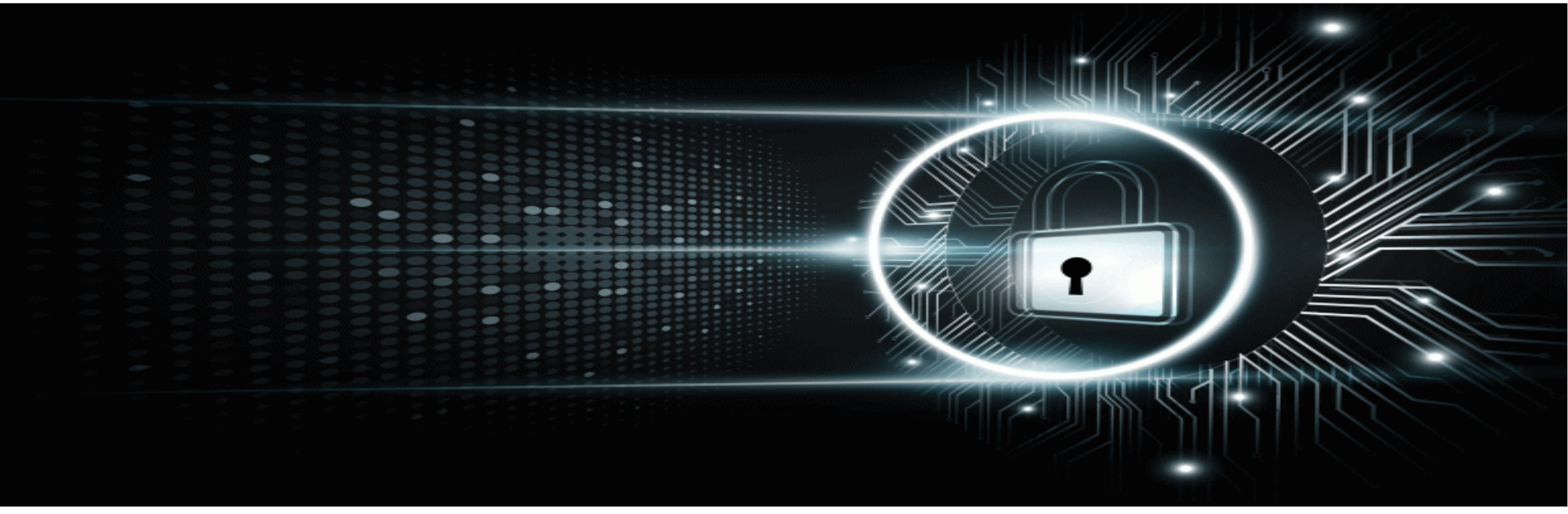
SERVICIO DE INTELIGENCIA SOBRE AMENAZAS [SIA]

AÑO 02 EDICIÓN 2.80



WWW.COREONEIT.COM
@COREONEIT

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

¿QUÉ ES EL SERVICIO DE INTELIGENCIA SOBRE AMENAZAS [SIA]?

Es una combinación de información de amenazas existentes en la red con el análisis e inteligencia del grupo de especialistas de CORE ONE IT, quienes analizan exhaustivamente todo tipo de amenazas informáticas y desarrollan una serie de recomendaciones adaptadas a cada tipo de cliente.

ALCANCE

Se personaliza de acuerdo al tipo de infraestructura y entorno de red del cliente basado en los tipos de dispositivos, modelos y fabricantes, con el fin de recibir solo información relevante y que pudiera afectar de manera directa o indirecta, la continuidad del negocio.

DEFINICIONES

•Riesgo: Probabilidad que una amenaza particular explote una vulnerabilidad particular de un sistema.

•Amenaza: Es la causa potencial de un incidente no deseado, el cual puede resultar en un daño a un sistema de información u organización.

•Ataque: Acción de tratar de traspasar controles de seguridad en un sistema. Un ataque puede ser activo, resultando en la modificación de datos, o pasivo, resultando en la divulgación de información. El hecho de que un ataque sea realizado no significa que será exitoso, el grado de éxito depende de la vulnerabilidad del sistema o actividad y de la eficiencia de las medidas existentes.

•Vulnerabilidad: Debilidad en los procedimientos de seguridad de un sistema, en el diseño del sistema, en la implementación, en los controles internos, y que puede ser explotada para violar la política de seguridad del sistema.

•API: Interfaz de Programación de Aplicaciones (Application Programming Interface, por sus siglas en inglés). Conjunto de subrutinas, funciones y procedimientos de una biblioteca para ser utilizado por otro software.

•Malware: también llamado badware, código maligno, software malicioso, software dañino o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

•Ransomware: Es un tipo especial de malware que amenaza con destruir los documentos y otros archivos de las víctimas.

•Troyano: Software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo.

•ISP: Proveedor de servicios de Internet (Internet Service Provider, por sus siglas en inglés).

•Keylogger: Software de vigilancia, el cual cuenta con la capacidad de grabar cada tecla pulsada en el sistema en un archivo, usualmente cifrado.

•BSOD: Blue Screen Of Death, “pantalla azul de la muerte”; se refiere a la pantalla mostrada por el sistema operativo de Windows cuando éste no puede recuperarse de un error del sistema.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

MICROSOFT PARCHEA EL PROBLEMA DE OUTLOOK 2010

¿Qué pasa en Redmond? Justo unas semanas después de publicar un parche que borraba los ficheros de los usuarios, Microsoft "arregló" Outlook 2010 con el denomiado November Patch Tuesday

El 13 de noviembre, Microsoft publicó una actualización de seguridad, KB4461529, que arreglaba cuatro vulnerabilidades de seguridad. Estos fallos podían permitir la ejecución de código remoto si un usuario abría un fichero comprometido de Office. KB4461529 solucionaba este problema para la versión .msi 64-bit de Outlook 2010 de la peor forma posible, impidiendo que el programa se ejecutase. Outlook se cerraba al ser abierto.

