Alerta de Seguridad Informática

Alerta de seguridad informática	9VSA-00039-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de agosto de 2019
Última revisión	23 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-2019-1982

Impacto

Una vulnerabilidad en el componente de filtrado de tráfico HTTP del software Cisco Firepower Threat Defense, el software Cisco FirePOWER Services para ASA y el software Cisco Firepower Management Center podría permitir que un atacante remoto no autenticado omita las protecciones de filtrado.

La vulnerabilidad se debe al manejo inadecuado de las solicitudes HTTP, incluidas las comunicadas a través de una conexión HTTPS segura, que contienen encabezados diseñados con fines malintencionados. Un atacante podría aprovechar esta vulnerabilidad enviando solicitudes maliciosas a un dispositivo afectado. Un exploit podría permitir al atacante evitar el filtrado y entregar solicitudes maliciosas a los sistemas protegidos, lo que permitiría a los atacantes entregar contenido malicioso que de otro modo se bloquearía.

Productos Afectados

- Cisco Firepower Threat Defense software.
- Cisco Firepower Services para ASA software.
- Cisco Firepower Management Center software.

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190816-ftd-http
https://quickview.cloudapps.cisco.com/quickview/bug/CSCvj19544
https://quickview.cloudapps.cisco.com/quickview/bug/CSCvq07297

Vulnerabilidad

CVE-2019-1980

Impacto

Una vulnerabilidad en el componente de detección de protocolo del software Cisco Firepower Threat Defense, el software Cisco FirePOWER Services para ASA y el software Cisco Firepower Management Center podría permitir que un atacante remoto no autenticado omita las protecciones de filtrado.

La vulnerabilidad se debe a la detección inadecuada del uso inicial de un protocolo en un puerto no estándar. Un atacante podría aprovechar esta vulnerabilidad enviando tráfico en un puerto no estándar para el protocolo en uso a través de un dispositivo afectado. Un exploit podría permitir al atacante omitir el filtrado y entregar solicitudes maliciosas a los sistemas protegidos que de otro modo se bloquearían. Una vez que se detecta el flujo de protocolo inicial en el puerto no estándar, los flujos futuros en el puerto no estándar se detectarán con éxito y se manejarán según lo configurado por la política aplicada.

Productos Afectados

- Cisco Firepower Threat Defense software.
- Cisco Firepower Services para ASA software.
- Cisco Firepower Management Center software.

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190816-ftd-nspd
https://quickview.cloudapps.cisco.com/quickview/bug/CSCvq39888

Vulnerabilidad

CVE-2019-1981

Impacto

Una vulnerabilidad en la funcionalidad de normalización del software Cisco Firepower Threat Defense, el software Cisco FirePOWER Services para ASA y el software Cisco Firepower Management Center podría permitir que un atacante remoto no autenticado omita las protecciones de filtrado.

La vulnerabilidad se debe a la insuficiente normalización de una carga útil basada en texto. Un atacante podría aprovechar esta vulnerabilidad enviando tráfico que contenga cargas útiles especialmente ofuscadas a través de un dispositivo afectado. Un exploit podría permitir al atacante evitar el filtrado y entregar cargas maliciosas a los sistemas protegidos que de otro modo se bloquearían.

Productos Afectados

- Cisco Firepower Threat Defense software.
- Cisco Firepower Services para ASA software.
- Cisco Firepower Management Center software.

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190816-ftd-null
https://quickview.cloudapps.cisco.com/quickview/bug/CSCvq39915

Vulnerabilidad

CVE-2019-1978

Impacto

A vulnerability in the stream reassembly component of Cisco Firepower Threat Defense Software, Cisco FirePOWER Services Software for ASA, and Cisco Firepower Management Center Software could allow an unauthenticated, remote attacker to bypass filtering protections.

The vulnerability is due to improper reassembly of traffic streams. An attacker could exploit this vulnerability by sending crafted streams through an affected device. An exploit could allow the attacker to bypass filtering and deliver malicious requests to protected systems that would otherwise be blocked.

Productos Afectados

- Cisco Firepower Threat Defense software.
- Cisco Firepower Services para ASA software.
- Cisco Firepower Management Center software.

