REPORTE DE OPERACIONES E INTELIGENCIA TECNICO DE CIBERSEGURIDAD

BANVIVIENDA

Octubre 2018

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

Info@glesec.com
www.glesec.com

Tabla de contenido

Tabla de contenido 2
Acerca de este reporte 3
Confidencialidad 3
Servicio Administrado de Vulnerabilidades 4
Descripción por Host 7
Vulnerabilidades de alta severidad 11
Vulnerabilidades de severidad media 12
Vulnerabilidades de severidad baja 13
Amenazas 16
Servicio de Detección y Respuesta en Dispositivos Finales 19

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

Acerca de este reporte

Este informe es un complemento del Informe ejecutivo mensual de inteligencia y operaciones. El propósito de este documento es proporcionar información a nivel técnico y táctico, detalles y recomendaciones en la medida en que puedan resumirse. GESEC procesa una gran cantidad de datos y no se puede presentar en un formato de informe detallado. Para obtener más información, puede consultar los paneles de la GMP o, si es necesario, comuníquese con nosotros en los Centros de operaciones de GLESEC (GOC).

Confidencialidad

GLESEC considera la confidencialidad de la información de los clientes como un secreto comercial. La información bajo este contexto se clasifica como:

- Nombre e información de contacto del cliente
- Arquitectura del sistema, configuración, métodos de acceso y control de acceso
- Contenido de seguridad

Todo lo mencionado arriba es resguardado de manera segura de la misma forma como GLESEC resguarda su propia información confidencial.

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

Servicio Administrado de Vulnerabilidades (MSS-VM)

El Servicio Administrado de Vulnerabilidades (MSS-VM) permite a las organizaciones minimizar los riesgos de las vulnerabilidades mediante la rápida detección de debilidades, midiendo el riesgo potencial y la exposición, generar alertas, proveer información de remediación necesaria para mitigar estos riesgos de forma regular y facilitando el reporte de desviaciones y el cumplimiento con las regulaciones y mejores prácticas.

Según el rango de direcciones proporcionado por BANVIVIENDA, hemos encontrado un total de 15 hosts, de los cuales 10 son vulnerables. Estas vulnerabilidades se dividen en las siguientes severidades como se muestra en la siguiente tabla. Además, puede observar la Métrica de Valor de riesgo de su organización de acuerdo con nuestras métricas.

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	21	7	28
Service detection		4	0	0	4
Misc.		0	2	1	3
Windows		0	1	0	1

- General

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

- Detección de servicios
- Misceláneos
- Windows

Para este mes descubrimos un total de 15 hosts, de los cuales 10 son vulnerables, BANVIVIENDA presenta un total de 40 vulnerabilidades; las cuales se dividen de la siguiente manera: 4 vulnerabilidades de riesgo alto, 26 vulnerabilidades de riesgo medio y 9 vulnerabilidades de riesgo bajo. No se han encontrado vulnerabilidades de gravedad crítica durante este mes.

A continuación, se muestran las categorías mas vulnerables:

GENERAL (77.7%) algunas de las vulnerabilidades que se presenta son de tipo:

Valor	Cantidad	Severidad
• SSL Medium Strength Cipher Suites Supported	6	Media
• SSL RC4 Cipher Suites Supported (Bar Mitzvah)	5	Baja

DETECCIÓN DE SERVICIO (11.1%) presenta solamente la vulnerabilidad de tipo:

Valor	Cantidad	Severidad
• SSL Version 2 and 3 Protocol Detection	4	Alta

MISCELÁNEOS (8.3%) algunas de las vulnerabilidades que se presentan son de tipo:

Valor	Cantidad	Severidad
• SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	1	Media
• SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	1	Media

WINDOWS (2.7%) la única vulnerabilidad que se presenta es de tipo:

Valor	Cantidad	Severidad
• Microsoft Exchange Client Access Server Information Disclosure	1	Media

Continúa presentando la vulnerabilidad severidad alta del tipo SSL Version 2 and 3

Protocol Detection en los hosts 200.90.137.87, 200.90.137.89, 200.46.19.100 y 200.46.227.230 (tienen puertos 443, 25, 10000 y 500 vulnerables), y pertenece a la categoría de Detección de Servicios.

