15	10

Risk Distribution				
Critical	High	Medium	Low	Total
0	5	26	9	40

According to the metrics:

RV= 0.294166667

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	23	8	31
Service detection		5	0	0	5
Misc.		0	2	1	3
Windows		0	1	0	1

- General
- Services detection
- Misc
- Windows

For this month we discovered 15 hosts in total, of which 10 are vulnerable, BANVIVIENDA has a total of 40 vulnerabilities.

The vulnerabilities are distributed as follows: 9 vulnerabilities of low severity (22.5%), median 26 (65%, mostly presented) and high 5 (12.5%). No critical severity vulnerabilities have been found during this month.

Below are the most vulnerable categories:

- General (77.5%) presents mostly vulnerabilities of type: SSL Medium Strength Cipher Suites Supported represent a medium level of severity and SSL RC4 Cipher Suites Supported (Bar Mitzvah) represent a low level of severity.

- Service Detection (12.5%) the main vulnerability is of type SSL Version 2 and 3 Protocol Detection represent a high level of severity.

- Misc. (7.5%) presents major vulnerabilities of type: SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) and represents a medium level of severity.

- Windows (2.5%) its main vulnerability is of type Microsoft Exchange Client Access Server Information Disclosure represents a medium level of severity.

Continues to present the high severity vulnerability of type SSL Version 2 and 3 Protocol Detection on hosts 200.90.137.87, 200.90.137.89, 200.90.137.83, 200.46.19.100 and 200.46.227.230 (they have ports 443, 25, 10000 and 500 vulnerable), and belongs to the service detection category.

Main vulnerable hosts for this period: 200.90.137.87, 200.90.137.89, 200.46.227.230, 200.90.137.83, 200.90.137.91, 200.90.137.94 and 200.46.19.100. Most of these are vulnerable by the TCP protocol, except for hosts 200.46.19.98 and 200.46.227.277 that show vulnerability in the UDP protocol.

The most vulnerable ports for this period are:

- 443 (https) most hosts are vulnerable by this port, among them we have: 200.46.227.230, 200.90.137.91, 200.90.137.83, 200.46.19.100 and

200.90.137.94.

- 25 (smtp) the 2 vulnerable hosts by this port are: 200.90.137.87 and 200.90.137.89.

- 10000 (ndmp), the only vulnerable host for this port is 200.90.137.91 and has the following vulnerabilities SSL Certificate Cannot Be Trusted, SSL Certificate Signed Using Weak Hashing Algorithm and SSL Self-Signed Certificate.

- 500 (Ipsec) the 2 vulnerable hosts by this port are: 200.46.19.98 and 200.46.227.277 have a vulnerability of type type Microsoft Exchange Client Access Server Information Disclosure.

Among the most frequent vulnerabilities for this period we have:

- SSL Medium Strength Cipher Suites Supported
- SSL RC4 Cipher Suites Supported (Bar Mitzvah)
- SSL Version 2 and 3 Protocol Detection
- SSL Certificate Cannot Be Trusted
- SSL Certificate Signed Using Weak Hashing Algorithm
- SSL Self-Signed Certificate
- SSL Weak Cipher Suites Supported

Additional details about these vulnerabilities are presented in the Vulnerabilities found in BANVIVIENDA by severity section of the MSS-VM **on page 11.**

Description by Host

For this month, the same vulnerabilities continue to be presented

The following hosts **200.90.137.89** and **200.90.137.87** present the same vulnerabilities:
Several vulnerabilities found on this host are stated here:
SSL Certificate Cannot Be Trusted, SSL Certificate Signed Using Weak Hashing Algorithm, SSL Medium Strength Cipher Suites Supported, SSL Self-Signed Certificate, SSL Version 2 and 3 Protocol Detection, SSL Weak Cipher Suites