Microsoft avisó a los usuarios de no desinstalar el parche. En cambio, sugería que se utilizase Outlook Web Access hasta que el problema fuera solucionado. Mientras tanto crearon un segundo parche el 21 de noviembre. KB4461585 solucionará el problema, dijeron.

Este no era el primer problema con los parches de Outlook 2010 que los usuarios de Microsoft se encontraron este mes. El 6 de noviembre publicaron las actualizaciones KB2863821 y KB4461522, que solucionaban un problema con el calendario japonés relacionado con las nuevas "eras". Estos parches también hacían que, en algunos casos, Access se bloqueara al arrancar. Los eliminaron.

El calendario japonés heredó la idea de las eras del chino en el siglo VII. Las eras marcan el reinado de un emperador o cualquier otro acontecimiento importante. Solo existe una cada pocos años, por lo que muchos usuarios querían que sus calendarios pudieran ser programados de esta manera.

Microsoft había publicado parches relacionados con Office antes. Una actualización del año pasado provocaba que texto desapareciera de las tablas en Word cundiendo el pánico entre los usuarios. El mes anterior habían publicado otro parche que causaba el mismo problema. Microsoft finalmente consiguió arreglarlo en octubre con otro parche.

Estos problemas vienen precedidos de un preocupante mes de octubre para los usuarios de Microsoft, ya que algunos vieron como desaparecían ficheros y configuraciones delante de sus ojos justo después de instalar la actualización 1809 para Windows 10. Microsoft se vio obligado a suspender la actualización mientras no se solucionasen los problemas.

La preocupación sobre la calidad de las actualizaciones de Microsoft surgió anteriormente este año cuando Susan Bradley, Microsoft Most Valuable Professional, escribió una carta abierta a la empresa sobre este problema.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Mientras parece que Microsoft se ha precipitado un poco a la hora de publicar algunas actualizaciones, se ha demorado mucho con otras. En mayo se negaron a parchear un bug que hacía fallar a Windows después de ser informado del problema, alegando que para provocar el fallo era necesario una memoria USB por lo que no cumplía con los estándares.

Posiblemente el problema aquí es la falta de confianza. Microsoft quiere que la gente instale sus actualizaciones lo antes posible (especialmente las de seguridad) porque previene la aparición de infecciones de malware. La amarga experiencia con Conficker y Wannacry les ha enseñado que simplemente publicar parches no es suficiente, se tienen que instalar. Windows 10 se actualiza por defecto cuando puede. Pero cuantos más parches fallen, más usuarios los eliminaran.

Los usuarios empresariales pueden parar los parches cambiando la configuración del servidor de actualizaciones de Windows. Los usuarios de Windows 10 Pro y Enterprise pueden pausar las actualizaciones. Los usuarios de Windows 10 Home no tienen ninguna opción sobre las actualizaciones de Windows, según dice la empresa.

Los parches de Office no son obligatorios, pero existe la opción de instalarlos automáticamente. Sin embargo, dado los últimos problemas, cada vez son más los usuarios que desactivan las actualizaciones cuando pueden, lo que son malas noticias para el ecosistema de la ciberseguridad.

FUENTES:

Security, N. (2018). Microsoft parchea el problema de Outlook 2010. Retrieved from https://news.sophos.com/es-es/2018/11/28/microsoft-parchea-el-problema-de-outlook-2010/

HACKERS IRANÍS ACUSADOS POR EEUU DE LOS ATAQUES DE RANSOMWARE SAMSAM

El gobierno de Estados Unidos ha acusado a dos ciudadanos iraníes por haber lanzado uno de los mayores ciberataques utilizando el ransomware conocido como SamSam ocasionando más de 30 millones de dólares en pérdidas a las víctimas y permitiendo a los presuntos ciberatacantes cobrar más de 6,5 millones de dólares en pagos de rescate. La sofisticada forma de operar del ransomware, así como el número de víctimas y la cantidad de dinero recaudado por los ciberdelincuentes fueron desvelados por una investigación realizada por SophosLabs en agosto de este año.

Sophos ha estado rastreando a SamSam y otros ataques similares, y ha llegado a la conclusión de que los autores de SamSam han recaudado estos 6,5 millones de dólares en el transcurso de casi tres años. Los ciberdelincuentes usan una técnica de ataque dirigido controlada por un equipo cualificado que lo despliega durante la noche mientras las víctimas duermen, lo que indica que los cibercriminales realizan un reconocimiento de las víctimas y planifican cuidadosamente quién, qué, dónde y cuándo se producirán dichos ataques.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

En el análisis, Sophos ha descubierto que los ciberatacantes se dirigen a puntos de entrada débiles y fuerzan las contraseñas de RDP (Protocolo de escritorio remoto). Una vez dentro, se mueven lateralmente, trabajando paso a paso para robar las credenciales de administrador de dominio, manipular los controles internos, deshabilitar las copias de seguridad entre otras acciones, para instalar manualmente el ransomware. Cuando la mayoría de los administradores de TI se dan cuenta de lo que está sucediendo, el daño ya está hecho.