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190816-ftd-srb
https://quickview.cloudapps.cisco.com/quickview/bug/CSCvq39955

Vulnerabilidad

CVE-2019-9506

Impacto

Una debilidad en la especificación central del protocolo Basic Rate/Enhanced Data Rate (BR / EDR) de Bluetooth expone una vulnerabilidad que podría permitir que un atacante adyacente no autenticado realice un ataque de hombre en el medio en una conexión Bluetooth cifrada. El ataque debe realizarse durante la negociación o renegociación de una conexión de dispositivo emparejado; las sesiones existentes no pueden ser atacadas.

El problema podría permitir al atacante reducir la entropía de la clave de sesión negociada que se utiliza para asegurar una conexión Bluetooth entre un dispositivo emparejado y un dispositivo host. Un atacante que pueda inyectar con éxito un mensaje malicioso en una conexión Bluetooth durante la negociación o renegociación de la sesión podría hacer que la fuerza de la clave de la sesión sea susceptible al ataque de fuerza bruta.

Productos Afectados

- Cisco Collaboration Desk Endpoints
  - Cisco Webex DX70
  - Cisco Webex DX80
- Cisco IP Phones
  - Cisco 8821 Wireless IP Phones
  - Cisco 8845 IP Phones
  - Cisco 8851 IP Phones
  - Cisco 8861 IP Phones
  - Cisco 8865 IP Phones
  - Cisco SPA525G2 Small Business IP Phones

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190813-bluetooth

---

Vulnerabilidad

CVE-2019-12626

Impacto

Una vulnerabilidad en la interfaz de administración basada en web de Cisco Unified Contact Center Express (Unified CCX) podría permitir que un atacante remoto autenticado realice un ataque cross-site scripting (XSS) almacenado contra un usuario de la interfaz de administración basada en web del dispositivo afectado.

La vulnerabilidad se debe a una validación insuficiente de la entrada proporcionada por el usuario por la interfaz de administración basada en web del software afectado. Un atacante podría aprovechar esta vulnerabilidad persuadiendo a un usuario de la interfaz para que haga clic en un enlace diseñado. Una explotación exitosa podría permitir al atacante ejecutar código de script arbitrario en el contexto de la interfaz afectada o acceder a información confidencial basada en el navegador. Para aprovechar esta vulnerabilidad, el atacante necesita credenciales de administrador válidas.

Productos Afectados

Cisco Unified CCX Software, versiones anteriores a 12.0(1) ES02.

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-ccx-xss

---

Vulnerabilidad

CVE-2019-1883

Impacto

Una vulnerabilidad en la interfaz de línea de comandos de Cisco Integrated Management Controller (IMC) podría permitir que un atacante local autenticado con credenciales de solo lectura inyecte comandos arbitrarios que podrían permitirles obtener privilegios de root.

La vulnerabilidad se debe a una validación insuficiente de la entrada proporcionada por el usuario en la interfaz de línea de comandos. Un atacante podría aprovechar esta vulnerabilidad autenticándose con privilegios de solo lectura a través de la CLI de un dispositivo afectado y enviando una entrada diseñada a los comandos afectados. Una explotación exitosa podría permitir a un atacante ejecutar comandos arbitrarios en el dispositivo con privilegios de root.

Productos Afectados

- UCS C-Series and S-Series Servers en modo standalone que corran Cisco IMC Software versiones anteriores a 3.0 y 4.0.
- UCS E-Series Servers que ejecuten Cisco IMC Software versiones anteriores a 3.2(8).
- 5000 Series Enterprise Network Compute System (ENCS) Platforms que estén ejecutando Cisco IMC Software versiones anteriores a 3.2(8).

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-cimc-cli-inject

---

Vulnerabilidad

CVE-2019-12627

Impacto

Una vulnerabilidad en la configuración de la política de aplicación del software Cisco Firepower Threat Defense (FTD) podría permitir que un atacante remoto no autenticado obtenga acceso de lectura no autorizado a datos confidenciales.