Principales hosts vulnerables para este período: 200.90.137.87, 200.90.137.89, 200.46.227.230, 200.90.137.91, 200.90.137.94 y 200.46.19.100. La mayoría de estos hosts son vulnerables por el protocolo TCP, a excepción de los hosts 200.46.19.98 y 200.46.227.277 que muestran una vulnerabilidad en el protocolo UDP.

Los puertos más vulnerables para este período son:

- 443 (https) la mayoría de los hosts son vulnerables por este puerto, entre ellos tenemos: 200.46.227.230, 200.90.137.91, 200.46.19.100 y 200.90.137.94.

- 25 (smtp) los 2 hosts vulnerables por este puerto son: 200.90.137.87 y 200.90.137.89.

- 10000 (ndmp), el único host vulnerable para este puerto es 200.90.137.91 y tiene las siguientes vulnerabilidades SSL Certificate Cannot Be Trusted, SSL Certificate Signed Using Weak Hashing Algorithm and SSL Self-Signed Certificate.

- 500 (Ipsec) los 2 hosts vulnerables por este puerto son: 200.46.19.98 y 200.46.227.277 tienen una vulnerabilidad de tipo Microsoft Exchange Client Access Server Information Disclosure.

Entre las vulnerabilidades más frecuentes para este periodo tenemos:

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

Lo más recomendable sería reforzarlos, puede encontrar más información sobre

ellos en la sección de inteligencia para MSS-VM.

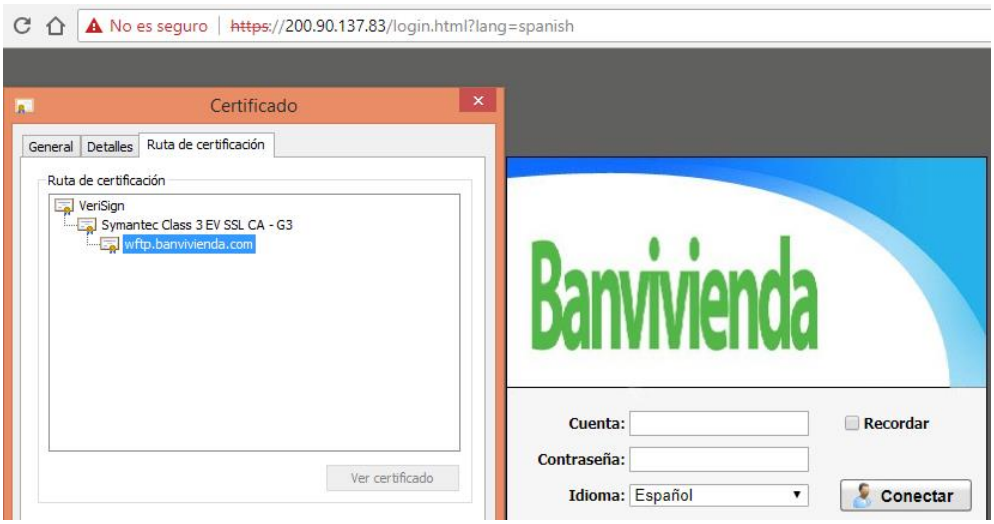
Descripción por Host

Actualmente se siguen presentando la mayoría de las vulnerabilidades que el mes anterior:

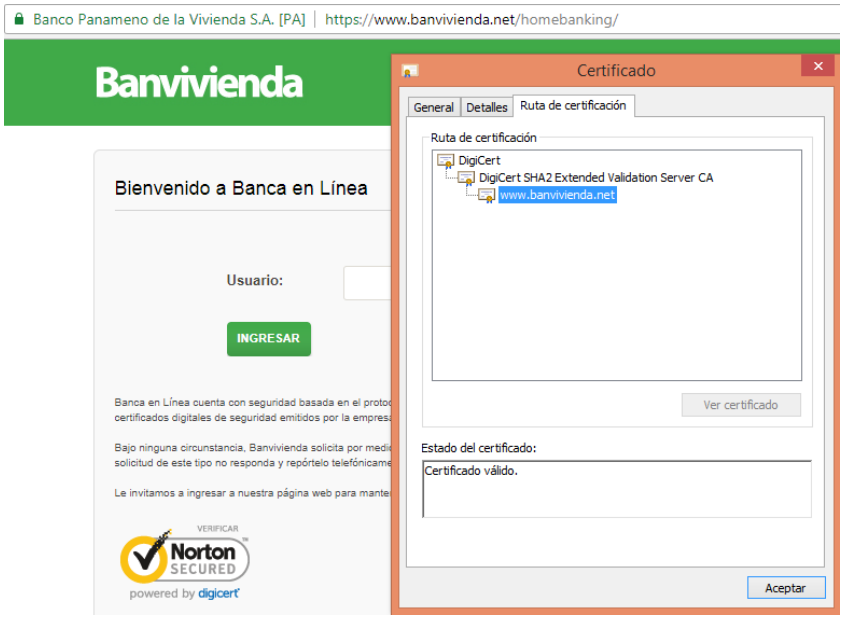
Los siguientes hosts **200.90.137.89** y **200.90.137.87** presentan las mismas vulnerabilidades:
Varias vulnerabilidades encontradas en estos hosts se indican aquí:
SSL Certificate Cannot Be Trusted, SSL Certificate Signed Using Weak Hashing Algorithm, SSL Medium Strength Cipher Suites Supported, SSL 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).
Recomendamos seguir el procedimiento de solución para estos problemas, descrito en la sección Vulnerabilidades por gravedad de este documento.

200.46.227.230 (https://www.banvivienda.com/es)
Varias vulnerabilidades encontradas en ese host se indican aquí:
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. Recomendamos seguir el procedimiento de solución para estos problemas, descrito en la sección Vulnerabilidades por gravedad de este documento.

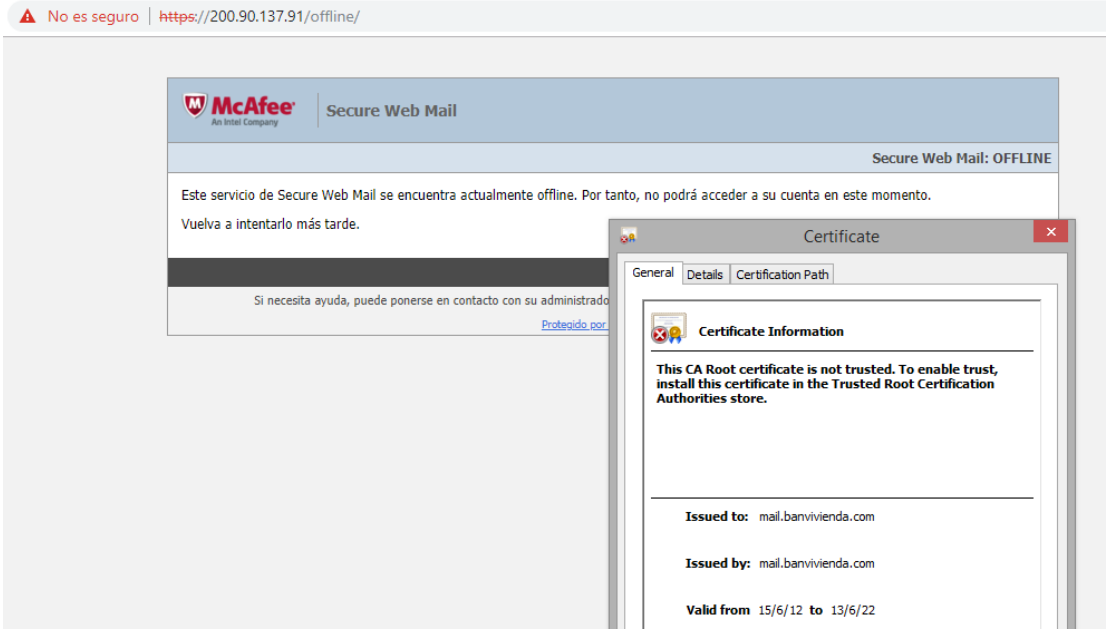
200.90.137.83 (https://200.90.137.83/login.html)
La vulnerabilidad encontrada en este host es:
SSL Medium Strength Cipher Suites Supported. Recomendamos seguir el procedimiento de solución para estos problemas, descrito en la sección Vulnerabilidades por gravedad de este documento.