Basándose en la investigación realizada, Sophos sospechaba que se trataba de un pequeño grupo de personas por el grado de seguridad operativa que empleaban. Por ejemplo, no solían entrar a foros de la Deep Web para alardear de sus hazañas, como suelen hacer muchos aficionados. Además, se intuía que la lengua materna de los autores no era el inglés por la gramática y puntuación usada. A estas pistas se sumaba, las horas de trabajo de los ciberdelincuentes que coincidían con el huso horario de Teherán es GMT+3:30.

La investigación sobre SamSam y el Informe de Ciberamenazas 2019 realizado por Sophos explican detalladamente cómo se ha llevado a cabo este ataque. La técnica, táctica y procedimiento de los delincuentes eran únicos y empleaban algunas medidas de protección muy sofisticadas que iban evolucionando con el tiempo. Lamentablemente, esta nueva metodología de ciberataque ha inspirado a toda una nueva generación de ciberdelincuentes que están usando las mismas técnicas contra otras organizaciones grandes y medianas.
El hecho de haber identificado a los ciberdelincuentes y su nueva metodología demuestra que todo tipo de ciberactividad puede ser rastreada hasta hallar a los culpables y acusarlos por robar y extorsionar a personas inocentes.

FUENTES:

Security, N. (2018). Hackers iranís acusados por EEUU de los ataques de ransomware SamSam. Retrieved from https://news.sophos.com/es-es/2018/11/29/hackers-iranis-acusados-por-eeuu-de-los-ataques-de-ransomware-samsam/

LA MFA DE OFFICE 365 FALLA POR SEGUNDA VEZ EN UNA SEMANA

La autenticación de múltiples factores (MFA) de Microsoft para Office 365 y Azure Active Directory ha caído por segunda vez en una semana. La página de estado de servicio de Azure daba las malas noticias.

Entre las 14:25 UTC y las 17:08 UTC del 27 de noviembre de 2018, lo usuarios que usen la autenticación de múltiples factores (MFA) pueden haber experimentado problemas intermitentes al conectarse a los servicios de Azure, como Azure Active Directory, cuando se requería MFA.

Oficialmente, son solo tres tristes horas de intermitencias o fallo de la MFA, aunque no fue hasta las 18:53 UTC cuando la cuenta de Microsoft a través de Twitter tuvo la certeza de poder anunciar que el servicio volvía a funcionar con normalidad.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Déjà vu
Este problema es el último de una larga serie de meteduras de pata de Microsoft en las últimas semanas. La empresa acaba de publicar una explicación para un problema más serio y largo con la MFA que sufrió el 19 de noviembre el cual impidió a muchos usuarios poder usar Office 365 o Azure durante todo un día laboral, y en algunos casos, incluso más.
Esto incluía reconocimientos sinceros de lo que la empresa dijo que eran tres problemas raíz interconectados:
Bajo grandes cargas de tráfico, los servidores de Azure de comunicaciones front-end con los servicios de cache fallan (lo que es irónico, ya que están ahí para mejorar el rendimiento).
Esto causa una "competición" al procesar las respuestas de los servidores MFA backend, es decir se produce una especie de desincronización lo suficientemente importante para provocar que no se comuniquen correctamente.
Esto causa una sobrecarga en los servicios backend que hace que la MFA deje de funcionar.
Increíblemente (esta es la parte que más ha molestado a algunos usuarios) Microsoft no detectó nada de esto hasta que algunos usuarios se quejaran delo problemas con la MFA. ¿Por qué?
Vacíos entre la telemetría y el seguimiento de los servicios de MFA retrasaron la identificación y la solución de estas causas raíz que provocaron un tiempo tan largo de espera.
Microsoft explica como al intentar solucionar los problemas en las regiones APAC y EMEA intentando redirigir todo el tráfico MFA a los caches en EEUU también complicó la situación en ese país.
Microsoft ha prometido publicar otro informe sobre el segundo incidente.

FUENTES:

Security, N. (2018). La MFA de Office 365 falla por segunda vez en una semana. Retrieved from https://news.sophos.com/es-es/2018/11/30/la-mfa-de-office-365-falla-por-segunda-vez-en-una-semana/

VULNERABILIDAD DE DENEGACIÓN DE SERVICIO DE CISCO ADAPTIVE SECURITY APPLIANCE Y CISCO FIREPOWER THREAT DEFENSE SOFTWARE

VULNERABILIDAD DE INYECCIÓN DE COMANDOS EN EL SERVICIO DE ACTUALIZACIÓN DE LA APLICACIÓN CISCO WEBEX MEETINGS

Criticidad: *Alta*
Impacto: *Inyección de comandos*
Vulnerabilidad:
Ejecución: *Local*
Plataforma(s)
Afectada(s):
Esta vulnerabilidad afecta a todas las versiones de la aplicación Cisco Webex Meetings Desktop antes de la versión 33.6.4, ya las versiones de la herramienta de productividad Cisco Webex 32.6.0 y posteriores a la versión 33.0.6, cuando se ejecuta en un sistema de usuario final de Microsoft Windows.
Referencia: *CVE-2018-15442*
Descripción:
Una vulnerabilidad en el servicio de actualización de la aplicación Cisco Webex Meetings Desktop para Windows podría permitir a un atacante local autenticado ejecutar comandos arbitrarios como usuario privilegiado.

La vulnerabilidad se debe a una validación insuficiente de los parámetros proporcionados por el usuario. Un atacante podría explotar esta vulnerabilidad invocando el comando del servicio de actualización con un argumento elaborado. Un exploit podría permitir al atacante ejecutar comandos arbitrarios con privilegios de usuario del SISTEMA.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Si bien la métrica CVSS Attack Vector denota el requisito de que un atacante tenga acceso local, los administradores deben tener en cuenta que en las implementaciones de Active Directory, la vulnerabilidad podría explotarse de forma remota aprovechando las herramientas de administración remota del sistema operativo.