La vulnerabilidad se debe a la identificación insuficiente de la aplicación. Un atacante podría aprovechar esta vulnerabilidad enviando tráfico diseñado a un dispositivo afectado. Una explotación exitosa podría permitir al atacante obtener acceso de lectura no autorizado a datos confidenciales.

Productos Afectados

Cisco FTD Software versiones anteriores a 6.4.0.4.

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-frpwr-td-info

---

Vulnerabilidad

CVE-2019-12621

Impacto

Una vulnerabilidad en el software Cisco HyperFlex podría permitir que un atacante remoto no autenticado realice un ataque man-in-the-middle.

La vulnerabilidad se debe a una gestión de claves insuficiente. Un atacante podría aprovechar esta vulnerabilidad al obtener una clave de cifrado específica para el clúster. Una explotación exitosa podría permitir al atacante realizar un ataque de hombre en el medio contra otros nodos en el clúster.

Productos Afectados

Cisco HyperFlex Software, versiones anteriores a 4.0(1a).

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-hyperflex-sslkey

---

Vulnerabilidad
CVE-2019-1871

Impacto

Una vulnerabilidad en la utilidad de configuración Import Cisco IMC de Cisco Integrated Management Controller (IMC) podría permitir que un atacante remoto autenticado cause una

condición de denegación de servicio (DoS) e implemente comandos arbitrarios con privilegios de root en un dispositivo afectado.

La vulnerabilidad se debe a una comprobación incorrecta de los límites por parte del proceso import-config. Un atacante podría aprovechar esta vulnerabilidad enviando paquetes maliciosos a un dispositivo afectado. Cuando se procesan los paquetes, puede ocurrir una condición de desbordamiento de búfer explotable. Una explotación exitosa podría permitir al atacante implementar código arbitrario en el dispositivo afectado con privilegios elevados.

Productos Afectados

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

- UCS C-Series y S-Series Servers en modo standalone.
- UCS E-Series Servers
- 5000 Series Enterprise Network Compute System (ENCS) Platform

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-bo

---

Vulnerabilidad

CVE-2019-1850

Impacto

Una vulnerabilidad en la interfaz de administración basada en la web del software Cisco Integrated Management Controller (IMC) podría permitir que un atacante remoto autenticado inyecte comandos arbitrarios que se ejecutan con privilegios de root en un dispositivo afectado. Un atacante necesitaría tener credenciales de administrador válidas en el dispositivo.

La vulnerabilidad se debe a una validación insuficiente de las entradas proporcionadas por el usuario por el software afectado. Un atacante con privilegios elevados podría aprovechar esta vulnerabilidad enviando comandos diseñados a la interfaz administrativa de administración web del software afectado. Una explotación exitosa podría permitir al atacante inyectar y ejecutar comandos arbitrarios a nivel de sistema con privilegios de root en un dispositivo afectado.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco:

- UCS C-Series y S-Series Servers en modo standalone ejecutando Cisco IMC Software versiones anteriores a 3.0 y 4.0.

- UCS E-Series Servers que estén ejecutando Cisco IMC Software versiones anteriores a 3.2(8).
- 5000 Series Enterprise Network Compute System (ENCS) Platforms que estén ejecutando Cisco IMC Software versiones anteriores a 3.2(8).

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-cmdinj-1850

Vulnerabilidad

CVE-2019-1864

Impacto

Una vulnerabilidad en la interfaz de administración basada en la web del software Cisco Integrated Management Controller (IMC) podría permitir que un atacante remoto autenticado inyecte comandos arbitrarios que se ejecutan con privilegios de root en un dispositivo afectado.

La vulnerabilidad se debe a una validación insuficiente de la entrada de comandos por parte del software afectado. Un atacante podría aprovechar esta vulnerabilidad enviando comandos maliciosos a la interfaz de administración basada en web del software afectado. Una explotación exitosa podría permitir al atacante, con privilegios de solo lectura, inyectar y ejecutar comandos arbitrarios a nivel de sistema con privilegios de root en un dispositivo afectado.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco:

- UCS C-Series y S-Series Servers en modo standalone ejecutando Cisco IMC Software versiones 1.4 – 1.5 – 2.0 - 3.0 - 4.0.
- UCS E-Series Servers que estén ejecutando Cisco IMC Software versiones anteriores a 3.2(8).
- 5000 Series Enterprise Network Compute System (ENCS) Platforms que estén ejecutando Cisco IMC Software versiones anteriores a 3.2(8).