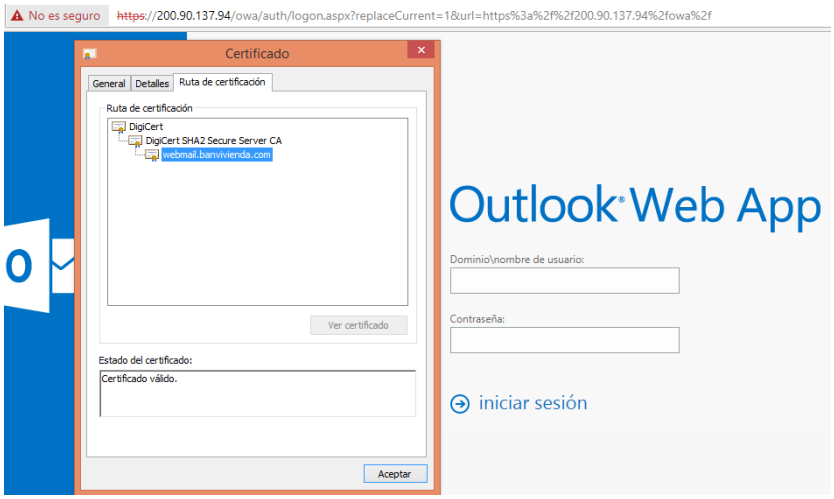
200.46.19.100 (https://www.banvivienda.net/homebanking/)
Varias vulnerabilidades encontradas en ese host se indican aquí:
SSL Version 2 and 3 Protocol Detection, SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE), SSL RC4 Cipher Suites Supported (Bar Mitzvah). Recomendamos seguir el procedimiento de solución para estos problemas, descrito en la sección Vulnerabilidades por gravedad de este documento.



200.90.137.91 (https://200.90.137.91/offline/)
Varias vulnerabilidades encontradas en ese host se indican aquí:
SSL Certificate Cannot Be Trusted, SSL Certificate Signed Using Weak Hashing Algorithm, SSL Self-Signed Certificate. Recomendamos seguir el procedimiento de solución para estos problemas, descrito en la sección Vulnerabilidades por gravedad de este documento.



200.90.137.94
(https://200.90.137.94/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2f200.90.137.94%2fowa%2f)
Varias vulnerabilidades encontradas en ese host se indican aquí:
Microsoft Exchange Client Access Server Information Disclosure, SSL Medium Strength Cipher Suites Supported, SSL RC4 Cipher Suites Supported (Bar Mitzvah). Recomendamos seguir el procedimiento de solución para estos problemas, descrito en la sección Vulnerabilidades por gravedad de este documento.



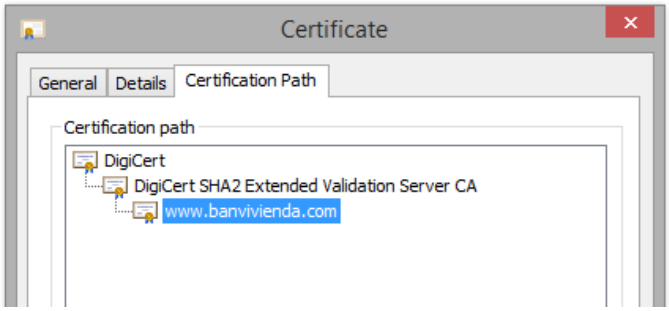
200.90.137.84

Varias vulnerabilidades encontradas en ese host se indican aquí:

SSL Medium Strength Cipher Suites Supported, SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam). Recomendamos seguir el procedimiento de solución para estos problemas, descrito en la sección Vulnerabilidades por gravedad de este documento.

