SERVICIO DE INTELIGENCIA SOBRE AMENAZAS [SIA]

AÑO 01 EDICIÓN 2.93

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"

CRIPTOMINEROS DE MONERO SECUESTRAN CIENTOS DE ALOJAMIENTOS WEB DOCKER SIN ACTUALIZAR

Una vulnerabilidad recientemente divulgada en la plataforma de contenerización Docker está siendo explotada activamente por ciberdelincuentes para minar la criptomoneda Monero (XMR) en cientos de servidores.
La empresa de seguridad Imperva usó Shodan para encontrar puertos abiertos ejecutando Docker, encontrando 3.822 en los que la API de la plataforma estaba expuesta públicamente.
De estos, unos 400 tenía direcciones IP en los puertos 2735/2736, los puertos en escucha de la API, descubriendo que la mayoría de ellos estaban realizando labores de criptominería, con servidores de producción MySQL y Apache legítimos en menor número.
Usados para configurar los contenedores, los puertos de la API de Docker no deberían ser accesibles externamente. Combinado con CVE-2019-5736, una vulnerabilidad crítica de acceso raíz en tiempo de ejecución del contenedor por defecto, runC, podría fácilmente comprometer completamente el equipo.

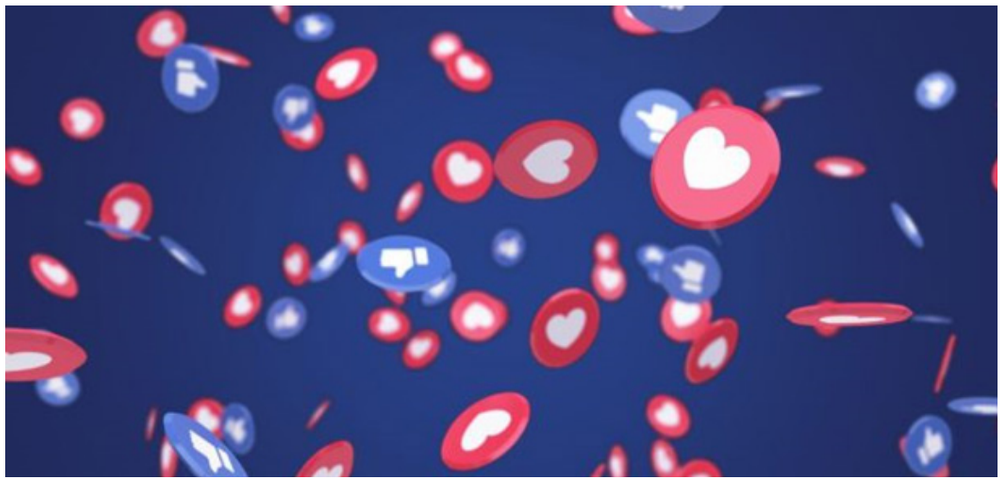
Aunque la criptominería suene muy mal, los investigadores explicaron que los atacantes podrían haber realizado acciones mucho peores en los alojamientos Docker, incluyendo robar credenciales para atacar la red interna, alojar campañas de phishing y malware o crear botnets.
Las posibilidades para los atacantes tras generar contenedores en un alojamiento Docker comprometido no tienen límite.
Sin mencionar que estos alojamientos todavía están minando activamente Monero para beneficio de los criminales.
Las transacciones de Monero están ofuscadas, por lo que es casi imposible encontrar la fuente, cantidad o destino de una transacción.
¿Qué hacer?
El problema es que cientos de servidores Docker ya están infectados y otros muchos lo estarán. Obviamente, si la vulnerabilidad en runC está siendo activamente explotada, significa que los administradores no la han parcheado. Dado la seriedad del asunto, es sorprendente.
Actualizar Docker a la versión v18.09.2 o posteriores debería solucionar la vulnerabilidad aunque aún es importante que se ha implementado de forma segura en primer lugar (Imperva ha encontrado credenciales almacenadas sin seguridad como variables de entorno, por ejemplo).
El pasado junio, webs que aún utilizaban el CMS Drupal fueron comprometidas por el ataque de criptominería de Monero "Drupalgeddon 2" meses después de que la vulnerabilidad CVE-2018-7600 fuera solucionada.