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-cmdinj-1864

Vulnerabilidad

CVE-2019-1865

Impacto

Una vulnerabilidad en la interfaz de administración basada en la web del software Cisco Integrated Management Controller (IMC) podría permitir que un atacante remoto autenticado inyecte comandos arbitrarios que se ejecutan con privilegios de root en un dispositivo afectado.

La vulnerabilidad se debe a una validación insuficiente de las entradas proporcionadas por el usuario por el software afectado. Un atacante podría aprovechar esta vulnerabilidad invocando un mecanismo de monitoreo de interfaz con un argumento diseñado sobre el software afectado. Una explotación exitosa podría permitir al atacante inyectar y ejecutar comandos arbitrarios a nivel de sistema con privilegios de root en un dispositivo afectado.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco:

- UCS C-Series y S-Series Servers en modo standalone ejecutando Cisco IMC Software versiones 1.4 – 1.5 – 2.0 - 3.0 - 4.0.
- UCS E-Series Servers que estén ejecutando Cisco IMC Software versiones anteriores a 3.2(8).
- 5000 Series Enterprise Network Compute System (ENCS) Platforms que estén ejecutando Cisco IMC Software versiones anteriores a 3.2(8).

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-cmdinj-1865

Vulnerabilidad

CVE-2019-1634

Impacto

Una vulnerabilidad en la Interfaz de administración de plataforma inteligente (IPMI) de Cisco Integrated Management Controller (IMC) podría permitir que un atacante remoto autenticado inyecte comandos arbitrarios que se ejecutan con privilegios de root en el sistema operativo (SO) subyacente.

La vulnerabilidad se debe a una validación de entrada insuficiente de los comandos proporcionados por el usuario. Un atacante que tenga privilegios de administrador y acceso a la red donde reside el IPMI podría aprovechar esta vulnerabilidad al enviar una entrada diseñada a los comandos afectados. Una explotación exitosa podría permitir al atacante obtener privilegios de root en el dispositivo afectado.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco:

- UCS C-Series y S-Series Servers en modo standalone ejecutando Cisco IMC Software versiones 1.4 – 1.5 – 2.0 - 3.0 - 4.0.
- UCS E-Series Servers que estén ejecutando Cisco IMC Software versiones anteriores a 3.2(8).
- 5000 Series Enterprise Network Compute System (ENCS) Platforms que estén ejecutando Cisco IMC Software versiones anteriores a 3.2(8).

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-cmdinject-1634

Vulnerabilidad

CVE-2019-1896

Impacto

Una vulnerabilidad en la interfaz web de administración de Cisco Integrated Management Controller (IMC) podría permitir que un atacante remoto autenticado inyecte comandos arbitrarios y obtenga privilegios de root.

La vulnerabilidad se debe a una validación insuficiente de la entrada proporcionada por el usuario en la función de Solicitud de firma de certificado (CSR) de la interfaz web de administración. Un atacante podría aprovechar esta vulnerabilidad al enviar una CSR diseñada en la interfaz de administración basada en la web. Una explotación exitosa podría permitir que un atacante con privilegios de administrador ejecute comandos arbitrarios en el dispositivo con todos los privilegios de root.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco:

- UCS C-Series y S-Series Servers en modo standalone ejecutando Cisco IMC Software versiones 1.4 – 1.5 – 2.0 - 3.0 - 4.0.
- UCS E-Series Servers que estén ejecutando Cisco IMC Software versiones anteriores a 3.2(8).

- 5000 Series Enterprise Network Compute System (ENCS) Platforms que estén ejecutando Cisco IMC Software versiones anteriores a 3.2(8).

