REPORTE DE OPERACIONES E INTELIGENCIA TÉCNICO DE CIBERSEGURIDAD

Copa Airlines

Octubre 2018

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

Info@glesec.com

www.glesec.com

CONFIDENCIAL

Tabla de Contenidos

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 de Vulnerabilidades Administrado (MSS-VM)

El Managed Vulnerability Service (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.

De acuerdo con el nuevo rango de direcciones IP provisto por COPA AIRLINES, 49 equipos fueron descubiertos de los cuales 33 son vulnerables.

El número total de vulnerabilidades presentadas en Copa Airlines para el mes de octubre es 103, esto muestra un incremento comparado al mes anterior (24). Estas vulnerabilidades están clasificadas de acuerdo con las siguientes severidades: 4 críticas, 8 altas, 67 medias y 24 bajas.

Adicionalmente puede observar que el valor de riesgo de su organización ha subido un 4% de acuerdo con nuestras métricas.

Total IP's Scanned				IP's Vulnerable
49				33
Risk Distribution				
Critical	**High**	**Medium**	**Low**	**Total**
4	8	67	24	103

According to the metrics:

RV= 0.3001188825

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

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

Todas las vulnerabilidades descubiertas en su organización pertenecen a las siguientes categorías:

Category	Critical	High	Medium	Low	Total
General	0	0	48	10	58
Misc.	0	0	7	11	18
Service detection	0	7	0	0	7
CGI abuses	0	1	5	0	6
Web Servers	1	0	5	0	6
FTP	0	0	1	3	4
Windows	3	0	1	0	4

- General (56%)
- Misc. (17%)
- Service Detection (7%)
- Web Servers (6%)
- CGI abuses (6%)
- FTP (4%)
- Windows (4%)

Detalles adicionales sobre estas vulnerabilidades están descritos en la sección del MSS-VM Vulnerabilidades encontradas en COPA AIRLINES por severidad en la **página 12**.

En general, las vulnerabilidades de COPA AIRLINES en este período fueron: 4 riesgo crítico, 8 riesgo alto, 67 riesgo medio y 24 riesgo bajo. Los hosts 200.46.240.230, 200.46.200.161, 200.46.240.24 presentan la vulnerabilidad del tipo MS15-034: Una vulnerabilidad en HTTP.sys podría permitir la ejecución remota de código (3042553) (uncredentialed check) y el host 200.46.240.139 presenta una vulnerabilidad del tipo Microsoft IIS 6.0 Detección de versión no soportada; Ambas vulnerabilidades son de riesgo CRÍTICO.

Otra vulnerabilidad de ALTA severidad que se continúa presentando para su organización, es permitir conexiones cifradas a través de SSL 2.0 y SSL 3, ya que se sabe que son vulnerables a varios tipos de ataques, entre los hosts que presentan esta vulnerabilidad tenemos: 201.218.212.10, 201.218.212.9, 200.406.240.228, 200.46.240.195, 200.46.240.179, 200.46.240.82 and 200.46.240.30.

A continuación, se presentan las vulnerabilidades más frecuentes por categoría en este período son:

General

Value	Count	Risk
• SSL Medium Strength Cipher Suites Supported	14	Medium
• SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)	13	Medium

Misc.

Value	Count	Risk
• Network Time Protocol (NTP) Mode 6 Scanner	4	Medium
• SSH Server CBC Mode Ciphers Enabled	4	Low

Service Detection

Value	Count	Risk
• SSL Version 2 and 3 Protocol Detection	7	High

Web Servers

Value	Count	Risk
• F5 BIG-IP Cookie Remote Information Disclosure	3	Medium
• Web Application Potentially Vulnerable to Clickjacking	2	Medium
• Microsoft IIS 6.0 Unsupported Version Detection	1	Critical

Los puertos más vulnerables para este período son:

• 443, la mayoría de los hosts son vulnerables por este puerto, entre ellos tenemos: 201.218.212.9, 201.218.212.10, 200.46.240.179, 200.46.240.228 y 200.46.240.30.

• 5061, el host vulnerable por este puerto es 200.46.240.195.