Cisco ha lanzado actualizaciones de software que abordan esta vulnerabilidad. No hay soluciones que aborden esta vulnerabilidad.

Después de que se informó a Cisco de un método de ataque adicional, se determinó que la solución anterior para esta vulnerabilidad era insuficiente. Se desarrolló una nueva solución y el aviso se actualizó el 27 de noviembre de 2018 para reflejar qué versiones de software incluyen la solución completa.

FUENTES:

Vulnerabilidad de inyección de comandos en el servicio de actualización de la aplicación Cisco Webex Meetings Desktop
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181024-webex-injection

VULNERABILIDAD DE INYECCIÓN SQL EN CISCO PRIME LICENSE MANAGER

Criticidad: *Crítica*
Impacto: *Acceso no autorizado*
Vulnerabilidad:
Ejecución: *Remota*
Plataforma(s) Afectada(s):
Esta vulnerabilidad afecta a Cisco Prime License Manager Releases 11.0.1 y posteriores. Se ven afectadas las implementaciones independientes de Cisco Prime License Manager y las implementaciones asociadas, donde Cisco Prime License Manager se instala automáticamente como parte de la instalación de Cisco Unified Communications Manager y Cisco Unity Connection.
Referencia: *CVE-2018-15441*
Descripción:
Una vulnerabilidad en el código de marco web de Cisco Prime License Manager (PLM) podría permitir que un atacante remoto no autenticado ejecutara consultas de SQL arbitrarias.

La vulnerabilidad se debe a la falta de validación adecuada de la entrada proporcionada por el usuario en las consultas SQL. Un atacante podría aprovechar esta vulnerabilidad enviando solicitudes HTTP POST creadas que contengan sentencias SQL maliciosas a una aplicación afectada. Una explotación exitosa podría permitir al atacante modificar y eliminar datos arbitrarios en la base de datos de PLM u obtener acceso de shell con los privilegios del usuario de Postgres.

Cisco ha lanzado actualizaciones de software que abordan esta vulnerabilidad. No hay soluciones que aborden esta vulnerabilidad.

FUENTES:

Vulnerabilidad de inyección SQL en Cisco Prime License Manager
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181128-plm-sql-inject

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

VULNERABILIDAD DE EJECUCIÓN REMOTA DE CÓDIGO EN LA BIBLIOTECA DE APACHE STRUTS COMMONS FILEUPLOAD QUE AFECTA A LOS PRODUCTOS DE CISCO

Criticidad: *Crítica*
Impacto: *Acceso no autorizado*
Vulnerabilidad:
Ejecución: *Local*
Plataforma(s)
Afectada(s):
La siguiente tabla enumera los productos y servicios de Cisco que se ven afectados por la vulnerabilidad que se describe en este aviso. Las fechas de disponibilidad del software en la columna Disponibilidad de la versión fija son estimaciones y la disponibilidad real del software puede diferir de las fechas que se proporcionan en la siguiente tabla.

Producto	ID de error de Cisco	Disponibilidad de liberación fija
Colaboración y redes sociales.		
Cisco SocialMiner	CSCvn22343	Archivo de parche disponible para 11.5 / 11.6 en diciembre de 2018 12.0.1 (enero de 2019)
Cisco Webex Meetings Server	CSCvn18895	Parche de seguridad 2.8MR3 1 (diciembre de 2018) Parche de seguridad 3.0MR2 2 (diciembre de 2018)
Clientes finales y software cliente		
Cisco Webex Management - Panel de control SuperAdmin	CSCvn18901	T33.7.2 (Dic 2018)
Enrutamiento y conmutación - Empresa y proveedor de servicios		
Director de niebla de Cisco IOx	CSCvn19758	1.8 (febrero de 2019)
Cisco IoT Field Network Director (anteriormente Cisco Connected Grid Network Management System)	CSCvn20600	4.3.2 (dic. 2018)
Dispositivos de voz y comunicaciones unificadas.		
Servicio de emergencia de Cisco	CSCvn18956	Archivo de parche disponible para 11.5.1 / 12.0.1 hasta diciembre de 2018 12.5.1 (enero de 2018)
Cisco Enterprise Chat y correo electrónico	CSCvn18957	11.6 ES6 (enero de 2019) 12.0.1 (enero de 2019)
Cisco Finesse	CSCvn22344	Archivo de parche disponible para 11.6 hasta diciembre de 2018 12.0.1 (enero de 2019)
Cisco Hosted Collaboration Mediation Fulfillment	CSCvn18961	11.5 (4) (Disponible)
Solución de colaboración alojada de Cisco para Contact Center	CSCvn18962	12.0.1 (enero 2019)
Cisco MediaSense	CSCvn22346	No hay solución planeada
Cisco Unified Communications Manager IM y servicio de presencia (anteriormente CUPS)	CSCvn18959	Archivo de parche disponible para 10.5.2 / 11.5.1 / 12.0.1 en diciembre de 2018 12.5.1 (enero de 2018)
Cisco Unified Communications Manager	CSCvn18952	Archivo de parche disponible para 10.5.2 / 11.5.1 / 12.0.1 en diciembre de 2018 12.5.1 (enero de 2018)
Cisco Unified Contact Center Enterprise	CSCvn18888	12.0.1 (enero 2019)
Cisco Unified Contact Center Express	CSCvn18955	Archivo de parche disponible para 11.5 / 11.6 en diciembre de 2018 12.0.1 (enero de 2019)
Cisco Unified E-Mail Interaction Manager	CSCvn18958	No hay solución planeada