FUENTE:

Naked Security. (2019, 8 marzo). Criptomineros de Monero secuestran cientos de alojamientos web Docker sin actualizar. Recuperado 10 marzo, 2019, de https://news.sophos.com/es-es/2019/03/08/criptomineros-de-monero-secuestran-cientos-de-alojamientos-web-docker-sin-actualizar/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

¿SE ESTÁ TRABAJANDO EN UNA FACEBOOK-COIN?



Facebook, Signal y Telegram están planeando crear criptomonedas. Pero ¿por qué ahora? Y ¿tendrán éxito?
El New York Times ha publicado un artículo sobre los planes de estas tres empresas sobre las criptomonedas, citando informes en los que se muestra que están avanzados. Los planes de Facebook son los más secretos.
Mark Zuckerberg ha mostrado públicamente su interés en criptomonedas al menos desde enero de 2018, cuando publicó su declaración de objetivos anual.
En mayo de ese año, nombró a David Marcus, anteriormente responsable de la app Messenger, para dirigir el equipo de la empresa para criptomonedas. Marcus tiene experiencia en ese ámbito, habiendo sido el presidente de PayPal y durante un tiempo como miembro del consejo de administración de la empresa de pagos en criptomonedas Coinbase. Dimitió de ese puesto tres meses después de aceptar el liderazgo en blockchain de Facebook.

Bloomberg informó en diciembre que Facebook estaba trabajando en una moneda estable (stablecoin), que es una criptomoneda que está vinculada a un valor subyacente como puede ser el dólar americano. Los stablecoins son menos parecidos a activos negociables que pueden multiplicar su precio y más a una típica moneda usada para las transacciones de todos los días. Esta criptomoneda podría permitir transferir dinero por WhatsApp, centrándose primero en el mercado de remesas de India.
Centrarse en India ayudaría a este gigante de las redes sociales a promover el crecimiento en un mercado emergente. Acosado por problemas de imagen debidos a varios fallos relacionados con la privacidad en un mercado occidental muy saturado, los mercados emergentes, como la India, representan una interesante manera de que la empresa recupere terreno.

También parece una evolución natural para WhatsApp Pay, un servicio que permite en la India transferir dinero directamente desde las cuentas bancarias a través del servicio de mensajería.

Introducir las criptomonedas en WhatsApp acompañaría a una reorganización masiva en la estrategia de mensajería de Facebook. La empresa ya ha anunciado planes para fusionar WhatsApp con sus aplicaciones Messenger e Instagram, haciendo posible enviar mensajes fácilmente entre los servicios.

El problema al que se enfrenta Facebook es reconciliar su agresivo modelo central de negocio, que se centra en controlar los datos del usuario, con una tecnología como blockchain totalmente descentralizada. Zuckerberg está interesado en utilizar blockchain como método de autenticación, según una entrevista del mes pasado con Harvard Law y el profesor en informática Jonathan Zittrain.

Sin embargo, hay un riesgo potencial para que desarrolladores deshonestos puedan aprovecharse más allá del control de la empresa, avisó, sin citar explícitamente a Cambridge Analytica, quien hizo exactamente eso.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

Telegram
Los planes de Telegram sobre una criptomoneda descentralizada son bien conocidos, siendo la base de una Oferta Inicial de Monedas (ICO), que rápidamente se convirtió en la más exitosa de la historia, recaudando 1.700 millones de dólares en dos tandas el año pasado. La ICO se limitó a inversores privados acreditados después de que la empresa cancelara la parte pública de la venta.

Telegram siempre ha planeado crear Gram, una criptomoneda que se pudiera utilizar para enviar pagos a través del sistema de mensajería cifrado. Formaría parte de un cambio en una blockchain llamada Telegram Open Network (TON), cuyos planes han publicado en un informe. Ya se ha completado el 90% de la infraestructura del blockchain.