Not Found

HTTP Error 404. The requested resource is not found.



Los hosts **200.46.19.98** y **200.46.227.227** tienen la siguiente vulnerabilidad:

Aggressive Internet Key Interchange Mode (IKE) with pre-shared key". Recomendamos seguir el procedimiento de solución para estos problemas, descrito en la sección Vulnerabilidades por gravedad de este documento.

De los ataques realizados a su organización, el 94% va específicamente al host 200.46.227.277 y el 6% va al host 200.46.19.98.

Vulnerabilidades por severidad

La siguiente sección describirá en detalle cada vulnerabilidad encontrada de acuerdo con su gravedad.

Vulnerabilidades de severidad alta

SSL Version 2 and 3 Protocol Detection

Descripción
El servicio remoto acepta conexiones cifradas utilizando SSL 2.0 y / o SSL 3.0. Estas versiones de SSL se ven afectadas por varias fallas criptográficas, que incluyen:

- Un esquema de relleno inseguro con cifrados CBC.

- Esquemas inseguros de renegociación y reanudación de sesiones.

Un atacante puede explotar estas fallas para realizar ataques de intermediarios o para descifrar las comunicaciones entre el servicio afectado y los clientes.

Si bien SSL / TLS tiene un medio seguro para elegir la versión con mayor compatibilidad del protocolo (de modo que estas versiones solo se utilizarán si el cliente o el servidor no admiten nada mejor), muchos navegadores web implementan esto de una manera insegura que le permite a un atacante degradar una conexión (como en POODLE). Por lo tanto, se recomienda que estos protocolos estén completamente desactivados.

Solución
Consulte la documentación de la aplicación para deshabilitar SSL 2.0 y 3.0.
Utilice TLS 1.1 (con conjuntos de cifrado aprobados) o superior en su lugar.

Sistemas Afectados
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.

Vulnerabilidades de severidad media

SSL Medium Strength Cipher Suites Supported

Descripción
El host remoto admite el uso de cifrados SSL que ofrecen cifrado de intensidad media. GLESEC considera la fuerza media como cualquier cifrado que utiliza longitudes de clave de al menos 64 bits y menos de 112 bits, o bien que utiliza el conjunto de cifrado 3DES.

Tenga en cuenta que es considerablemente más fácil evitar el cifrado de intensidad media si el atacante está en la misma red física.

Solución
Reconfigure la aplicación afectada si es posible para evitar el uso de cifrados de resistencia media.

Sistemas Afectados
25 / tcp / smtp 200.90.137.87, 200.90.137.89

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

SSL Certificate Signed Using Weak Hashing Algorithm

Description
El servicio remoto utiliza una cadena de certificados SSL que se ha firmado con un algoritmo de hashing criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a los ataques de colisión. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, permitiendo que un atacante se haga pasar por el servicio afectado.

Tenga en cuenta que este complemento informa de todas las cadenas de

certificados SSL firmadas con SHA-1 que caducan después del 1 de enero de 2017 como vulnerables. Esto está de acuerdo con la puesta en marcha gradual de Google del algoritmo hash criptográfico SHA-1.

Sistemas Afectados

25 / tcp / smtp	200.90.137.87200.90.137.89
443 / tcp / possible_wls	200.90.137.83,200.90.137.83
443 / tcp / possible_wls	200.46.227.230, 200.46.227.230
443 / tcp / possible_wls	200.90.137.91
10000 / tcp / possible_wls	200.90.137.91

SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability(POODLE)

Description

El host remoto se ve afectado por una vulnerabilidad de divulgación de información de man-in-the-middle (MitM) conocida como POODLE. La vulnerabilidad se debe a la forma en que SSL 3.0 maneja los bytes de relleno al descifrar mensajes encriptados usando cifrados de bloque en el modo de encadenamiento de bloques de cifrado (CBC).