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Cisco Unified Intelligence Center	CSCvn18887	Archivo de parche disponible para 11.5 / 11.6 en diciembre de 2018 12.0.1 (enero de 2019)
Empresa de gestión de contactos inteligentes unificada de Cisco	CSCvn18888	12.0.1 (enero 2019)
Cisco Unified Web Interaction Manager	CSCvn18958	No hay solución planeada
Cisco Unity Connection	CSCvn18954	Archivo de parche disponible para 10.5.2 / 11.5.1 / 12.0.1 en diciembre de 2018 12.5.1 (enero de 2018)
Cisco Virtualized Voice Browser	CSCvn18963	Archivo de parche disponible para 11.5 / 11.6 en diciembre de 2018 12.0.1 (enero de 2019)
Dispositivos de video, transmisión, telepresencia y transcodificación		
Suite de distribución de video de Cisco para transmisión de Internet (VDS-IS)	CSCvn18928	Archivo de parche disponible para diciembre de 2018
Inalámbrico		
Motor de servicios de movilidad de Cisco	CSCvn22305	Archivo de parche disponible para diciembre de 2018
Sistema de gestión de Cisco Universal Small Cell RAN (USC RMS)	CSCvn18939	No hay solución planeada
Servicios alojados en la nube de Cisco		
Cisco Prime Gestión de cambios y configuración de red	CSCvn19865	3.6.1 (diciembre de 2018) 3.7 (marzo de 2019)
Espacios conectados inteligentes de Cisco	CSCvn22310	Archivo de parche disponible para diciembre de 2018
Cisco Smart Net Total Care - Contratos Controlador de procesos del sistema de información	CSCvn18884	4.3.6 (dic. 2018)
Centros Cisco Webex: centro de reuniones, centro de capacitación, centro de eventos, centro de soporte	CSCvn24113	T33.7.2 (diciembre de 2018) T32.20.2 (diciembre de 2018)
Reuniones de Cisco Webex	CSCvn18908	Cisco actualizará los sistemas afectados en diciembre de 2018

Referencia: CVE-2016-1000031
Descripción:
El equipo de Apache Struts lanzó un anuncio de seguridad instando a una actualización de la biblioteca Commons FileUpload a la versión 1.3.3 en sistemas que utilizan Struts 2.3.36 o versiones anteriores. Los sistemas que usan versiones anteriores de esta biblioteca pueden estar expuestos a ataques que podrían permitir la ejecución de código arbitrario o modificaciones de archivos en el sistema. El problema se debe a una vulnerabilidad reportada previamente de la biblioteca FileSpload de Apache Commons, asignada a CVE-2016-1000031.

La vulnerabilidad se debe a la validación insuficiente de la entrada proporcionada por el usuario por el software afectado. Un atacante podría aprovechar esta vulnerabilidad al enviar datos diseñados a un sistema afectado. Una explotación exitosa podría permitir al atacante ejecutar código arbitrario o manipular archivos en el sistema de destino.

Este aviso se actualizará a medida que haya información adicional disponible.

FUENTES:

Vulnerabilidad de ejecución remota de código en la biblioteca de Apache Struts Commons FileUpload que afecta a los productos de Cisco
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181107-struts-commons-fileupload

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

F5
DETALLES DE VULNERABILIDAD: CVE-2018-15310

Una vulnerabilidad en el acceso 11.5.1-11.5.7, 11.6.0-11.6.3 y 12.1.0-12.1.3 del portal de BIG-IP APM revela la versión del software BIG-IP en las páginas reescritas.
Puntuaciones de CVSS y tipos de vulnerabilidad:
Puntuación de CVSS 4.0
Confidencialidad Impacto Parcial (Existe una divulgación informativa considerable).
Impacto en la integridad Ninguno (No hay impacto en la integridad del sistema)
Disponibilidad Impacto Ninguna (No hay ningún impacto en la disponibilidad del sistema).
Complejidad de acceso baja (No existen condiciones de acceso especializadas o circunstancias atenuantes. Se requiere muy poco conocimiento o habilidad para explotar).
Autenticación de un solo sistema (la vulnerabilidad requiere que un atacante inicie sesión en el sistema (como en una línea de comandos o mediante una sesión de escritorio o una interfaz web).)
Acceso ganado Ninguno
Tipo (s) de vulnerabilidad ID CWE 200

Productos afectados por CVE-2018-15310

- ***Application F5 Big-ip Access Policy Manager 11.5.1***
- ***Application F5 Big-ip Access Policy Manager 11.5.2***
- ***Application F5 Big-ip Access Policy Manager 11.5.3***
- ***Application F5 Big-ip Access Policy Manager 11.5.4***
- ***Application F5 Big-ip Access Policy Manager 11.5.5***
- ***Application F5 Big-ip Access Policy Manager 11.5.6***
- ***Application F5 Big-ip Access Policy Manager 11.5.7***
- ***Application F5 Big-ip Access Policy Manager 11.6.0***
- ***Application F5 Big-ip Access Policy Manager 11.6.1***
- ***Application F5 Big-ip Access Policy Manager 11.6.2***
- ***Application F5 Big-ip Access Policy Manager 11.6.3***
- ***Application F5 Big-ip Access Policy Manager 12.1.0***
- ***Application F5 Big-ip Access Policy Manager 12.1.1***
- ***Application F5 Big-ip Access Policy Manager 12.1.2***
- ***Application F5 Big-ip Access Policy Manager 12.1.3***