Signal
Signal, la otra empresa citada en el informe del New York Times, ha planeado su MobileCoin desde al menos diciembre de 2011, cuando publicó un informe técnico. La moneda, que tiene su propia web, funcionaría utilizando el protocolo de Signal, que también usa WhatsApp. Esto lo haría interoperable entre WhatsApp y Signal. MobileCoin está asesorado por el fundador de Signal Moxie Marlinspike, quien tiene suficiente credibilidad en el mundo de la ciberseguridad habiendo dirigido la seguridad de Twitter.

Estas no son las únicas empresas que han ideado crear sus propias criptomonedas. Reddit también planeó crear su propia criptomoneda hace cinco años, según declaraciones del CEO de aquel momento Yishan Wong. La idea ya descartada, surgió después de que los inversores en una ronda de financiación de 50 millones de dólares, decidieran dar el 10% de la ronda de vuelta a la comunidad.

Pero ¿qué tienen en común Telegram, Signal y WhatsApp? Las tres son apps muy populares de mensajería buscando nueva formas de ganar dinero. Creando sus propia criptomonedas le permitiría al instante utilizarlas a una gran cantidad de sus usuarios, integrando su uso con un interfaz de mensajería muy conocido.

Bien ejecutado, esto ayudaría a florecer el mercado general de criptomonedas, pasando de ser una apuesta especulativa plagada de problemas de fraude, seguridad y usabilidad a una proposición mucho más establecida. Vale la pena seguir estos proyectos, que prometen convertir a 2019 en un año fascinante para el desarrollo de las criptomonedas, una década después de que Bitcoin hiciera su debut.

FUENTE:

Naked Security. (2019, 7 marzo). ¿Se está trabajando en una Facebookcoin? Recuperado 10 marzo, 2019, de https://news.sophos.com/es-es/2019/03/07/se-esta-trabajando-en-una-facebookcoin/

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

VULNERABILIDADES CRÍTICAS DE SEGURIDAD PARA TOMAR LAS MEDIDAS PREVENTIVAS Y CORRECTIVAS FRENTE A LAS AMENAZAS TECNOLÓGICAS

VULNERABILIDAD DE INYECCIÓN DE COMANDOS EN LA CLI DEL SOFTWARE CISCO NX-OS (CVE-2019-1610)

Criticidad: Alta
Impacto: Inyección de comandos
Vulnerabilidad: -
Ejecución: Local
Plataforma(s) afectada(s): Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión vulnerable del software Cisco NX-OS:

- Nexus 3000 Series Switches
- Interruptores de plataforma Nexus 3500

Referencia: CVE-2019-1610
Descripción:
Una vulnerabilidad en la CLI del software Cisco NX-OS podría permitir a un atacante local autenticado ejecutar comandos arbitrarios en el sistema operativo subyacente de un dispositivo afectado.
La vulnerabilidad se debe a una validación insuficiente de los argumentos pasados a ciertos comandos de la CLI. Un atacante podría aprovechar esta vulnerabilidad al incluir una entrada maliciosa como el argumento de un comando afectado. Una explotación exitosa podría permitir al atacante ejecutar comandos arbitrarios en el sistema operativo subyacente con privilegios elevados. Un atacante necesitaría credenciales de administrador válidas para aprovechar esta vulnerabilidad.
Cisco ha lanzado actualizaciones de software que abordan esta vulnerabilidad. No hay soluciones que aborden esta vulnerabilidad.