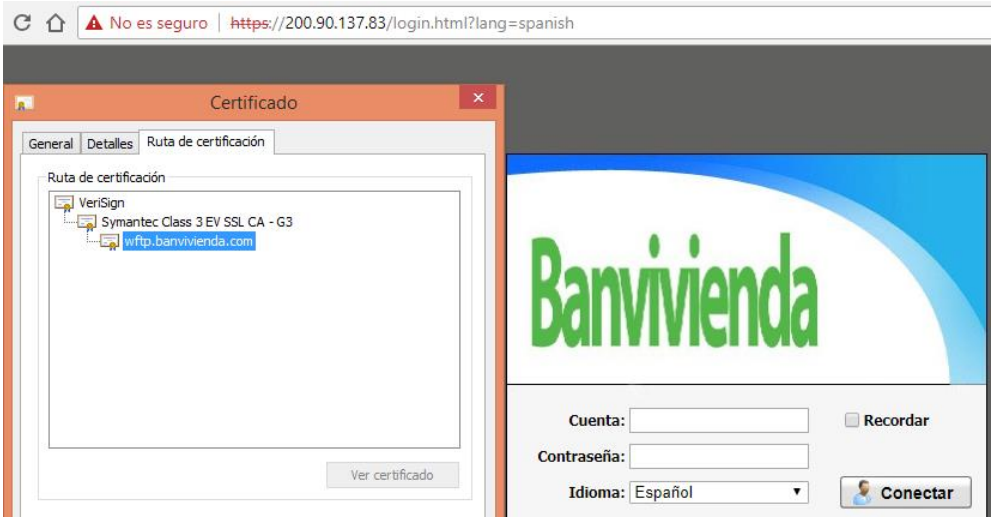
Supported, OpenSSL AES-NI Padding Oracle MitM Information Disclosure, SSL RC4 Cipher Suites Supported (Bar Mitzvah). We recommend following the solution procedure for these issues, described in the Vulnerabilities by severity section of this document.

200.46.227.230

Several vulnerabilities found on this host are stated here:
SSL Medium Strength Cipher Suites Supported, SSL RC4 Cipher Suites Supported (Bar Mitzvah), SSL Version 2 and 3 Protocol Detection and SSL Weak Cipher Suites Supported. We recommend following the solution procedure for these issues, described in the Vulnerabilities by severity section of this document.
https://www.banvivienda.com/es

200.90.137.83

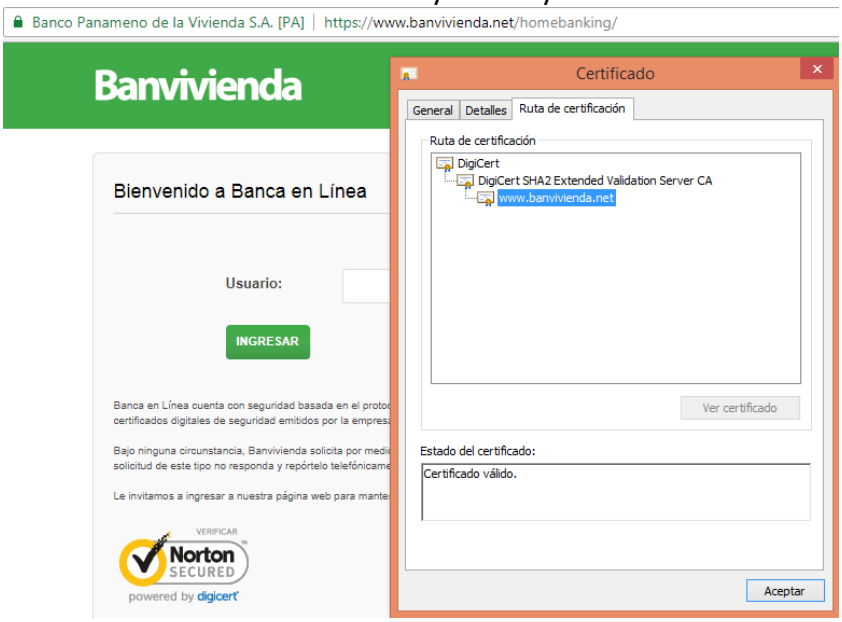
Several vulnerabilities found on this host are stated here:
SSL Certificate Cannot Be Trusted, SSL Medium Strength Cipher Suites Supported, SSL Version 2 and 3 Protocol Detection, SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE), SSL RC4 Cipher Suites Supported (Bar Mitzvah). We recommend following the solution procedure for these issues, described in the Vulnerabilities by severity section of this document.