Número de versiones afectadas por producto

Vendor	Product	Vulnerable Versions
F5	Big-ip Access Policy Manager	15

FUENTES:

Referencias para CVE-2018-15310
https://support.f5.com/csp/article/K40625021
https://www.cvedetails.com/cve/CVE-2018-15310/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

F5

DETALLES DE VULNERABILIDAD: CVE-2018-15311

Cuando F5 BIG-IP 13.0.0-13.1.0.5, 12.1.0-12.1.3.5, 11.6.0-11.6.3.2, o 11.5.1-11.5.6 está procesando tráfico TCP especialmente diseñado con la descarga de recepción grande (LRO) característica habilitada, TMM puede fallar, lo que lleva a un evento de failover. Esta vulnerabilidad no está expuesta a menos que la LRO esté habilitada, por lo que la mayoría de los clientes afectados estarán en 13.1.x. LRO ha estado disponible desde 11.4.0, pero no está habilitado por defecto hasta 13.1.0.

Puntuaciones de CVSS y tipos de vulnerabilidad:
Puntuación VSS 4.3
Confidencialidad Impacto Ninguna (No hay ningún impacto en la confidencialidad del sistema).
Impacto en la integridad Ninguno (No hay impacto en la integridad del sistema)
Disponibilidad de impacto parcial (Hay un rendimiento reducido o interrupciones en la disponibilidad de recursos).
Medio de complejidad de acceso (Las condiciones de acceso son algo especializadas. Algunas condiciones previas deben ser satistificadas para explotar)
No se requiere autenticación (No se requiere autenticación para explotar la vulnerabilidad).
Acceso ganado Ninguno
Tipo (s) de vulnerabilidad ID CWE 399

Productos afectados por CVE-2018-15311

- *Product Type Vendor Product Version*
- *Application F5 Big-ip Access Policy Manager 11.5.1*
- *Application F5 Big-ip Access Policy Manager 11.5.2*
- *Application F5 Big-ip Access Policy Manager 11.5.3*
- *Application F5 Big-ip Access Policy Manager 11.5.4*
- *Application F5 Big-ip Access Policy Manager 11.5.5*
- *Application F5 Big-ip Access Policy Manager 11.5.6*
- *Application F5 Big-ip Access Policy Manager 11.6.1*
- *Application F5 Big-ip Access Policy Manager 11.6.2*
- *Application F5 Big-ip Access Policy Manager 11.6.3*
- *Application F5 Big-ip Access Policy Manager 12.1.1*
- *Application F5 Big-ip Access Policy Manager 12.1.2*
- *Application F5 Big-ip Access Policy Manager 12.1.3*
- *Application F5 Big-ip Access Policy Manager 12.1.3.1*
- *Application F5 Big-ip Access Policy Manager 12.1.3.2*
- *Application F5 Big-ip Access Policy Manager 12.1.3.3*
- *Application F5 Big-ip Access Policy Manager 12.1.3.4*
- *Application F5 Big-ip Access Policy Manager 12.1.3.5*
- *Application F5 Big-ip Access Policy Manager 13.0.1*
- *Application F5 Big-ip Access Policy Manager 13.1.0*
- *Application F5 Big-ip Access Policy Manager 13.1.0.1*
- *Application F5 Big-ip Access Policy Manager 13.1.0.2*
- *Application F5 Big-ip Access Policy Manager 13.1.0.3*
- *Application F5 Big-ip Access Policy Manager 13.1.0.4*
- *Application F5 Big-ip Access Policy Manager 13.1.0.5*
- *Application F5 Big-ip Advanced Firewall Manager 11.5.1*
- *Application F5 Big-ip Advanced Firewall Manager 11.5.2*
- *Application F5 Big-ip Advanced Firewall Manager 11.5.3*
- *Application F5 Big-ip Advanced Firewall Manager 11.5.4*
- *Application F5 Big-ip Advanced Firewall Manager 11.5.5*
- *Application F5 Big-ip Advanced Firewall Manager 11.5.6*
- *Application F5 Big-ip Advanced Firewall Manager 11.6.1*
- *Application F5 Big-ip Advanced Firewall Manager 11.6.2*
- *Application F5 Big-ip Advanced Firewall Manager 11.6.3*
- *Application F5 Big-ip Advanced Firewall Manager 12.1.1*
- *Application F5 Big-ip Advanced Firewall Manager 12.1.2*

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

- *Application F5 Big-ip Advanced Firewall Manager 12.1.3*
- *Application F5 Big-ip Advanced Firewall Manager 13.0.1*
- *Application F5 Big-ip Advanced Firewall Manager 13.1.0*
- *Application F5 Big-ip Analytics 11.5.1*
- *Application F5 Big-ip Analytics 11.5.2*
- *Application F5 Big-ip Analytics 11.5.3*
- *Application F5 Big-ip Analytics 11.5.4*
- *Application F5 Big-ip Analytics 11.5.5*
- *Application F5 Big-ip Analytics 11.5.6*
- *Application F5 Big-ip Analytics 11.6.1*
- *Application F5 Big-ip Analytics 11.6.2*
- *Application F5 Big-ip Analytics 11.6.3*
- *Application F5 Big-ip Analytics 12.1.1*
- *Application F5 Big-ip Analytics 12.1.2*
- *Application F5 Big-ip Analytics 12.1.3*
- *Application F5 Big-ip Analytics 13.0.1*
- *Application F5 Big-ip Analytics 13.1.0*
- *Application F5 Big-ip Application Acceleration Manager 11.5.1*
- *Application F5 Big-ip Application Acceleration Manager 11.5.2*
- *Application F5 Big-ip Application Acceleration Manager 11.5.3*
- *Application F5 Big-ip Application Acceleration Manager 11.5.4*
- *Application F5 Big-ip Application Acceleration Manager 11.5.5*
- *Application F5 Big-ip Application Acceleration Manager 11.5.6*
- *Application F5 Big-ip Application Acceleration Manager 11.6.1*
- *Application F5 Big-ip Application Acceleration Manager 11.6.2*
- *Application F5 Big-ip Application Acceleration Manager 11.6.3*
- *Application F5 Big-ip Application Acceleration Manager 12.1.1*
- *Application F5 Big-ip Application Acceleration Manager 12.1.2*
- *Application F5 Big-ip Application Acceleration Manager 12.1.3*
- *Application F5 Big-ip Application Acceleration Manager 13.0.1*