FUENTE:

Fuente:
Vulnerabilidad de inyección de comandos en la CLI del software Cisco NX-OS (CVE-2019-1610)
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-

VULNERABILIDAD DE INYECCIÓN DE COMANDOS DE LA CLI DEL SOFTWARE CISCO FXOS Y NX-OS (CVE-2019-1611)

Criticidad: Alta
Impacto: Inyección de comandos
Vulnerabilidad: -
Ejecución: Local
Plataforma(s) afectada(s): Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión vulnerable del software Cisco NX-OS o Cisco FXOS:

- Firewower 4100 Series Firewalls de última generación
- Firepower 9300 Security Appliance
- Interruptores multicapa de la serie MDS 9000
- Extensores de tejido Nexus 2000 Series
- Nexus 3000 Series Switches
- Interruptores de plataforma Nexus 3500
- Interruptores de plataforma Nexus 3600
- Interruptores de plataforma Nexus 5500
- Interruptores de plataforma Nexus 5600
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches
- Nexus 7700 Series Switches
- Nexus 9000 Series Switches en modo NX-OS independiente
- Tarjetas de línea Nexus 9500 R

Referencia: CVE-2019-1611
Descripción:
Una vulnerabilidad en la CLI del software Cisco NX-OS y Cisco FXOS podría permitir que un atacante local autenticado ejecute comandos arbitrarios en el sistema operativo subyacente de un dispositivo afectado.

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

La vulnerabilidad se debe a una validación insuficiente de los argumentos pasados a ciertos comandos de la CLI. Un atacante podría aprovechar esta vulnerabilidad al incluir una entrada maliciosa como el argumento de un comando afectado. Una explotación exitosa podría permitir al atacante ejecutar comandos arbitrarios en el sistema operativo subyacente con privilegios elevados. Un atacante necesitaría credenciales de administrador válidas para aprovechar esta vulnerabilidad.

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

FUENTES:

Vulnerabilidad de inyección de comandos de la CLI del software Cisco FXOS y NX-OS (CVE-2019-1611)
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-cmdinj-1611

VULNERABILIDAD DE INYECCIÓN DE COMANDOS DE LA CLI DEL SOFTWARE CISCO FXOS Y NX-OS (CVE-2019-1611)

Criticidad: Alta
Impacto: Inyección de comandos
Vulnerabilidad:
Ejecución: Local
Plataforma(s) Afectada(s):
Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión vulnerable del software Cisco NX-OS:

- Nexus 3000 Series Switches
- Interruptores de plataforma Nexus 3500
- Interruptores de plataforma Nexus 3600
- Nexus 9000 Series Switches en modo NX-OS independiente
- Tarjetas de línea Nexus 9500 R

Referencia: CVE-2019-1612
Descripción:
Una vulnerabilidad en la CLI del software Cisco NX-OS podría permitir a un atacante local autenticado ejecutar comandos arbitrarios en el sistema operativo subyacente de un dispositivo afectado.

La vulnerabilidad se debe a una validación insuficiente de los argumentos pasados a ciertos comandos de la CLI. Un atacante podría aprovechar esta vulnerabilidad al incluir una entrada maliciosa como el argumento de un comando afectado. Una explotación exitosa podría permitir al atacante ejecutar comandos arbitrarios en el sistema operativo subyacente con privilegios elevados. Un atacante necesitaría credenciales de administrador válidas para aprovechar esta vulnerabilidad.

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

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

FUENTES:

Vulnerabilidad de inyección de comandos en la CLI del software Cisco NX-OS (CVE-2019-1612)
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-cmdinj-1612

VULNERABILIDAD DE INYECCIÓN DE COMANDOS EN LA CLI DEL SOFTWARE CISCO NX-OS (CVE-2019-1613)

Criticidad: Alta
Impacto: Inyección de comandos
Vulnerabilidad:
Ejecución: Local
Plataforma(s)
Afectada(s):
Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión vulnerable del software Cisco NX-OS:

- Interruptores multicapa de la serie MDS 9000
- Nexus 3000 Series Switches
- Interruptores de plataforma Nexus 3500
- Interruptores de plataforma Nexus 3600
- Nexus 7000 Series Switches
- Nexus 7700 Series Switches
- Nexus 9000 Series Switches en modo NX-OS independiente
- Tarjetas de línea Nexus 9500 R

Referencia: CVE-2019-1613
Descripción: Una vulnerabilidad en la CLI del software Cisco NX-OS podría permitir a un atacante local autenticado ejecutar comandos arbitrarios en el sistema operativo subyacente de un dispositivo afectado.