• 500, el host vulnerable por este puerto es 201.218.212.9.

La mayoría de estas vulnerabilidades son de gravedad media.

Principales hosts vulnerables para este período: 200.46.240.82, 200.46.240.30, 200.46.240.24, 200.46.240.1 y 52.86.152.128. La mayoría de estos son vulnerables por el protocolo TCP, excepto el host 201.218.212.9 que es vulnerable por el protocolo UDP.

Lo más recomendable sería reforzarlos, puede encontrar más información sobre ellos en la sección de inteligencia para MSS-VM.

Descripción por host

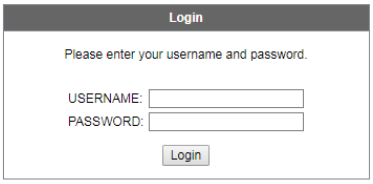
- 201.218.212.9 (https://201.218.212.9/+CSCOE+/logon.html)
- 200.46.240.82 (http://200.46.240.82/wtouch/ereps.EXE)
- 201.218.212.72 (http://201.218.212.72/Homepage.aspx?lang=en)
- 201.218.212.35 (https://201.218.212.35/+CSCOE+/logon.html#form_title_text)
- 200.46.240.137(https://200.46.240.137/wtouch/wtouch.exe/index?MAC=0&VER=1)
- 201.218.212.175(https://201.218.212.175/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2f201.218.212.175%2fowa%2f)

Varias de las vulnerabilidades encontradas en este host se mencionan aquí:

Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key, 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, SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE), TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE), SSL RC4 Cipher Suites Supported (Bar Mitzvah), F5 BIG-IP Cookie Remote Information Disclosure, Web Application Potentially Vulnerable to Clickjacking. Recomendamos seguir el procedimiento de solución para estos problemas, descrito en la sección Vulnerabilidades por gravedad de este documento.

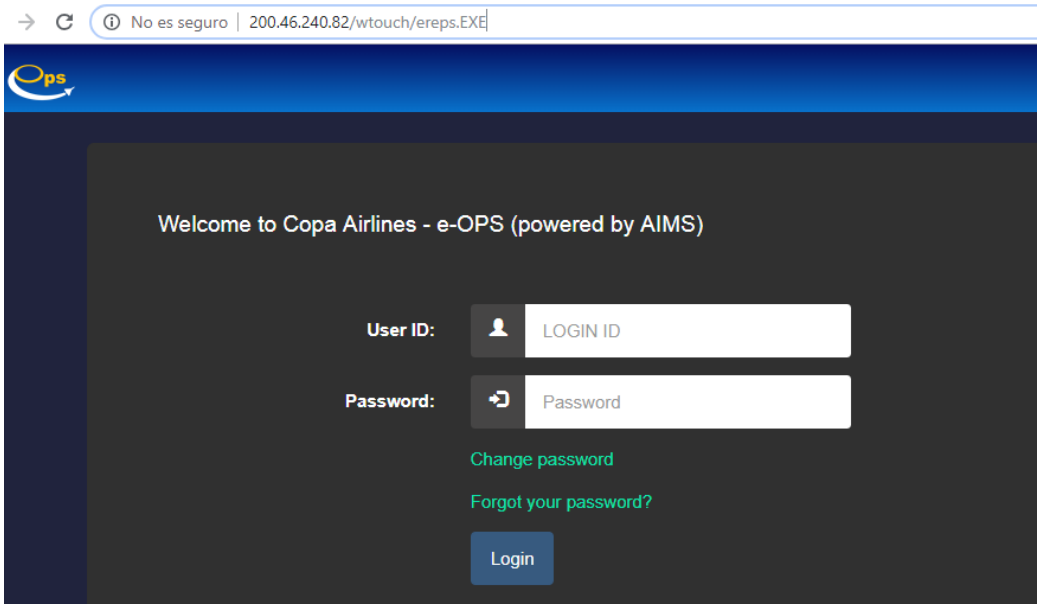
https://201.218.212.9/+CSCOE+/logon.html
Esta dirección IP tiene las siguientes vulnerabilidades: SSL Version 2 and 3 Protocol Detection, Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key, SSL Certificate Cannot Be Trusted, SSL Certificate Signed Using Weak Hashing Algorithm, SSL Medium Strength Cipher Suites Supported , SSL Self-Signed Certificate, SSL / TLS

Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST), SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) y TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE).