- *Application F5 Big-ip Advanced Firewall Manager 12.1.3*
- *Application F5 Big-ip Advanced Firewall Manager 13.0.1*
- *Application F5 Big-ip Advanced Firewall Manager 13.1.0*
- *Application F5 Big-ip Analytics 11.5.1*
- *Application F5 Big-ip Analytics 11.5.2*
- *Application F5 Big-ip Analytics 11.5.3*
- *Application F5 Big-ip Analytics 11.5.4*
- *Application F5 Big-ip Analytics 11.5.5*
- *Application F5 Big-ip Analytics 11.5.6*
- *Application F5 Big-ip Analytics 11.6.1*
- *Application F5 Big-ip Application Security Manager 11.5.2*
- *Application F5 Big-ip Application Security Manager 11.5.3*
- *Application F5 Big-ip Application Security Manager 11.5.4*
- *Application F5 Big-ip Application Security Manager 11.5.5*
- *Application F5 Big-ip Application Security Manager 11.5.6*
- *Application F5 Big-ip Application Security Manager 11.6.1*
- *Application F5 Big-ip Application Security Manager 11.6.2*
- *Application F5 Big-ip Application Security Manager 11.6.3*
- *Application F5 Big-ip Application Security Manager 12.1.1*
- *Application F5 Big-ip Application Security Manager 12.1.2*
- *Application F5 Big-ip Application Security Manager 12.1.3*
- *Application F5 Big-ip Application Security Manager 13.0.1*
- *Application F5 Big-ip Application Security Manager 13.1.0*
- *Application F5 Big-ip Domain Name System 11.5.1*
- *Application F5 Big-ip Domain Name System 11.5.2*
- *Application F5 Big-ip Domain Name System 11.5.3*
- *Application F5 Big-ip Domain Name System 11.5.4*
- *Application F5 Big-ip Domain Name System 11.5.5*
- *Application F5 Big-ip Domain Name System 11.5.6*
- *Application F5 Big-ip Domain Name System 11.6.1*

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

- *Application F5 Big-ip Domain Name System 11.6.2*
- *Application F5 Big-ip Domain Name System 11.6.3*
- *Application F5 Big-ip Domain Name System 12.1.1*
- *Application F5 Big-ip Domain Name System 12.1.2*
- *Application F5 Big-ip Domain Name System 12.1.3*
- *Application F5 Big-ip Domain Name System 13.0.1*
- *Application F5 Big-ip Domain Name System 13.1.0*
- *Application F5 Big-ip Edge Gateway 11.5.1*
- *Application F5 Big-ip Edge Gateway 11.5.2*
- *Application F5 Big-ip Edge Gateway 11.5.3*
- *Application F5 Big-ip Edge Gateway 11.5.4*
- *Application F5 Big-ip Edge Gateway 11.5.5*
- *Application F5 Big-ip Edge Gateway 11.5.6*
- *Application F5 Big-ip Edge Gateway 11.6.1*
- *Application F5 Big-ip Edge Gateway 11.6.2*
- *Application F5 Big-ip Edge Gateway 11.6.3*
- *Application F5 Big-ip Edge Gateway 12.1.1*
- *Application F5 Big-ip Edge Gateway 12.1.2*
- *Application F5 Big-ip Edge Gateway 12.1.3*
- *Application F5 Big-ip Edge Gateway 13.0.1*
- *Application F5 Big-ip Edge Gateway 13.1.0*
- *Application F5 Big-ip Fraud Protection Service 11.5.1*
- *Application F5 Big-ip Fraud Protection Service 11.5.2*
- *Application F5 Big-ip Fraud Protection Service 11.5.3*
- *Application F5 Big-ip Fraud Protection Service 11.5.4*
- *Application F5 Big-ip Fraud Protection Service 11.5.5*
- *Application F5 Big-ip Fraud Protection Service 11.5.6*
- *Application F5 Big-ip Fraud Protection Service 11.6.1*
- *Application F5 Big-ip Fraud Protection Service 11.6.2*
- *Application F5 Big-ip Fraud Protection Service 11.6.3*