200.46.19.100

Several vulnerabilities found on this host are stated here:
SSL Version 2 and 3 Protocol Detection, SSLv3 Padding Oracle On Downgraded

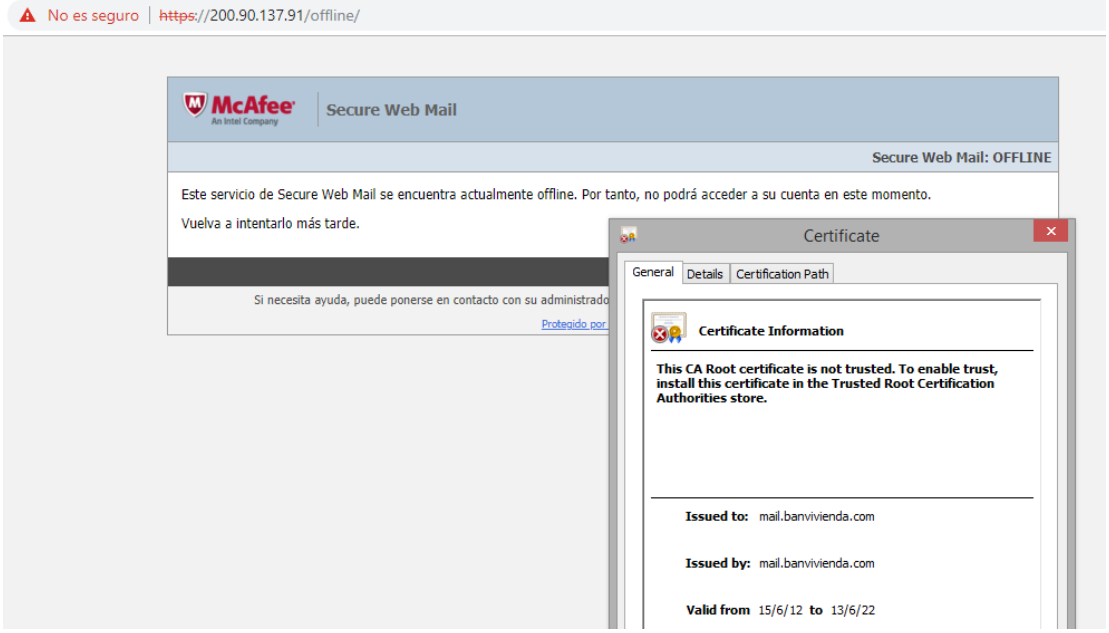
Legacy Encryption Vulnerability (POODLE), SSL RC4 Cipher Suites Supported (Bar Mitzvah). We recommend following the solution procedure for these issues, described in the Vulnerabilities by severity section of this document.



200.90.137.91

Several vulnerabilities found on this host are stated here:

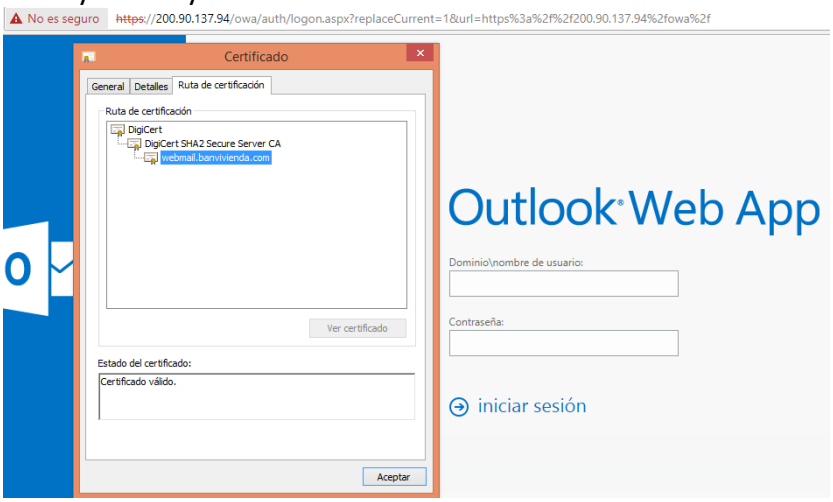
SSL Certificate Cannot Be Trusted, SSL Certificate Signed Using Weak Hashing Algorithm, SSL Self-Signed Certificate. We recommend following the solution procedure for these issues, described in the Vulnerabilities by severity section of this document.