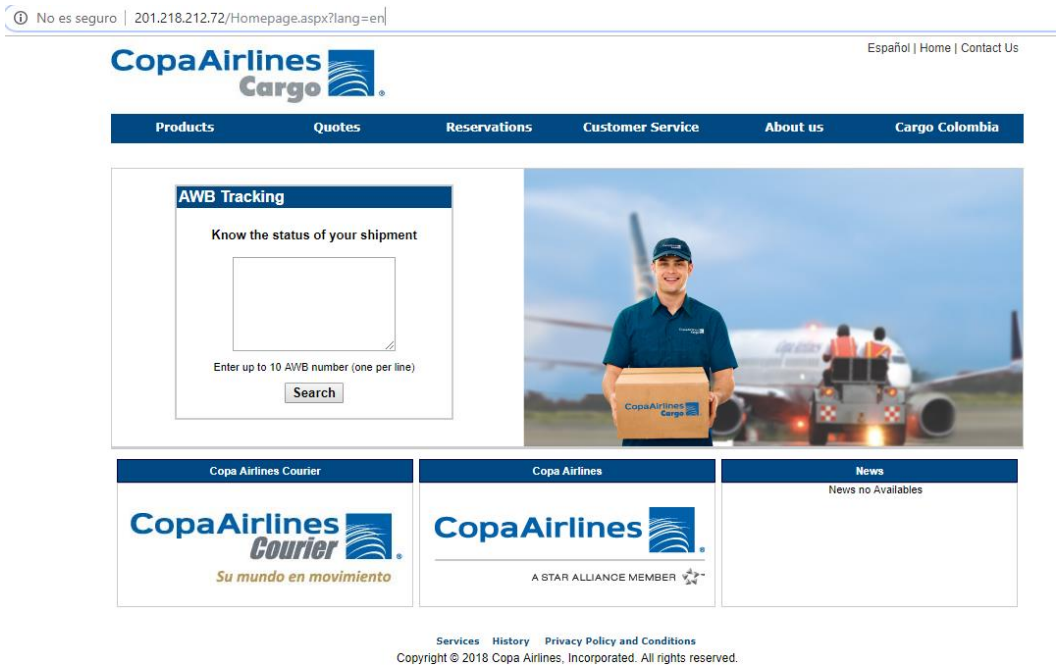
http://200.46.240.82/wtouch/ereps.EXE

Esta dirección IP tiene las siguientes vulnerabilidades: SSL Version 2 and 3 Protocol Detection, SSL Medium Strength Cipher Suites Supported, SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE), SSL RC4 Cipher Suites Supported (Bar Mitzvah) y SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)



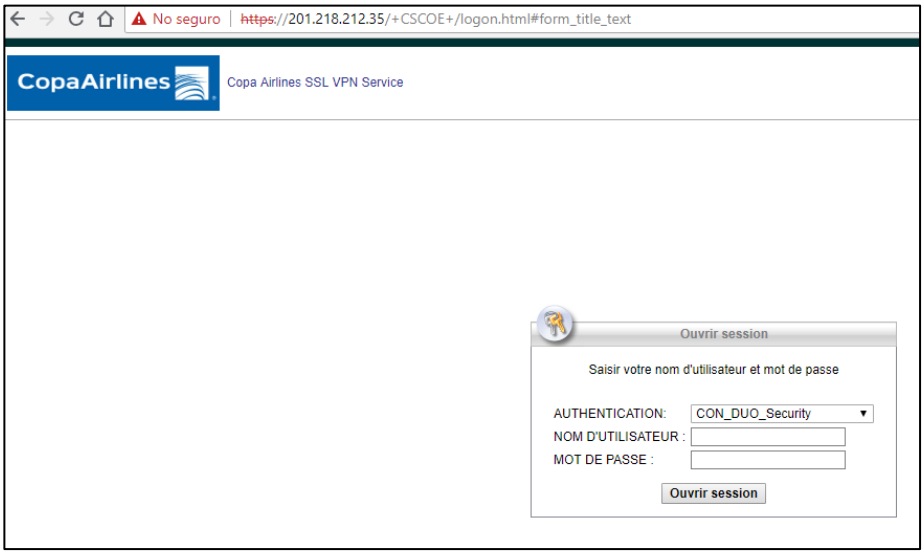
http://201.218.212.72/Homepage.aspx?lang=en