- *Application F5 Big-ip Fraud Protection Service 12.1.1*
- *Application F5 Big-ip Fraud Protection Service 12.1.2*
- *Application F5 Big-ip Fraud Protection Service 12.1.3*
- *Application F5 Big-ip Fraud Protection Service 13.0.1*
- *Application F5 Big-ip Fraud Protection Service 13.1.0*
- *Application F5 Big-ip Global Traffic Manager 11.5.1*
- *Application F5 Big-ip Global Traffic Manager 11.5.2*
- *Application F5 Big-ip Global Traffic Manager 11.5.3*
- *Application F5 Big-ip Global Traffic Manager 11.5.4*
- *Application F5 Big-ip Global Traffic Manager 11.5.5*
- *Application F5 Big-ip Global Traffic Manager 11.5.6*
- *Application F5 Big-ip Global Traffic Manager 11.6.1*
- *Application F5 Big-ip Global Traffic Manager 11.6.2*
- *Application F5 Big-ip Global Traffic Manager 11.6.3*
- *Application F5 Big-ip Global Traffic Manager 12.1.1*
- *Application F5 Big-ip Global Traffic Manager 12.1.2*
- *Application F5 Big-ip Global Traffic Manager 12.1.3*
- *Application F5 Big-ip Global Traffic Manager 13.0.1*
- *Application F5 Big-ip Global Traffic Manager 13.1.0*
- *Application F5 Big-ip Link Controller 11.5.1*
- *Application F5 Big-ip Link Controller 11.5.2*
- *Application F5 Big-ip Link Controller 11.5.3*
- *Application F5 Big-ip Link Controller 11.5.4*
- *Application F5 Big-ip Link Controller 11.5.5*
- *Application F5 Big-ip Link Controller 11.5.6*
- *Application F5 Big-ip Link Controller 11.6.1*
- *Application F5 Big-ip Link Controller 11.6.2*
- *Application F5 Big-ip Link Controller 11.6.3*
- *Application F5 Big-ip Link Controller 12.1.1*
- *Application F5 Big-ip Link Controller 12.1.2*
- *Application F5 Big-ip Link Controller 12.1.3*

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

- *Application F5 Big-ip Link Controller 13.0.1*
- *Application F5 Big-ip Link Controller 13.1.0*
- *Application F5 Big-ip Local Traffic Manager 11.5.1*
- *Application F5 Big-ip Local Traffic Manager 11.5.2*
- *Application F5 Big-ip Local Traffic Manager 11.5.3*
- *Application F5 Big-ip Local Traffic Manager 11.5.4*
- *Application F5 Big-ip Local Traffic Manager 11.5.5*
- *Application F5 Big-ip Local Traffic Manager 11.5.6*
- *Application F5 Big-ip Local Traffic Manager 11.6.1*
- *Application F5 Big-ip Local Traffic Manager 11.6.2*
- *Application F5 Big-ip Local Traffic Manager 11.6.3*
- *Application F5 Big-ip Local Traffic Manager 12.1.1*
- *Application F5 Big-ip Local Traffic Manager 12.1.2*
- *Application F5 Big-ip Local Traffic Manager 12.1.3*
- *Application F5 Big-ip Local Traffic Manager 13.0.1*
- *Application F5 Big-ip Local Traffic Manager 13.1.0*
- *Application F5 Big-ip Policy Enforcement Manager 11.5.1*
- *Application F5 Big-ip Policy Enforcement Manager 11.5.2*
- *Application F5 Big-ip Policy Enforcement Manager 11.5.3*
- *Application F5 Big-ip Policy Enforcement Manager 11.5.4*
- *Application F5 Big-ip Policy Enforcement Manager 11.5.5*
- *Application F5 Big-ip Policy Enforcement Manager 11.5.6*
- *Application F5 Big-ip Policy Enforcement Manager 11.6.1*
- *Application F5 Big-ip Policy Enforcement Manager 11.6.2*
- *Application F5 Big-ip Policy Enforcement Manager 11.6.3*
- *Application F5 Big-ip Policy Enforcement Manager 12.1.1*
- *Application F5 Big-ip Policy Enforcement Manager 12.1.2*
- *Application F5 Big-ip Policy Enforcement Manager 12.1.3*
- *Application F5 Big-ip Policy Enforcement Manager 13.0.1*
- *Application F5 Big-ip Policy Enforcement Manager 13.1.0*
- *Application F5 Big-ip Webaccelerator 11.5.1*
- *Application F5 Big-ip Webaccelerator 11.5.2*
- *Application F5 Big-ip Webaccelerator 11.5.3*
- *Application F5 Big-ip Webaccelerator 11.5.4*
- *Application F5 Big-ip Webaccelerator 11.5.5*
- *Application F5 Big-ip Webaccelerator 11.5.6*
- *Application F5 Big-ip Webaccelerator 11.6.1*
- *Application F5 Big-ip Webaccelerator 11.6.2*
- *Application F5 Big-ip Webaccelerator 11.6.3*
- *Application F5 Big-ip Webaccelerator 12.1.1*
- *Application F5 Big-ip Webaccelerator 12.1.2*
- *Application F5 Big-ip Webaccelerator 12.1.3*
- *Application F5 Big-ip Webaccelerator 13.0.1*
- *Application F5 Big-ip Webaccelerator 13.1.0*

----Espacio Intencionalmente en blanco-----

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Número de versiones afectadas por producto

Vendor	Product	Vulnerable Versions
F5	Big-ip Access Policy Manager	24
F5	Big-ip Advanced Firewall Manager	14
F5	Big-ip Analytics	14
F5	Big-ip Application Acceleration Manager	14
F5	Big-ip Application Security Manager	14
F5	Big-ip Domain Name System	14
F5	Big-ip Edge Gateway	14
F5	Big-ip Fraud Protection Service	14
F5	Big-ip Global Traffic Manager	14
F5	Big-ip Link Controller	14
F5	Big-ip Local Traffic Manager	14
F5	Big-ip Policy Enforcement Manager	14
F5	Big-ip Webaccelerator	14

FUENTES:

Referencias para CVE-2018-15310
https://support.f5.com/csp/article/K40625021
https://www.cvedetails.com/cve/CVE-2018-15310/