Alerta de seguridad informática	9VSA-00041-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de agosto de 2019
Última revisión	31 de agosto de 2019

NOTIFICACIÓN
La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por CISCO referente vulnerabilidades detectadas en varios de sus productos y sus respectivas actualizaciones para mitigar el riesgo.

Vulnerabilidad

CVE-2019-1977

Impacto

Una vulnerabilidad dentro de la función Endpoint Learning de los switches Cisco Nexus de la serie 9000 que se ejecutan en el modo Application Centric Infrastructure (ACI) podría permitir que un atacante remoto no autenticado cause una condición de denegación de servicio (DoS) en un dispositivo de punto final en ciertas circunstancias.

La vulnerabilidad se debe a un aprendizaje inadecuado del punto final cuando los paquetes se reciben en un puerto específico desde fuera de la estructura ACI y se destinan a un punto final ubicado en una hoja de borde cuando se ha habilitado la opción Desactivar el aprendizaje remoto del punto final Esto puede provocar que se cree una entrada remota (XR) para el punto final afectado que se volverá obsoleta si el punto final migra a un puerto o conmutador hoja diferente. Esto da como resultado que el tráfico no llegue al punto final afectado hasta que la entrada remota pueda ser reaprendida por otro mecanismo.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a los Switches Fabric Cisco Nexus 9000 Series en modo ACI que ejecuten versiones de software Cisco NX-OS ACI anteriores a 12.2 (4M), 13.1 (2u) o 13.2 (1l).

Mitigación

Actualizar el producto según lo indicado por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190828-nexus-aci-dos

---

Vulnerabilidad

CVE-2019-1968

Impacto

Una vulnerabilidad en la función NX-API del software Cisco NX-OS podría permitir que un atacante remoto no autenticado haga que un proceso del sistema NX-API se reinicie inesperadamente.

La vulnerabilidad se debe a la validación incorrecta del encabezado HTTP de una solicitud que se envía a la NX-API. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud HTTP diseñada a la NX-API en un dispositivo afectado. Una explotación exitosa podría permitir al atacante causar una condición de denegación de servicio (DoS) en el servicio NX-API; sin embargo, el dispositivo NX-OS en sí mismo aún estaría disponible y pasaría tráfico de red.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a los siguientes productos de Cisco si ejecutaban una versión vulnerable del software Cisco NX-OS y tengan habilitada la función NX-API:

- MDS 9000 Series Multilayer Switches
- Nexus 3000 Series Switches
- Nexus 3500 Platform Switches
- Nexus 3600 Platform Switches
- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches

- Nexus 7700 Series Switches
- Nexus 9000 Series Switches in standalone NX-OS mode
- Nexus 9500 R-Series Switching Platform

Mitigación

Actualizar el producto según lo indicado por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190828-nxos-api-dos

---

Vulnerabilidad

CVE-2019-1967

Impacto

Una vulnerabilidad en la función Network Time Protocol (NTP) del software Cisco NX-OS podría permitir que un atacante remoto no autenticado cause una condición de denegación de servicio (DoS) en un dispositivo afectado.

La vulnerabilidad se debe al uso excesivo de los recursos del sistema cuando el dispositivo afectado está registrando una acción de caída para los paquetes NTP MODE_PRIVATE (Modo 7) recibidos. Un atacante podría aprovechar esta vulnerabilidad inundando el dispositivo con un flujo constante de paquetes NTP en Modo 7. Una explotación exitosa podría permitir al atacante causar un alto uso de CPU y memoria en el dispositivo afectado, lo que podría provocar que los procesos internos del sistema se reinicien o que el dispositivo afectado se recargue inesperadamente.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a los siguientes productos de Cisco si ejecutaban una versión vulnerable del software Cisco NX-OS y tengan habilitada la función NTP:

- MDS 9000 Series Multilayer Switches
- Nexus 3000 Series Switches
- Nexus 3500 Platform Switches
- Nexus 3600 Platform Switches
- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches
- Nexus 7700 Series Switches

- Nexus 9000 Series Switches in standalone NX-OS mode
- Nexus 9500 R-Series Switching Platform

Mitigación

Actualizar el producto según lo indicado por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190828-nxos-ntp-dos

---

Vulnerabilidad

CVE-2019-1969

Impacto

Una vulnerabilidad en la implementación de la función Simple Network Management Protocol (SNMP) Access Control List (ACL) del software Cisco NX-OS podría permitir que un atacante remoto no autenticado realice un sondeo SNMP de un dispositivo afectado, incluso si está configurado para negar Tráfico SNMP