Esta dirección IP tiene las siguientes vulnerabilidades: CGI Generic SQL Injection (blind) esta vulnerabilidad require atención debido a severidad alta; ASP.NET DEBUG Method Enabled, Browsable Web Directories y F5 BIG-IP Cookie Remote Information Disclosure.



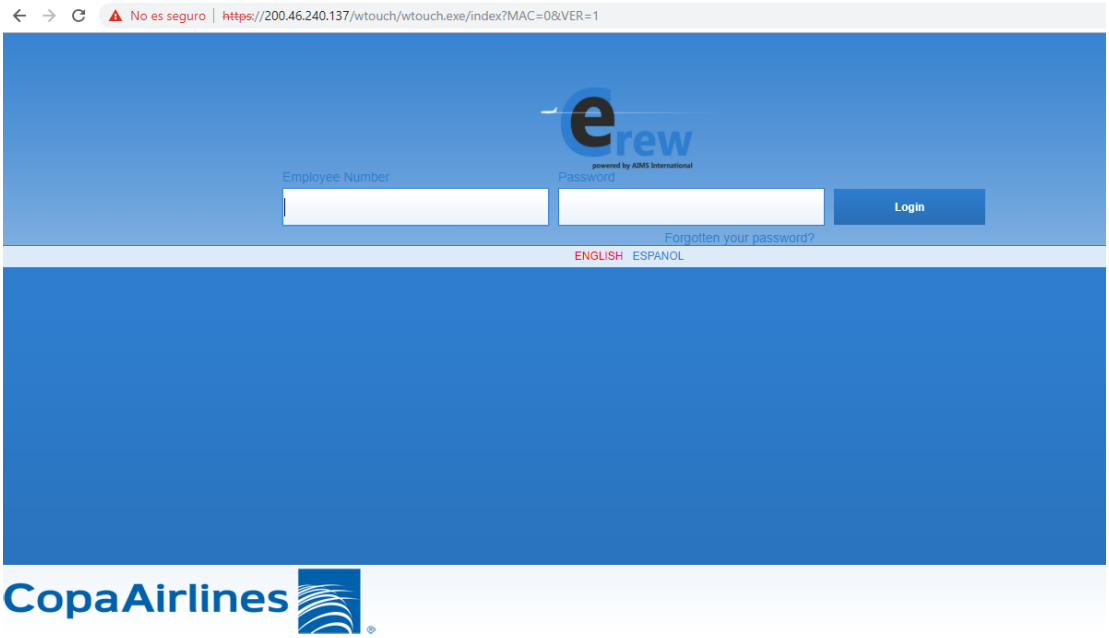
https://201.218.212.35/+CSCOE+/logon.html#form_title_text

Esta IP presenta la vulnerabilidad SSL / TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST). Esto se basa en el protocolo SSL, tal como se usa en ciertas configuraciones en Microsoft Windows y Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera y otros productos, cifra los datos utilizando el modo CBC con vectores de inicialización encadenados, lo que permite atacantes intermediarios obtener encabezados HTTP de texto plano a través de un ataque de límite elegido en bloques (BCBA) en una sesión HTTPS, junto con el código JavaScript que utiliza (1) el HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, conocidos como el ataque "BEAST".