200.90.137.94

Several vulnerabilities found on this host are stated here:

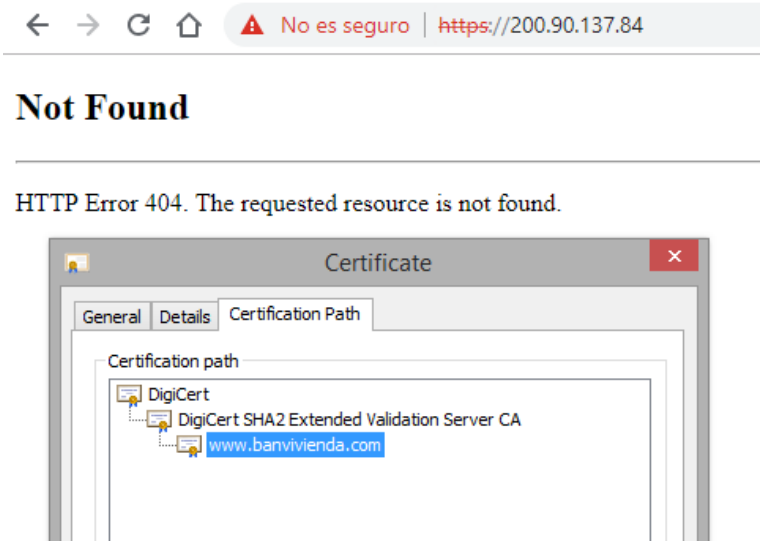
Microsoft Exchange Client Access Server Information Disclosure, SSL Medium Strength Cipher Suites Supported, SSL RC4 Cipher Suites Supported (Bar Mitzvah). We recommend following the solution procedure for these issues, described in the Vulnerabilities by severity section of this document.



200.90.137.84

Several vulnerabilities found on this host are stated here:

SSL Medium Strength Cipher Suites Supported, SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam). We recommend following the solution procedure for these issues, described in the Vulnerabilities by severity section of this document.



The hosts **200.46.19.98** and **200.46.227.227** have the following vulnerability:
During this month, the GLESEC operations center, we rediscovered the same vulnerability called "Aggressive Internet Key Interchange Mode (IKE) with pre-shared key". We recommend following the solution procedure for this problem, which is described in the Vulnerabilities by severity section of this document.

Of the attacks made to your organization, 43% goes specifically to host 200.46.19.98 and 44% goes to host 200.46.227.277.

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

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:

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

- An insecure padding scheme with CBC ciphers.
- 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

25 / tcp / smtp 200.90.137.87, 200.90.137.89.
443/tcp/ possible_wls 200.46.19.100, 200.90.137.83 and 200.46.227.230.

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 use 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

25 / tcp / smtp 200.90.137.87200.90.137.89

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)

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

Affected Systems

443 / tcp / possible_wls 200.46.227.230, 200.46.227.230, 200.90.137.83, 200.90.137.83, 200.90.137.84, 200.90.137.84, 200.90.137.94, 200.90.137.94