La vulnerabilidad se debe a una verificación de longitud incorrecta cuando el nombre de ACL configurado es la longitud máxima, que es de 32 caracteres ASCII. Un atacante podría aprovechar esta vulnerabilidad realizando consultas SNMP de un dispositivo afectado. Una explotación exitosa podría permitir al atacante realizar consultas SNMP que deberían haberse denegado. El atacante no tiene control de la configuración del nombre de ACMP SNMP.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a los siguientes productos de Cisco si ejecutaban una versión vulnerable del software Cisco NX-OS con una ACL SNMP específica configurada:

- Nexus 3000 Series Switches
- Nexus 3500 Platform Switches
- Nexus 3600 Platform Switches
- Nexus 9000 Series Switches in standalone NX-OS mode
- Nexus 9500 R-Series Switching Platform

Mitigación

Actualizar el producto según lo indicado por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190828-nxos-snmp-bypass

---

Vulnerabilidad

CVE-2019-1963

Impacto

Una vulnerabilidad en el procesador de paquetes de entrada del Protocolo simple de administración de redes (SNMP) del Software Cisco FXOS y del Software Cisco NX-OS podría permitir que un atacante remoto autenticado haga que la aplicación SNMP en un dispositivo afectado se reinicie inesperadamente.

La vulnerabilidad se debe a la validación incorrecta de las variables codificadas en la sintaxis abstracta de notación uno (ASN.1) en los paquetes SNMP. Un atacante podría aprovechar esta vulnerabilidad enviando un paquete SNMP diseñado al demonio SNMP en el dispositivo afectado. Una explotación exitosa podría permitir al atacante hacer que la aplicación SNMP se reinicie varias veces, lo que provocaría un reinicio a nivel del sistema y una condición de denegación de servicio (DoS).

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco si tienen configurado SNMP y están ejecutando una versión vulnerable del software Cisco FXOS o NX-OS:

- Firepower 4100 Series
- Firepower 9300 Security Appliances
- MDS 9000 Series Multilayer Switches
- Nexus 1000 Virtual Edge for VMware vSphere
- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- Nexus 3000 Series Switches
- Nexus 3500 Platform Switches
- Nexus 3600 Platform Switches
- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches

- Nexus 7700 Series Switches
- Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode
- Nexus 9000 Series Switches in standalone NX-OS mode
- Nexus 9500 R-Series Switching Platform
- UCS 6200 Series Fabric Interconnects
- UCS 6300 Series Fabric Interconnects
- UCS 6400 Series Fabric Interconnects

Mitigación

Actualizar el producto según lo indicado por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190828-fxnxos-snmp-dos

---

Vulnerabilidad

CVE-2019-1962

Impacto

Una vulnerabilidad en el componente Cisco Fabric Services del software Cisco NX-OS podría permitir que un atacante remoto no autenticado cause bloqueos del proceso, lo que puede provocar una condición de denegación de servicio (DoS) en un sistema afectado.

La vulnerabilidad se debe a una validación insuficiente de los paquetes TCP cuando los procesa la función Cisco Fabric Services sobre IP (CFSoIP). Un atacante podría aprovechar esta vulnerabilidad al enviar un paquete TCP de Cisco Fabric Services malicioso a un dispositivo afectado. Una explotación exitosa podría permitir al atacante provocar bloqueos en el proceso, lo que provocaría una recarga del dispositivo y una condición DoS.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco si están ejecutando una versión vulnerable del software Cisco NX-OS con CFSoIP habilitado:

- MDS 9000 Series Multilayer Switches
- Nexus 3000 Series Switches
- Nexus 3500 Platform Switches
- Nexus 3600 Platform Switches
- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches

- Nexus 6000 Series Switches
- Nexus 7000 Series Switches
- Nexus 7700 Series Switches
- Nexus 9000 Series Switches in standalone NX-OS mode
- Nexus 9500 R-Series Switching Platform
- UCS 6200 Series Fabric Interconnects
- UCS 6300 Series Fabric Interconnects

Mitigación

Actualizar el producto según lo indicado por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190828-nxos-fsip-dos

---

Vulnerabilidad

CVE-2019-1964

Impacto

Una vulnerabilidad en la administración de sesión de Virtual Shell (VSH) para el software Cisco NX-OS podría permitir que un atacante remoto autenticado haga que un proceso VSH no se elimine al finalizar. Esto puede conducir a una acumulación de procesos VSH que pueden agotar la memoria del sistema. Cuando no hay memoria del sistema disponible, esto puede causar comportamientos inesperados del sistema y fallas.