La vulnerabilidad se debe a una validación insuficiente de los argumentos pasados a ciertos comandos de la CLI. Un atacante podría aprovechar esta vulnerabilidad al incluir una entrada maliciosa como el argumento de un comando afectado. Una explotación exitosa podría permitir al atacante ejecutar comandos arbitrarios en el sistema operativo subyacente con privilegios elevados. Un atacante necesitaría credenciales de administrador válidas para aprovechar esta vulnerabilidad.
Cisco ha lanzado actualizaciones de software que abordan esta vulnerabilidad. No hay soluciones que aborden esta vulnerabilidad.

FUENTES:

Vulnerabilidad de inyección de comandos en la CLI del software Cisco NX-OS (CVE-2019-1613)
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-cmdinj-1613

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

VULNERABILIDAD DE ACCESO NO AUTORIZADO AL ACCESO AL DIRECTORIO DE CISCO FXOS Y NX-OS SOFTWARE

Criticidad: Alta
Impacto: Acceso no autorizado
Vulnerabilidad:
Ejecución: Local
Plataforma(s) Afectada(s):
Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión vulnerable del software Cisco FXOS o del software Cisco NX-OS:

- Firewower 4100 Series Firewalls de última generación
- Firepower 9300 Security Appliance
- Interruptores multicapa de la serie MDS 9000
- Extensores de tejido Nexus 2000 Series
- Nexus 3000 Series Switches
- Interruptores de plataforma Nexus 3500
- Interruptores de plataforma Nexus 3600
- Interruptores de plataforma Nexus 5500
- Interruptores de plataforma Nexus 5600
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches
- Nexus 7700 Series Switches
- Nexus 9000 Series Switches en modo NX-OS independiente
- Tarjetas de línea Nexus 9500 R

Referencia: CVE-2019-1600

Descripción:
Una vulnerabilidad en los permisos del sistema de archivos de Cisco FXOS Software y Cisco NX-OS Software podría permitir a un atacante local autenticado acceder a información confidencial almacenada en el sistema de archivos de un sistema afectado.

La vulnerabilidad se debe a la implementación incorrecta de los permisos del sistema de archivos. Un atacante podría aprovechar esta vulnerabilidad al acceder y modificar los archivos restringidos. Una explotación exitosa podría permitir al atacante acceder a archivos importantes y críticos.

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

FUENTES:

Vulnerabilidad de acceso no autorizado al acceso al directorio de Cisco FXOS y NX-OS Software
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-directory

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

VULNERABILIDAD DE AMPLIACIÓN DE PRIVILEGIOS EN EL SOFTWARE DE CISCO NX-OS

Criticidad: Alta
Impacto: Acceso no autorizado
Vulnerabilidad:
Ejecución: Local
Plataforma(s) Afectada(s):
Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión vulnerable del software Cisco NX-OS:

- Nexus 3000 Series Switches
- Interruptores de plataforma Nexus 3500
- Interruptores de plataforma Nexus 3600
- Nexus 9000 Series Switches en modo NX-OS independiente
- Tarjetas de línea Nexus 9500 R

Referencia: CVE-2019-1602

Descripción:

Descripción:

Una vulnerabilidad en los permisos del sistema de archivos del software Cisco NX-OS podría permitir a un atacante local autenticado acceder a datos confidenciales que podrían usarse para elevar sus privilegios al administrador .

La vulnerabilidad se debe a la implementación incorrecta de los permisos del sistema de archivos. Un atacante podría aprovechar esta vulnerabilidad si inicia sesión en la CLI de un dispositivo afectado, accede a un archivo específico y aprovecha esta información para autenticarse en el servidor NX-API. Una explotación exitosa podría permitir que un atacante realice cambios de configuración como administrador .