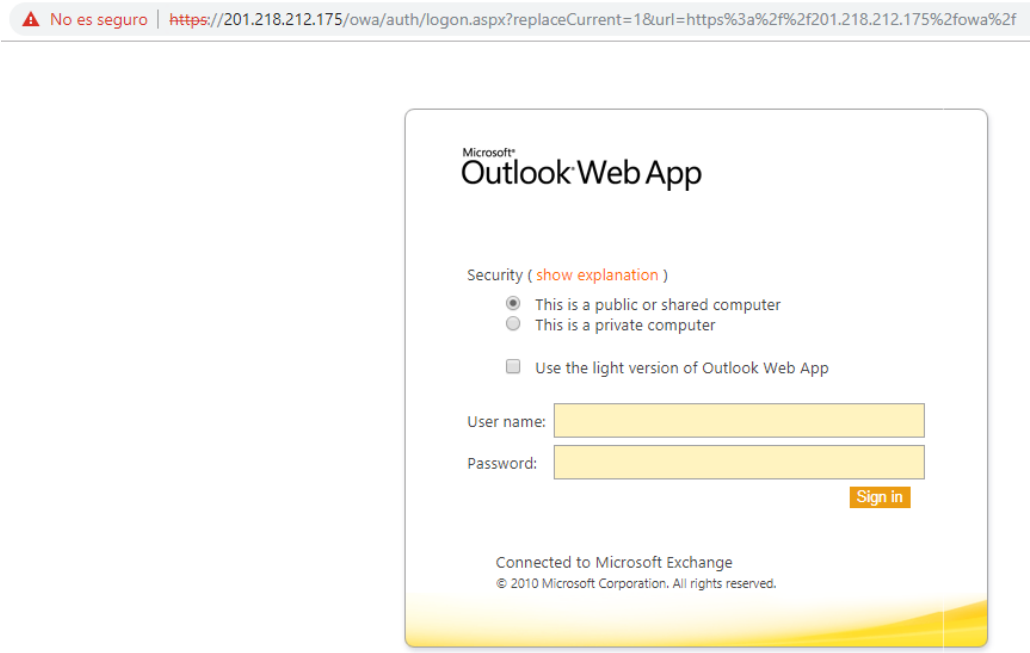
https://200.46.240.137/wtouch/wtouch.exe/index?MAC=0&VER=1

Esta dirección IP tiene las siguientes vulnerabilidades: F5 BIG-IP Cookie Remote Information Disclosure, SSL Medium Strength Cipher Suites Supported, SSL / TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST) y Web Application Potentially Vulnerable to Clickjacking.



https://201.218.212.175/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2f201.218.212.175%2fowa%2f

Esta dirección IP tiene las siguientes vulnerabilidades: Microsoft Exchange Client Access Server Information Disclosure y SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST).



Vulnerabilidades por severidad

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

Vulnerabilidades de severidad Crítica

MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code ExecutioMS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution

Descripción
La versión de Windows que se ejecuta en el host remoto se ve afectada por una condición de desbordamiento de entero en la pila de protocolo HTTP (HTTP.sys) debido a un análisis incorrecto de las solicitudes HTTP elaboradas.

Solución
Microsoft ha lanzado un conjunto de parches para Windows 7, 2008 R2, 8, 8.1, 2012 y 2012 R2.

Sistemas Afectados

443 / tcp / www	200.46.240.24, 200.46.240.230
80 / tcp / www	200.46.240.161

Microsoft IIS 6.0 Unsupported Version Detection

Descripción
De acuerdo con su número de versión, la instalación de Microsoft Internet Information Services (IIS) 6.0 en el host remoto ya no es compatible.

La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Solución
Actualice a una versión de Microsoft IIS que actualmente es compatible.

Sistemas Afectados
80 / tcp / www 200.46.240.139

Microsoft Windows Server 2003 Unsupported Installation Detection

Descripción
El host remoto ejecuta Microsoft Windows Server 2003. El soporte para este sistema operativo de Microsoft finalizó el 14 de julio de 2015.

La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad

Solución
Actualiza a una versión de Windows que actualmente es compatible.

Sistemas Afectados
N / A 200.46.240.139

Unix Operating System Unsupported Version Detection

Descripción
Según su número de versión , el sistema operativo Unix que se ejecuta en el host remoto ya no es compatible.