La vulnerabilidad se debe a que el proceso VSH no se elimina correctamente cuando se desconecta una conexión de administración remota al dispositivo. Un atacante podría aprovechar esta vulnerabilidad al realizar repetidamente una conexión de administración remota al dispositivo y terminar la conexión de manera inesperada. Una explotación exitosa podría permitir al atacante hacer que los procesos VSH no se eliminen, lo que puede conducir a una condición de denegación de servicio (DoS) en todo el sistema. El atacante debe tener credenciales de usuario válidas para iniciar sesión en el dispositivo utilizando la conexión de administración remota.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco si están ejecutando una versión vulnerable del software Cisco NX-OS:

- MDS 9000 Series Multilayer Switches
- Nexus 3000 Series Switches
- Nexus 3500 Platform Switches

- Nexus 3600 Platform Switches
- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches
- Nexus 7700 Series Switches
- Nexus 9000 Series Switches in standalone NX-OS mode
- Nexus 9500 R-Series Switching Platform
- UCS 6200 Series Fabric Interconnects
- UCS 6300 Series Fabric Interconnects

Mitigación

Actualizar el producto según lo indicado por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190828-nxos-memleak-dos

---

Vulnerabilidad

CVE-2019-1965

Impacto

Una vulnerabilidad en la administración de sesión de Virtual Shell (VSH) para el software Cisco NX-OS podría permitir que un atacante remoto autenticado haga que un proceso VSH no se elimine al finalizar. Esto puede conducir a una acumulación de procesos VSH que pueden agotar la memoria del sistema. Cuando no hay memoria del sistema disponible, esto puede causar comportamientos inesperados del sistema y fallas.

La vulnerabilidad se debe a que el proceso VSH no se elimina correctamente cuando se desconecta una conexión de administración remota al dispositivo. Un atacante podría aprovechar esta vulnerabilidad al realizar repetidamente una conexión de administración remota al dispositivo y terminar la conexión de manera inesperada. Una explotación exitosa podría permitir al atacante hacer que los procesos VSH no se eliminen, lo que puede conducir a una condición de denegación de servicio (DoS) en todo el sistema. El atacante debe tener credenciales de usuario válidas para iniciar sesión en el dispositivo utilizando la conexión de administración remota.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco si están ejecutando una versión vulnerable del software Cisco NX-OS:

- MDS 9000 Series Multilayer Switches
- Nexus 3000 Series Switches
- Nexus 3500 Platform Switches
- Nexus 3600 Platform Switches
- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches
- Nexus 7700 Series Switches
- Nexus 9000 Series Switches in standalone NX-OS mode
- Nexus 9500 R-Series Switching Platform
- UCS 6200 Series Fabric Interconnects
- UCS 6300 Series Fabric Interconnects

Mitigación

Actualizar el producto según lo indicado por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190828-nxos-memleak-dos

---

Vulnerabilidad

CVE-2019-1966

Impacto

Una vulnerabilidad en un comando CLI específico dentro del contexto de administración local (local-mgmt) para el software Cisco UCS Fabric Interconnect podría permitir que un atacante local autenticado obtenga privilegios elevados como usuario root en un dispositivo afectado.

La vulnerabilidad se debe a las opciones de subcomando extrañas presentes para un comando CLI específico dentro del contexto local-mgmt. Un atacante podría aprovechar esta vulnerabilidad autenticándose en un dispositivo afectado, ingresando el contexto local-mgmt, y emitiendo un comando CLI específico y enviando la entrada del usuario. Una explotación exitosa podría permitir al atacante ejecutar comandos arbitrarios del sistema operativo como root en un dispositivo afectado. El atacante necesitaría tener credenciales de usuario válidas para el dispositivo.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco si están ejecutando una versión vulnerable del software Cisco UCS Fabric Interconnect:

- UCS 6200 Series Fabric Interconnects
- UCS 6300 Series Fabric Interconnects
- UCS 6400 Series Fabric Interconnects

Mitigación

Actualizar el producto según lo indicado por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190828-ucs-privescalation

---

Vulnerabilidad

CVE-2019-12643

Impacto

Una vulnerabilidad en el contenedor de servicios virtuales API REST de Cisco para el software Cisco IOS XE podría permitir que un atacante remoto no autenticado omita la autenticación en el dispositivo Cisco IOS XE administrado.

La vulnerabilidad se debe a una verificación incorrecta realizada por el área de código que administra el servicio de autenticación API REST. Un atacante podría aprovechar esta vulnerabilidad al enviar solicitudes HTTP maliciosas al dispositivo objetivo. Una explotación exitosa podría permitir al atacante obtener el identificador de token de un usuario autenticado. Este token-id podría usarse para omitir la autenticación y ejecutar acciones privilegiadas a través de la interfaz del contenedor del servicio virtual REST API en el dispositivo Cisco IOS XE afectado.