Nota : NX-API está deshabilitado de forma predeterminada.

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

FUENTES:

Vulnerabilidad de ampliación de privilegios en el software de Cisco NX-OS
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-escalation

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

VULNERABILIDAD DE DENEGACIÓN DE SERVICIO DE CISCO FABRIC SERVICES EN EL SOFTWARE CISCO NX-OS

Criticidad: Alta
Impacto: Denegación de servicio
Vulnerabilidad:
Ejecución: Remota
Plataforma(s) Afectada(s):
Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión vulnerable del software Cisco NX-OS:

- Interruptores multicapa de la serie MDS 9000
- Nexus 3000 Series Switches
- Interruptores de plataforma Nexus 3500
- Interruptores de plataforma Nexus 3600
- Nexus 7000 Series Switches
- Nexus 7700 Series Switches
- Nexus 9000 Series Switches en modo NX-OS independiente
- Tarjetas de línea Nexus 9500 R y módulos de tela
- UCS 6200 Series Interconexiones de tela
- UCS 6300 Series Fabric Interconexiones
- UCS 6400 Series Fabric Interconexiones

Referencia: CVE-2019-1616
Descripción:
Una vulnerabilidad en el componente Cisco Fabric Services del software Cisco NX-OS podría permitir que un atacante remoto no autenticado provoque un desbordamiento del búfer, lo que resulta en una condición de denegación de servicio (DoS).

La vulnerabilidad se debe a la validación insuficiente de los paquetes de Cisco Fabric Services. Un atacante podría aprovechar esta vulnerabilidad enviando un paquete de Cisco Fabric Services a un dispositivo afectado. Una explotación exitosa podría permitir al atacante causar un desbordamiento del búfer, lo que provocaría fallos en el proceso y una condición DoS en el dispositivo.

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

FUENTES:

Vulnerabilidad de denegación de servicio de Cisco Fabric Services en el software Cisco NX-OS
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-fabric-dos

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

VULNERABILIDAD DE DENEGACIÓN DE SERVICIO DE LOS SERVICIOS WEB DE CISCO ADAPTIVE SECURITY APPLIANCE

Criticidad: Alta
Impacto: Denegación de servicio
Vulnerabilidad:
Ejecución: Remota
Plataforma(s)
Afectada(s):
Esta vulnerabilidad afecta al software Cisco ASA y al software Cisco Firepower Threat Defense (FTD) que se ejecuta en los siguientes productos Cisco:

- Dispositivo de seguridad industrial serie 3000 (ISA)
- Cortafuegos ASA 1000V Cloud
- Dispositivos de seguridad adaptable de la serie ASA 5500
- Cortafuegos de última generación de la serie ASA 5500-X
- Módulo de servicios ASA para Cisco Catalyst 6500 Series Switch y Cisco 7600 Series Routers
- Dispositivo virtual de seguridad adaptable (ASAv)
- Firepower 2100 Series Security Appliance
- Firepower 4100 Series Security Appliance
- Firepower 9300 ASA Security Module
- FTD Virtual (FTDv)

Referencia: CVE-2018-0296

Descripción:
Una vulnerabilidad en la interfaz web de Cisco Adaptive Security Appliance (ASA) podría permitir que un atacante remoto no autenticado haga que un dispositivo afectado se vuelva a cargar inesperadamente, lo que resulta en una condición de denegación de servicio (DoS).

También es posible en ciertas versiones de software que el ASA no se vuelva a cargar, pero un atacante podría ver información confidencial del sistema sin autenticación mediante el uso de técnicas de desplazamiento de directorios.

La vulnerabilidad se debe a la falta de validación de entrada adecuada de la URL HTTP. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud HTTP diseñada a un dispositivo afectado. Un exploit podría permitir al atacante causar una condición DoS o una divulgación de información no autenticada. Esta vulnerabilidad se aplica al tráfico HTTP de IPv4 e IPv6.