Los atacantes de MitM pueden descifrar un byte seleccionado de un texto cifrado en tan solo 256 intentos si pueden forzar a una aplicación víctima a enviar repetidamente los mismos datos a través de las conexiones SSL 3.0 recién creadas.

Solución

Desactivar SSLv3.

Sistemas Afectados

443 / tcp / www	200.46.19.100, 200.46.19.100, 200.90.137.83

Vulnerabilidades de severidad baja

SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Descripción

El host remoto admite el uso de RC4 en una o más suites de cifrado.

El cifrado RC4 tiene fallas en su generación de un flujo de bytes pseudoaleatorios,

por lo que se introduce una amplia variedad de pequeños sesgos en el flujo, lo que disminuye su aleatoriedad.

Si el texto simple se cifra repetidamente (por ejemplo, las cookies HTTP), y un atacante puede obtener muchos textos cifrados (es decir, decenas de millones), el atacante puede derivar el texto simple.

Solución
Reconfigure la aplicación afectada, si es posible, para evitar el uso de cifrados RC4. Considere el uso de TLS 1.2 con las suites AES-GCM sujetas a soporte de navegador y servidor web.

Sistemas Afectados
25 / tcp / smtp 200.90.137.87, 200.90.137.89
443 / tcp / possible_wls 200.90.137.94
443 / tcp / possible_wls 200.46.19.100, 200.46.19.100,200.90.137.83, 200.90.137.83
443 / tcp / possible_wls 200.46.227.230

OpenSSL AES-NI Padding Oracle MitM Information Disclosure

Descripción
El host remoto se ve afectado por una vulnerabilidad de divulgación de información de man-in-the-middle (MitM) debido a un error en la implementación de conjuntos de cifrado que utilizan AES en modo CBC con HMAC-SHA1 o HMAC-SHA256.
La implementación está especialmente escrita para utilizar la aceleración AES disponible en los procesadores x86 / amd64 (AES-NI). Los mensajes de error devueltos por el servidor permiten que un atacante de tipo "man in the middle" realice un ataque de oráculo de relleno, lo que da como resultado la capacidad de descifrar el tráfico de la red.

Solución
Actualice a la versión 1.0.1t / 1.0.2h o posterior de OpenSSL..

Sistemas Afectados
25 / tcp / smtp 200.90.137.87, 200.90.137.89

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

Descripción

El host remoto permite conexiones SSL / TLS con uno o más módulos Diffie-Hellman menores o iguales a 1024 bits. A través del análisis criptográfico, un tercero puede encontrar el secreto compartido en un corto período de tiempo (dependiendo del tamaño del módulo y los recursos del atacante). Esto puede permitir a un atacante recuperar el texto sin formato o potencialmente violar la integridad de las conexiones.

Solución

Reconfigure el servicio para usar un único módulo Diffie-Hellman de 2048 bits o más.

Sistemas Afectados

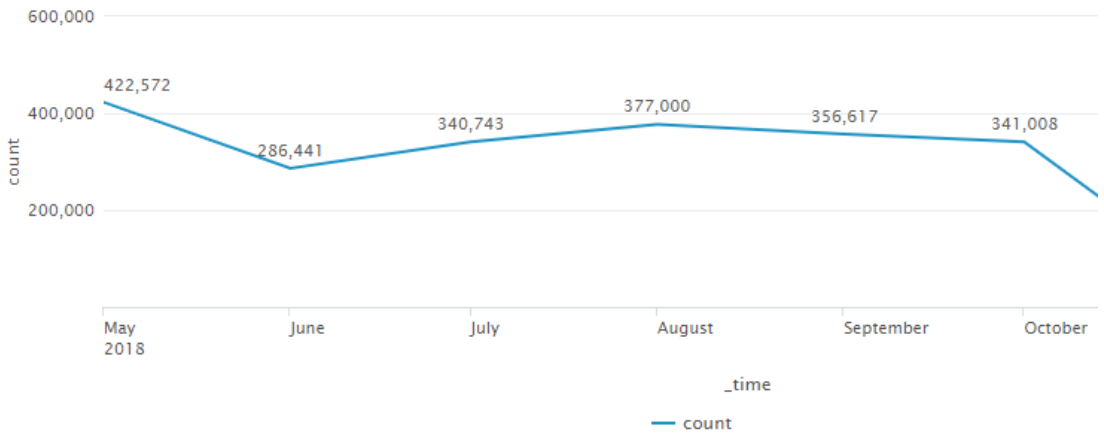
443 / tcp / possible_wls 200.90.137.84

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

Amenazas

GLESEC utiliza MSS-APS, MSS-EPS, MSS-SIEM, MSS-EDR y MSS-UTM para determinar la actividad de inteligencia de amenazas.