Productos Afectados

Esta vulnerabilidad afecta a los dispositivos Cisco que están configurados para usar una versión vulnerable del contenedor de servicios virtuales API REST de Cisco. En el momento de la publicación, esta vulnerabilidad afectaba a los siguientes productos:

- Cisco 4000 Series Integrated Services Routers
- Cisco ASR 1000 Series Aggregation Services Routers
- Cisco Cloud Services Router 1000V Series
- Cisco Integrated Services Virtual Router

Mitigación

Actualizar el producto según lo indicado por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190828-iosxe-rest-auth-bypass

---

Vulnerabilidad

CVE-2019-1944
CVE-2019-1945

Impacto

Una vulnerabilidad en la funcionalidad de túnel inteligente de Cisco ASA podría permitir a un atacante local autenticado elevar los privilegios al usuario raíz. Esta escalada de privilegios ocurre en un dispositivo cliente que intenta establecer una conexión de túnel inteligente con Cisco ASA. La escalada no se produce en el propio ASA.

Productos Afectados

Estas vulnerabilidades afectan el software Cisco ASA.

Mitigación

Actualizar el producto según lo indicado por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190807-asa-multi

---

Vulnerabilidad

CVE-2019-12299

Impacto

Una vulnerabilidad en el proceso para crear bloques de IP predeterminados durante la inicialización del dispositivo para los dispositivos de seguridad Cisco Firepower 4100 Series y Firepower 9300 que ejecutan el software Cisco FXOS podría permitir que un atacante remoto no

autenticado envíe tráfico a la dirección IP local del dispositivo, evitando cualquier filtro que están configurados para denegar el tráfico de administración de IP local.

Productos Afectados

Esta vulnerabilidad afecta a los dispositivos de seguridad Cisco Firepower 4100 Series y Firepower 9300.

Mitigación

Actualizar el producto según lo indicado por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-firepower1

Vulnerabilidad

CVE-2019-1936

Impacto

Una vulnerabilidad en la interfaz de administración web de Cisco Integrated Management Controller (IMC) Supervisor, Cisco UCS Director y Cisco UCS Director Express para Big Data podría permitir que un atacante remoto autenticado ejecute comandos arbitrarios en el shell Linux subyacente como raíz usuario. La explotación de esta vulnerabilidad requiere acceso privilegiado a un dispositivo afectado.

Productos Afectados

- Cisco IMC Supervisor releases:
  - 2.1
  - 2.2.0.0 a 2.2.0.6
- Cisco UCS Director releases:
  - 6.0
  - 6.5
  - 6.6.0.0 y 6.6.1.0
  - 6.7.0.0 y 6.7.1.0
- Cisco UCS Director Express for Big Data releases:
  - 3.0
  - 3.5

- 3.6
- 3.7.0.0 y 3.7.1.0

Mitigación

Actualizar el producto según lo indicado por el fabricante.
Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imcs-ucs-cmdinj

---

Vulnerabilidad

CVE-2019-1937

Impacto

Una vulnerabilidad en la interfaz de administración web de Cisco Integrated Management Controller (IMC) Supervisor, Cisco UCS Director y Cisco UCS Director Express para Big Data podría permitir que un atacante remoto no autenticado adquiera un token de sesión válido con privilegios de administrador, evitando al usuario autenticación.

Productos Afectados

- Cisco IMC Supervisor releases:
  - 2.2.0.3 a 2.2.0.6
- Cisco UCS Director releases:
  - 6.6.0.0 y 6.6.1.0
  - 6.7.0.0 y 6.7.1.0
- Cisco UCS Director Express for Big Data releases:
  - 3.6
  - 3.7.0.0 y 3.7.1.0

Mitigación

Actualizar el producto según lo indicado por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imcs-ucs-authby

---

Vulnerabilidad

CVE-2019-1935

Impacto

Una vulnerabilidad en el Cisco Integrated Management Controller (IMC) Supervisor, Cisco UCS Director, and Cisco UCS Director Express for Big Data podría permitir que un atacante remoto no autenticado inicie sesión en la CLI de un sistema afectado utilizando la cuenta de usuario SCP (scpuser) , que tiene credenciales de usuario predeterminadas.

Productos Afectados

- Cisco IMC Supervisor releases:
  - 2.2.0.3 a 2.2.0.6
- Cisco UCS Director releases:
  - 6.0
  - 6.5
  - 6.6.0.0 y 6.6.1.0
  - 6.7.0.0 y 6.7.1.0
- Cisco UCS Director Express for Big Data releases:
  - 3.0
  - 3.5
  - 3.6
  - 3.7.0.0 y 3.7.1.0

Mitigación

Actualizar el producto según lo indicado por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imcs-usercred

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.08.30 22:11:01 -04'00'