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 200.90.137.87200.90.137.89

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/O=McAfee, Inc./OU=Email Gateway/CN=mail1.banvivienda.com/E=support@mcafee.com
|-Issuer  : C=US/O=McAfee, Inc./OU=Email Gateway/CN=mail1.banvivienda.com/E=support@mcafee.com
```

Affected Systems

443 / tcp / possible_wls 200.90.137.83,200.90.137.83

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 : 1.3.6.1.4.1.311.60.2.1.3=PA/2.5.4.15=Private
Organization/2.5.4.5=64474/C=PA/ST=Panama/L=Panama/O=Banco Panameno de la Vivienda
S.A./OU=IT/CN=wftp.banvivienda.com
|-Issuer  : C=US/O=Symantec Corporation/OU=Symantec Trust Network/CN=Symantec Class 3 EV SSL CA
- G3
```

Affected Systems

443 / tcp / possible_wls 200.46.227.230, 200.46.227.230

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 : 2.5.4.15=Private
Organization/1.3.6.1.4.1.311.60.2.1.3=PA/2.5.4.5=64474/C=PA/ST=Panama/L=Panama City/O=Banco
Panameno de la Vivienda SA/OU=IT Department/CN=chat.banvivienda.com
|-Issuer  : C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 Extended Validation Server
CA
```

Affected Systems

443 / tcp / possible_wls 200.90.137.91
10000 / tcp / possible_wls 200.90.137.91

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=mail.banvivienda.com/C=US/O=McAfee, Inc./OU=Email Gateway
|-Issuer  : CN=mail.banvivienda.com/C=US/O=McAfee, Inc./OU=Email Gateway
```

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
25 / tcp / smtp 200.90.137.87, 200.90.137.89
443 / tcp / possible_wls 200.46.19.100, 200.46.19.100,200.90.137.83, 200.90.137.83
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

25 / tcp / smtp 200.90.137.87, 200.90.137.89
10000 / tcp / www 200.90.137.91

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/O=McAfee, Inc./OU=Email
Gateway/CN=mail1.banvivienda.com/E=support@mcafee.com
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Oct 10 22:51:42 2014 GMT
|-Valid To            : Oct 07 22:51:42 2024 GMT
```

Affected Systems

443 / tcp / possible_wls 200.90.137.91
10000 / tcp / possible_wls 200.90.137.91

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             : CN=mail.banvivienda.com/C=US/O=McAfee, Inc./OU=Email Gateway
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Jun 15 18:52:06 2012 GMT
|-Valid To            : Jun 13 18:52:06 2022 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
443 / tcp / www 200.46.19.100, 200.46.19.100, 200.90.137.83
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 / www 200.90.137.94
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 :

10.100.201.119
```

SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

Description

The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.

Solution

Reconfigure the service to remove support for EXPORT_RSA cipher suites.

Affected Systems

443 / tcp / www 200.46.227.230, 200.46.227.230

Output

```
EXPORT_RSA cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

    EXP-RC2-CBC-MD5             Kx=RSA(512)    Au=RSA      Enc=RC2-CBC(40)          Mac=MD5
export
    EXP-RC4-MD5                 Kx=RSA(512)    Au=RSA      Enc=RC4(40)              Mac=MD5
export

The fields above are :

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

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 / ikev1 200.46.227.227

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

25 / tcp / smtp 200.90.137.87, 200.90.137.89
443 / tcp / possible_wls 200.90.137.94

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}
```

Affected Systems

443 / tcp / possible_wls 200.46.19.100, 200.46.19.100,200.90.137.83, 200.90.137.83

Output

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

  Low Strength Ciphers (<= 64-bit key)

    EXP1024-RC4-SHA             Kx=RSA(1024)   Au=RSA      Enc=RC4(56)             Mac=SHA1
export
    EXP-RC4-MD5                 Kx=RSA(512)    Au=RSA      Enc=RC4(40)             Mac=MD5
export

  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}
```

Affected Systems

443 / tcp / possible_wls 200.46.227.230

Output

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

  Low Strength Ciphers (<= 64-bit key)

    EXP1024-RC4-SHA             Kx=RSA(1024)   Au=RSA      Enc=RC4(56)             Mac=SHA1
export
    EXP-RC4-MD5                 Kx=RSA(512)    Au=RSA      Enc=RC4(40)             Mac=MD5
export

  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}
```

OpenSSL AES-NI Padding Oracle MitM Information Disclosure

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability due to an error in the implementation of ciphersuites that use AES in CBC mode with HMAC-SHA1 or HMAC-SHA256.