Las amenazas informadas por MSS-APS, MSS-EPS, MSS-SIEM, MSS-EDR, MSS-UTM para este mes, hay un total de **341,008** ataques denegados por las reglas del firewall.



En base a la información recopilada de las medidas de seguridad durante este mes, todos los intentos de acceso para BANVIVIENDA fueron bloqueados por las reglas de ACL configuradas. Las diferentes fuentes de direcciones IP envían paquetes de tipo ICMP, UDP y TCP a los hosts 200.46.227.227 (93.6%) y 200.46.19.98 (6.36%). Explore una cantidad significativa de ataques que pueden considerarse reconocimiento por ataques posteriores, le recomendamos que verifique la actividad de los dispositivos donde se registran estos eventos.

Entre los 5 principales países que frecuentan el mayor número de ataques están:

- China (29%)
- Rusia (19%)
- Estados Unidos (17%)
- Brasil (11%)
- Panamá (8.5%)

Para este período, el total de eventos de seguridad para CISCO ASA fue: 1,371,815; que se dividen de la siguiente manera: 1,042,328 se registraron en el host 200.46.19.98 y 329,487se registraron en el host 200.46.227.227.

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

En la siguiente lista podemos ver las acciones que fueron bloqueadas por las reglas de ACL y los ataques que se registraron en cada una de ellas:

Acción	Tipo de Ataque
• Deny	ANTI-SPOOF
• Connection deny	TCP CHECK
• Deny Inbound	UDP CHECK, ICMP CHECK, DNS SNOOP, L3 DROP

Entre las actividades de red más frecuentes se encuentran: Network Access Point, IKE and IPsec, User Session, Access Lists, IP Stack, NAT and PAT, High Availability (Failover) y Command Interface.

Tipos de ataques presentados durante este mes:

A continuación, se muestran los ataques más frecuentes y la cantidad que se registró en cada uno de ellos.

Tipo de ataque	Cantidad
• ANTI-SPOOF	162,085
• TCP CHECK	126,780
• UDP CHECK	6,978
• MGMT PLANE	923
• ICMP CHECK	840
• DNS SNOOP	258
• L3 DROP	17

Intentos de ataque bloqueados hacia un puerto de destino específico

En esta sección, muestra una lista de los puertos atacados durante este período se enumeran en orden descendente donde el primer puerto fue el que recibió la mayoría de los ataques.

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

Las cinco principales fuentes de IP (locales o públicas)

La dirección IP privada aparece en esta sección porque el dispositivo de contramedidas de seguridad ha denegado la conexión TCP a otro dispositivo interno, esto puede suceder debido a configuraciones erróneas. Las IP públicas se destacan para un reconocimiento más rápido

- 200.46.73.116 (24%)
- 10.100.201.49 (22%)
- 104.248.119.106 (11%)
- 104.248.67.229 (9.9%)
- 200.46.136.31 (9.8%)

Los cinco principales IP de destino (locales o públicos)

En esta sección presentamos las direcciones IP de destino de las conexiones denegadas o descartadas que fueron más recurrentes durante este período.