La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Solución
Actualice a una versión del sistema operativo Unix que actualmente es compatible.

Sistemas Afectados
N / A 200.46.240.166

Vulnerabilidades de alta severidad

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.

NIST ha determinado que SSL 3.0 ya no es aceptable para comunicaciones seguras. A partir de la fecha de ejecución encontrada en PCI DSS v3.1, cualquier versión de SSL no cumplirá con la definición de "criptografía fuerte" del SSC de PCI.

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
443 / tcp / www 200.46.240.179, 200.46.240.228, 200.46.240.196, 200.46.240.30, 200.46.240.82
443 / tcp / sip 200.46.240.195
5061 / tcp 200.46.240.195
443 / tcp / cisco-ssl-vpn-svr 201.218.212.9, 201.218.212.9, 201.218.212.10

Vulnerabilidades de severidad media

Web Application Potentially Vulnerable to Clickjacking

Descripción
El servidor web remoto no establece un encabezado de respuesta de Opciones de X-Frame o un encabezado de respuesta de antepasados de marco de Política de seguridad de contenido en todas las respuestas de contenido. Esto podría exponer al sitio a un ataque de clickjacking o reparación de UI, en el que un atacante puede engañar a un usuario para que haga clic en un área de la página vulnerable que sea

diferente de lo que el usuario percibe que es la página. Esto puede hacer que un usuario realice transacciones fraudulentas o malintencionadas.

Solución

Devuelva el encabezado HTTP de las Opciones de marco-X o Política de seguridad de contenido con la respuesta de la página.
Esto evita que el contenido de la página sea procesado por otro sitio cuando se usan las etiquetas de marco o iframe HTML

Sistemas Afectados

443 / tcp / www	200.46.240.137 200.46.240.137
80 / tcp / www	201.218.212.76

F5 BIG-IP Cookie Remote Information Disclosure

Descripción

El host remoto parece ser un equilibrador de carga F5 BIG-IP. El equilibrador de carga codifica la dirección IP del servidor web real en el que actúa en nombre de una cookie. Además, la información después de 'BIGipServer' es configurada por el usuario y puede ser el nombre lógico del dispositivo. Estos valores pueden revelar información confidencial, como nombres y direcciones IP internas.

Sistemas Afectados

443 / tcp / www	200.46.240.230,200.46.240.137, 201.218.212.72

Network Time Protocol (NTP) Mode 6 Scanner

Descripción

El servidor NTP remoto responde a las consultas del modo 6. Los dispositivos que responden a estas consultas tienen el potencial de ser utilizados en ataques de amplificación NTP. Un atacante remoto no autenticado podría potencialmente explotar esto, a través de una consulta de modo 6 especialmente diseñada, para provocar una condición de denegación de servicio reflejada.

Solución

Restringir las consultas del modo NTP 6.

Sistemas Afectados
123 / udp / ntp 200.46.241.161, 200.46.240.253, 200.46.240.254

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 mail2.copaair.com
443 / tcp / www 200.46.240.179 200.46.240.228
443 / tcp 200.46.240.196
443 / tcp / sip 200.46.240.195
5061 / tcp 200.46.240.195
443 / tcp / www 200.46.240.30 200.46.240.82
443 / tcp / cisco-ssl-vpn-svr 201.218.212.9 201.218.212.9 201.218.212.10 201.218.212.35 201.218.212.35 201.218.212.36
443 / tcp / www 200.46.240.24 200.46.240.137 200.46.240.137 200.46.240.230 ec2-52-86-152-128.compute-1.amazonaws.com ec2-52-86-152-128.compute-1.amazonaws.com

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.

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 mail2.copaair.com
443 / tcp / www 200.46.240.30 200.46.240.82 200.46.240.179 200.46.240.196
443 / tcp / sip 200.46.240.195
5061 / tcp 200.46.240.195
443 / tcp / cisco-ssl-vpn-svr 201.218.212.9 201.218.212.9 201.218.212.10

FTP Supports Cleartext Authentication

Descripción
El servidor FTP remoto permite que el nombre y la contraseña del usuario se transmitan en texto no cifrado, que puede ser interceptado por un rastreador de red o un ataque.