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

FUENTES:
Vulnerabilidad de denegación de servicio de los servicios web de Cisco Adaptive Security Appliance
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-asaftd

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

JUNOS: FALLO DE RPD AL PROCESAR ANUNCIOS RIP (CVE-2017-2303)

Impacto: Medio
Vulnerabilidad:
Ejecución: Remota
Plataforma(s)
Afectada(s): A cualquier producto o plataforma que ejecute Junos OS donde RIP esté habilitado.
Referencia: (CVE-2017-2303)

Descripción:
Ciertos anuncios RIP recibidos por el enrutador pueden hacer que el daemon RPD se bloquee. Mientras que el demonio RPD se reinicia después de un bloqueo, los bloqueos repetidos del demonio RPD pueden dar como resultado una condición extendida de denegación de servicio.

Este problema solo afecta a los dispositivos donde RIP está habilitado.

Juniper SIRT no tiene conocimiento de ninguna explotación maliciosa de esta vulnerabilidad.

Ningún otro producto o plataforma de Juniper Networks está afectado por este problema. Solución:
Las siguientes versiones de software se han actualizado para resolver este problema específico: Junos OS 12.1X46-D50, 12.1X47-D40, 12.3R12-S4, 12.3R13, 12.3X48-D30, 13.2X51-D40, 13.3R10, 14.1R8, 14.1 X53-D35, 14.1X55-D35, 14.2R5, 15.1F6, 15.1R3, 15.1X49-D30, 15.1X49-D40, 15.1X53-D35, 16.1R1, y todas las versiones posteriores.

Este problema se está rastreando como PR 1129202 y se puede ver en el sitio web de atención al cliente.

KB16765 - "¿En qué versiones se corrigen las vulnerabilidades?" describe qué vulnerabilidades de la versión se corrigen según nuestras políticas de soporte al final de la ingeniería y al final de la vida útil.
No hay soluciones alternativas conocidas que puedan evitar este problema.
Es una buena práctica de seguridad limitar la superficie de ataque explotable de los equipos de redes de infraestructura crítica. Use listas de acceso o filtros de firewall para limitar el acceso al enrutador solo desde redes o hosts administrativos y de confianza

FUENTES:

Junos OS: Fallo de RPD al procesar anuncios RIP (CVE-2017-2303), Marzo 2019 de Juniper Networks, Sitio Web:
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10772&cat=SIRT_1&actp=LIST

SERVICIO DE INTELIGENCIA CONTRA AMENAZAS "SIA"

JUNOS: VULNERABILIDAD DE DENEGACIÓN DE SERVICIO EN RPD (CVE-2017-2302)

Impacto: Medio
Vulnerabilidad:
Ejecución: Remota
Plataforma(s)
Afectada(s): A cualquier producto o plataforma que ejecute Junos OS.
Referencia: (CVE-2017-2302)

Descripción:

En los dispositivos Junos OS donde la función de ruta de acceso BGP está habilitada con la opción "enviar" o con las opciones "enviar" y "recibir", un atacante basado en la red puede hacer que el demonio rpd de Junos OS se bloquee y se reinicie. Los bloqueos repetidos del demonio rpd pueden dar como resultado una condición de de-negación de servicio extendida.

Los dispositivos del sistema operativo Junos que no tienen habilitada la función de agregar ruta BGP no se ven afectados por este problema.

Este problema no afecta a los dispositivos Junos OS que solo tienen la opción 'recibir' con la función de ruta de acceso BGP habilitada.

Juniper SIRT no tiene conocimiento de ninguna explotación maliciosa de esta vulne-rabilidad.

Ningún otro producto o plataforma de Juniper Networks está afectado por este pro-blema.

Este problema ha sido asignado CVE-2017-2302.

FUENTES:

Junos OS: Junos: Vulnerabilidad de denegación de servicio en RPD (CVE-2017-2302), Marzo 2019 de Juniper Networks, Sitio Web:
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10771&cat=SIRT_1&actp=LIST