The implementation is specially written to use the AES acceleration available in x86/amd64 processors (AES-NI). The error messages returned by the server allow a man-in-the-middle attacker to conduct a padding oracle attack, resulting in the ability to decrypt network traffic.

Solution

Upgrade to OpenSSL version 1.0.1t / 1.0.2h or later.

Affected Systems

25 / tcp / smtp 200.90.137.87, 200.90.137.89

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 200.90.137.84

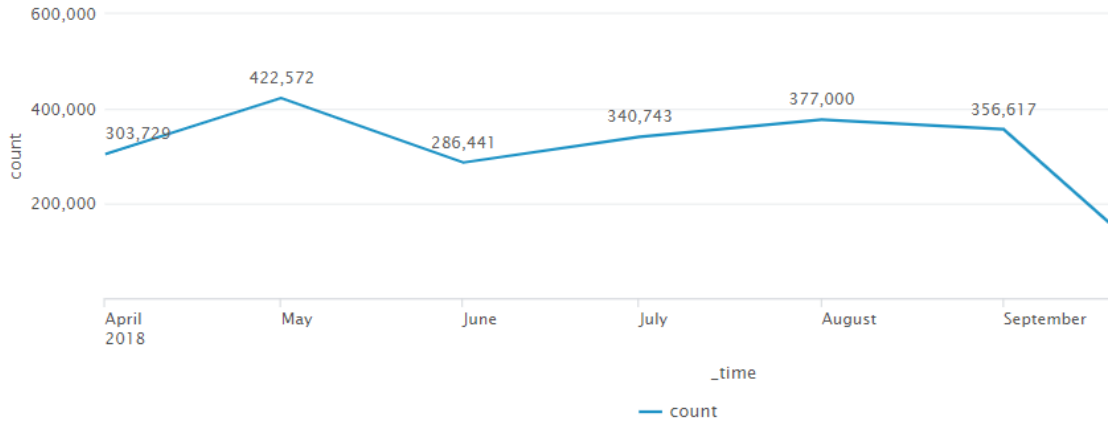
Output

```
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)
```

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, MSS-UTM for this month there are a total of **356,617** attacks denied by the rules of the firewall.



Based on the information collected from the security measures during this month, all access attempts for BANVIVIENDA were blocked by the configured ACL rules. Different source IP addresses send packets of type ICMP, UDP and TCP to hosts 200.46.227.227 (94%) and 200.46.19.98 (4%). Explore a significant number of attacks that can be considered recognition for subsequent attacks, we recommend that you check the activity of the devices where these events are recorded.

Top 5 countries that frequent the highest number of attacks we can mention:

- China (28%)
- Russian Federation (23%)
- United States (15%)
- Panama (11%)
- Brazil (10%)

For this period, the total of security events for the CISCO ASA was: 8,257,795 which are divided as follows: 7,918,234 were registered in the host 200.46.19.98 and 339,561 were registered in the host 200.46.227.227.

In the following list we can see the actions that were blocked by the ACL rules and

the attacks that were registered in each of them:

Action	Type of attack
• Deny	ANTI-SPOOF
• Connection deny	TCP CHECK
• Deny Inbound	UDP CHECK, ICMP CHECK, DNS SNOOP, L3 DROP

Among the most frequent network activities are: Network Access Point and IKE and IPsec, followed by User Session, Access Lists, IP Stack, NAT and PAT; and High Availability (Failover) these last ones are less frequent.

Types of attacks presented during this month:

Below are the most frequent attacks and the amount that were recorded in each of them.

Type of attack	Count
• ANTI-SPOOF	212,580
• TCP CHECK	95,352
• UDP CHECK	5,572
• MGMT PLANE	875
• ICMP CHECK	432
• DNS SNOOP	234
• L3 DROP	14

Attack attempts blocked towards specific destination Port

In this section, a list of the ports that were selected during the period are listed in descent order where the first port was the one that received the most attacks.