- 200.46.227.227
- 200.46.19.98
- 172.20.15.43
- 172.16.99.99
- 172.16.78.15

Servicio de Detección y Respuesta en Dispositivos Finales (MSS-EDR)

El MSS-EDR es un servicio de detección preventiva, respuesta y forense para identificar sin firmas y mitigar un ataque a los puntos finales y servidores de una organización. El servicio funciona buscando activamente actividad maliciosa en la red del cliente en función de comportamientos sospechosos (no basados en firmas). Esta tecnología permite a nuestros analistas detectar software malicioso que puede haber evadido las contramedidas de seguridad existentes. Al mismo tiempo, llevamos a cabo investigaciones respondiendo a una alerta de seguridad: este servicio se basa en aprovechar una poderosa plataforma de investigación para acortar el tiempo de investigación, responder a más incidentes y llegar a la causa raíz de cada incidente.

Todas las alertas registradas en este mes son de fuerza bruta, debido a que los usuarios realizaban una cantidad excesiva de intentos de acceso fallidos al realizar cambios en sus contraseñas.

Las alertas que se enumeran a continuación provienen de actividades realizadas dentro de su organización (eventos), que representan un nivel de gravedad (crítico, alto, medio, bajo o informativo) de acuerdo con el comportamiento registrado.

El análisis de seguridad realizado dentro de nuestro GOC se centra en detectar amenazas, correlacionar y analizar indicadores en cuatro áreas críticas de su organización: archivos, usuarios, redes y puntos finales.

1. Usuario

Fuerza Bruta

- Entre los usuarios más frecuentes que presentaron esta alerta podemos mencionar: angeliki.gionis (23%), agustin.calderon (20%), rolando.rojas (12%), deyvis.tejedor (5%) y jose.mulino (4%).
- Se registro un total de 142 eventos.

A continuación, se listan un resumen de los eventos más relevantes relacionados a fuerza bruta para este periodo.

Incidente detectado			
Fecha	**Hora**	**Usuario**	**Numero de Intentos Fallidos**
4 OCTUBRE	11:02	deyvis.tejedor	16
5 OCTUBRE	12:06	rolando.rojas	12
	16:56	Jazmin.perez	22
6 OCTUBRE	10:00	Rolando.rojas	12
	11:09	Rolando.rojas	14
	11:33	Jazmin.perez	12
	12:55	Rolando.rojas	26
7 OCTUBRE	21:22	Jazmin.perez	28
	22:21	Jannet.giraldez	12
8 ORTUBRE	08:21	Rolando.rojas	20
	10:17	Jazmin.perez	12
	15:12	Jezer-mock	15
9 OCTUBRE	13:30	Agustin.calderon	16
10 OCTUBRE	17:25		17
11 OCTUBRE	10:11	Joaquin.victoria	24
	13:39	Maria.avila	12
	18:48	Agutin.calderon	15
14 OCTUBRE	14:39 – 22:35	Angeliki.gionis	De 16 a 126
15 OCTUBRE	9:07	Eiber.gonzales	11
16 OCTUBRE	7:56	Angeliki.gionis	16
19 OCTUBRE	17:12 – 17:15	Vielka.garcia	21
20 OCTUBRE	9:08	Giancarlo.guevara	15
21 OCTUBRE	22:31	Maria.avila	12
23 OCTUBRE	12:34	Emanuel.jeanm	11
27 OCTUBRE	19:16	Deyvis.tejedor	11
	19:23	Jose.mulino	112
28 OTUBRE	03:04	Deyvis.tejedor	12
	15:17	Jose.mulino	16

29 OCTUBRE	07:52	Deyvis.tejedor	12
	07:54	Jose.mulino	20
	13:34	Lina.delaguardia	14
	14:25	Belisario.castillo	13
	15:01	Lina.delaguardia	18
	15:04	Belisario.castillo	19
	16:02	Jose.mulino	18
	19:47	Maria.avila	12
30 OCTUBRE	05:56	Linda.delaguardia	16
	09:33	Jose.mulino	14
	01:09	Agapito.bustamante	14
31 OCTUBRE	21:02	Jose.mulino	134
	22:35	Deyvis.tejedor	11

El evento de Fuerza Bruta tiene un nivel de severidad alto y se registra en el host BpvExch02.

Todas estas actividades que fueron reportadas durante el mes de octubre fueron notificadas e informadas al cliente.

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

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

Info@glesec.com
www.glesec.com