Solución
Cambie a SFTP (parte de la suite SSH) o FTPS (FTP sobre SSL / TLS). En este último caso, configure el servidor para que las conexiones de control estén encriptadas.

Sistemas Afectados
8021 / tcp / ftp 201.218.212.149
21 / tcp / ftp 200.46.240.33 201.218.212.122 201.218.212.149

Sección de Inteligencia del Servicio Managed Trusted Access (MSS-TAS)

El Managed Trusted Access Service (MSS-TAS) es un servicio holístico de seguridad que a) asegura que el acceso de los usuarios es confiable (usuario válido) y b) el dispositivo usado para autenticarse cumple con los estándares de seguridad de la organización. Esto se logra a través del servicio basado en la nube de GLESEC, que es parte de la plataforma TIP™.

Durante este periodo del mes Copa Airlines tuvo una tasa de acceso exitoso de 89.9%. Se registraron 649 autenticaciones denegadas: 552 autenticaciones denegadas por accidente debido a error del usuario, 48 autenticaciones denegadas voluntariamente por los usuarios en las que el usuario tomo acción para denegarlas en la notificación de Duo o Duo Mobile, 33 autenticaciones bloqueadas por políticas o reglas del sistema.

El número total de usuarios para el mes de octubre fue de 462.

El 87.2 % de los usuarios que utilizan la aplicación Duo, se autentifican con el método "Passcode", se recomienda utilizar el método de autentificación "Duo Push".

El país donde mayormente se reciben autentificaciones es Colombia con un 45.6 %, seguido de Panamá con 31% y Estados Unidos con 17%.

Sistemas Operativos de Dispositivos Móviles con vulnerabilidades (148 endpoints desactualizados):

- ✓ 25 IOS
- ✓ 123 Android

Endoints con Navegadores Desactualizados (20 endpoints desactualizados):

- ✓ 3 navegadores Firefox
- ✓ 2 internet Explorer
- ✓ 13 chrome
- ✓ 2 edge

Endpoints con complementos desactualizados (16 puntos finales desactualizados):

- ✓ 16 actualización de flash player

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

Tener sistemas operativos y/o aplicaciones desactualizadas; es decir, con actualizaciones del fabricante no aplicados al *endpoint* que resuelven vulnerabilidades de *Zero-Day* conocidos con lleva a un riesgo de seguridad crítico ya que deja al *endpoint* sin las protecciones necesarias para repeler o mitigar este ataque, exponiéndolo y a la red de Copa Airlines (en la mayoría de los casos) a ataques que pueden con llevar una disrupción temporal, total de parte o todo el sistema.
Se recomienda que se tomen las medidas necesarias e inmediatas para solventar esta situación.
Nuestro Servicios Profesionales en GLESEC (y haciendo uso de la hora de consultoría contratada por Uds.) puede ayudarlos a abordar y remediar estas situaciones.

Whole Compiled Recommendations

GLESEC recomienda a Copa Airlines abordar lo siguiente:

1. Tomar acciones inmediatas siguiendo las recomendaciones detalladas en este reporte.

2. Los certificados inválidos deben ser corregidos para que puedan ser confiables, aún más cuando el servicio es expuesto a internet.

3. Las cadenas de certificado SSL que contienen llaves RSA con menos de 2048 bits deben ser corregidos

1. Las suites de cifrado SSL con fortaleza media no se deben permitir para conexiones SSL. Para corregir esta vulnerabilidad se debe habilitar TLS 1.2 o superior y deshabilitar todas las versiones previas, que son vulnerables.

2. Recomendamos aplicar los parches más recientes para sus equipos finales, debido a que identificamos que el 75% de los dispositivos utilizados para el servicio TAS tienen software desactualizado instalado.

3. El equipo con IP 201.218.212.9, presenta una vulnerabilidad en el protocolo IKE (Internet Key Exchange) en modo agresivo con llave pre-compartida.

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