- TELNET (23)
- HTTP (80)
- HTTPS (443)
- SSH (22)
- SNMP (161)

Top Five Source IPs (Local or public)

Private IP address appears in this section because the security countermeasures

device has denied TCP connection to other internal device, this can happen due to misconfigurations. The public IPs is highlighted for quicker recognition.

- 10.200.201.45
- 200.46.201.49
- 10.100.6.98
- 172.104.6.98
- 200.46.67.35

A total of 1,983 connection attempts were made which were denied, coming from the IP address 10.200.201.45 to the host 200.46.227.227.

Top Five 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.

- 200.46.19.98
- 200.46.227.227
- 172.28.1.76
- 172.20.15.43
- 10.100.210.1

Managed End Point Detection and Response Service (MSS-EDR)

The MSS-EDR is a preventive detection and response and a forensic service to identify without signatures and mitigate an attack to the end-points and servers of an organization. The service works by actively seeking malicious activity in the customer's network based on suspicious behaviors (not based on signatures). This technology allows our analysts to detect malicious software that may have evaded existing security countermeasures. At the same time we conduct investigations by responding to a security alert – this service is based on leveraging a powerful investigation platform to shorten the investigation time, respond to more incidents and get to the root cause of each incident.

Many of the alerts registered during this month are brute force, in which users made an excessive amount of failed access attempts when making changes to their passwords. Other events recorded in smaller amounts were Side movement and malicious process command.

The alerts that will be listed below come from activities carried out within your organization (events), which represent a severity level (critical, high, medium, low or informative) according to the registered behavior.

The security analysis performed within the GOC is focused to detect threats, correlate and analyze indicators in four critical areas of an organization: files, users, networks and endpoints.

Below are the most frequent alerts for hosts:

Host	Name alert
BpvExch01	• Lateral Movement • Malicious Process Command/cmd.exe (file)
BpvExch02	• Brute Force • Lateral Movement
bpvblbe1 BPVBLWB1	• Superscan scanner.exe (file) • dwrcas.exe (file)
bpvblwb2 BPVBLBE2	• dwrcas.exe (file)

1. User

- ***Brute Force***

Brute force is a way to get a key to try to access a website by trying all possible combinations to find the one that allows access.

The following table shows the most relevant events related to Brute Force:

User	Number of failed login attempts	First seen	Last seen
meyvis.barahona	11	09/11/2018 21:43	09/11/2018 21:43
carmen.davis	15	09/18/2018 19:11	09/19/2018 13:47
maria.avila	12	09/19/2018 00:20	09/19/2018 00:20
michelle.harris	14	09/21/2018 03:57	09/21/2018 03:57
cynthia.atencio	11	09/21/2018 22:21	09/21/2018 10:21
	11	09/21/2018 22:56	09/21/2018 22:56
	13	09/21/2018 23:10	09/21/2018 23:10
	12	09/22/2018 01:00	09/22/2018 01:00
	14	09/22/2018 02:25	09/22/2018 02:25
michelle.harris	18	09/22/2018 23:24	09/22/2018 23:24
cynthia.atencio	13	09/22/2018 15:21	09/22/2018 15:21
	15	09/22/2018 15:43	09/22/2018 15:43
belisario.castillo	16	09/22/2018 16:32	09/24/2018 11:48
cynthia.atencio	12	09/23/2018 00:23	09/23/2018 00:23
	12	09/23/2018 02:13	09/23/2018 02:13
	15	09/23/2018 02:53	09/23/2018 02:56
	14	09/23/2018 04:00	09/23/2018 04:00
michelle.harris	16	09/23/2018 20:04	09/23/2018 20:04
maria.avila	12	09/24/2018 04:19	09/24/2018 04:19
cynthia.atencio	11	09/24/2018 05:10	09/24/2018 05:10
	17	09/24/2018 05:11	09/24/2018 05:11
michelle.harris	16	09/24/2018 11:48	09/24/2018 11:48
	13	09/24/2018 12:29	09/24/2018 12:29
	21	09/24/2018 12:37	09/24/2018 12:37
	11	09/24/2018 12:42	09/24/2018 12:42
dora.rosas	12	09/25/2018 15:24	09/25/2018 15:24

eduardo.alain	11	09/26/2018 11:01	09/26/2018 11:01
	14	09/26/2018 12:43	09/26/2018 12:43
webmail.banvivienda.com\ agustin.calderon	25	09/26/2018 04:36	09/26/2018 04:36
agustin.calderon	11	09/27/2018 03:27	09/27/2018 03:27
	11	09/27/2018 04:02	09/27/2018 04:02
carmen.davis	24	09/27/2018 17:20	09/27/2018 17:20
francias.barria	16	09/27/2018 19:53	09/27/2018 19:53
	15	09/27/2018 20:53	09/27/2018 20:53
carmen.davis	11	09/28/2018 18:32	09/28/2018 18:32
	24	09/29/2018 01:44	09/29/2018 01:44
	16	09/29/2018 14:22	09/29/2018 14:22
belisario.castillo	13	09/29/2018 18:40	09/29/2018 18:42
	11	09/29/2018 18:54	09/29/2018 18:54
	14	09/29/2018 18:55	09/29/2018 18:57
carmen.davis	16	09/29/2018 19:23	09/29/2018 23:38
deyvis.tejedor	13	09/30/2018 18:10	09/30/2018 18:10
agustin.calderon	12	09/30/2018 23:46	10/1/2018 02:50

This event has a high level of severity and is registered on the host BpvExch02.

- ***Lateral Movement***

The following table shows the events related to lateral movement:
This section shows the hosts and users where this activity was registered, the level of severity it represents, IP host and the date.

Severity:	**High**			
Host	BpvExch01		BpvExch02	
User	ruthsara.quintero	milena.batista	agustin.calderon	milena.batista
First seen	10/09/2018 22:50	10/09/2018 22:50	10/09/2018 23:25	10/09/2018 23:25
Last seen	10/09/2018 22:50	10/09/2018 22:50	10/09/2018 23:25	10/09/2018 23:25
Host IP	200.46.19.98			

2. File

The following tables will show the files that were registered with malicious behavior:

- ***scanner.exe***

Description:	Superscan is a security scanner used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Superscan sends specially crafted packets to the target host and then analyzes the responses.	
Severity:	Medium	
Host	bpvblbe1	BPVBLWB1
User	gmadm00	gmadm00
First seen	06/09/2018 22:45	04/09/2018 23:30
Last seen	06/09/2018 22:45	04/09/2018 23:30
Path	c:\program files (x86)\superscan\scanner.exe	
Hash	AFA241787FDE424249C8B445B1D66F40DE8B08BC7BED7BEF97C1FEC4B069E53B	

- ***cmd.exe***

Description:	A modification of the register of user accounts was made by a script.
Severity:	Critical
Host	BpvExch01
User	jorge.jarpa
First seen	10/09/2018 23:01
Last seen	10/09/2018 23:01
Path	c:\windows\system32\cmd.exe
Malicious Command Line	C:\Windows\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
Hash	6F88FB88FFB0F1D5465C2826E5B4F523598B1B8378377C8378FFEBC171BAD18B

- ***dwrcas.exe***

Description	DameWare Software that allows a remote "operator" to control a system as if it had physical access to that system.

Severity	Informative			
Host	bpvblbe1	BPVBLWB1	bpvblwb2	BPVBLBE2
First seen	04/09/2018 23:33	06/09/2018 22:35	10/09/2018 22:17	10/09/2018 22:17
Last seen	04/09/2018 23:33	06/09/2018 22:35	10/09/2018 22:17	10/09/2018 22:17
Path	c:\windows\syswow64\dwrcs.exe			
Hash	EB30A0075CDC0C3DDEA9B22B92E4D0F275932F9FDCB10B9D4D4BD8B3C03DA0BE			

All these activities that were reported during the month of September were notified and informed to the client.

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