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-cmdinject-1896

Vulnerabilidad

CVE-2019-1900

Impacto

Una vulnerabilidad en el servidor web de Cisco Integrated Management Controller (IMC) podría permitir que un atacante remoto no autenticado provoque el bloqueo del proceso del servidor web, provocando una condición de denegación de servicio (DoS) en un sistema afectado.
La vulnerabilidad se debe a una validación insuficiente de la entrada proporcionada por el usuario en la interfaz web. Un atacante podría aprovechar esta vulnerabilidad al enviar una solicitud HTTP diseñada a ciertos puntos finales del software afectado. Una explotación exitosa podría permitir que un atacante haga que el servidor web se bloquee. Es posible que se requiera acceso físico al dispositivo para reiniciar.
Productos Afectados

Esta vulnerabilidad afecta a los servidores Cisco UCS C-Series y S-Series en modo independiente si están ejecutando una versión 4.0 del software Cisco IMC.

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-dos

---

Vulnerabilidad

CVE-2019-1908

Impacto
Una vulnerabilidad en la implementación de la Interfaz de administración de plataforma inteligente (IPMI) de Cisco Integrated Management Controller (IMC) podría permitir que un atacante remoto no autenticado vea información confidencial del sistema.

La vulnerabilidad se debe a restricciones de seguridad insuficientes impuestas por el software afectado. Una explotación exitosa podría permitir al atacante ver información confidencial que pertenece a otros usuarios. El atacante podría usar esta información para realizar ataques adicionales.

Productos Afectados

Esta vulnerabilidad afecta a los servidores Cisco UCS C-Series y S-Series en modo independiente si están ejecutando la versión 2.0, 3.0 o 4.0 del software Cisco IMC.

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-infodisc
Vulnerabilidad

CVE-2019-1907

Impacto

Una vulnerabilidad en el servidor web de Cisco Integrated Management Controller (IMC) podría permitir que un atacante remoto autenticado establezca valores de configuración confidenciales y obtenga privilegios elevados.

La vulnerabilidad se debe al manejo inadecuado de las operaciones de comparación de subcadenas que realiza el software afectado. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud HTTP diseñada al software afectado. Una explotación exitosa podría permitir al atacante con privilegios de solo lectura obtener privilegios de administrador.

Productos Afectados

Esta vulnerabilidad afecta a los servidores Cisco UCS C-Series y S-Series en modo independiente si están ejecutando una versión 4.0 del software Cisco IMC.

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-privescal

---

Vulnerabilidad

CVE-2019-1863

Impacto

Una vulnerabilidad en la interfaz de administración web del software Cisco Integrated Management Controller (IMC) podría permitir que un atacante remoto autenticado realice cambios no autorizados en la configuración del sistema.

La vulnerabilidad se debe a la insuficiente aplicación de la autorización. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud HTTP diseñada al software afectado. Una explotación exitosa podría permitir a un usuario con privilegios de solo lectura cambiar configuraciones críticas del sistema utilizando privilegios de administrador.

Productos Afectados

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

- UCS C-Series and S-Series Servers en modo standalone, versiones 1.5 – 2.0 – 3.0 – 4.0
- UCS E-Series Servers, Cisco IMC Software veriones anterior a 3.2(8)
- 5000 Series Enterprise Network Compute System (ENCS) Platforms, Cisco IMC Software veriones anterior a 3.2(8)

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-privilege

---

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.

La vulnerabilidad se debe a una validación insuficiente del encabezado de la solicitud durante el proceso de autenticación. Un atacante podría aprovechar esta vulnerabilidad enviando una serie de solicitudes maliciosas a un dispositivo afectado. Un exploit podría permitir al atacante usar el token de sesión adquirido para obtener acceso completo del administrador al dispositivo afectado.

Productos Afectados

- Cisco IMC Supervisor, versiones 2.2.0.3 hasta 2.2.0.6
- Cisco UCS Director, versiones:
  - 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, versiones:
  - 3.6
  - 3.7.0.0 y 3.7.1.0

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

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

---

Vulnerabilidad

CVE-2019-1974

Impacto

Una vulnerabilidad en la interfaz de administración web de Cisco Integrated Management Controller (IMC) Supervisor, Cisco UCS Director, y Cisco UCS Director Express for Big Data podría permitir que un atacante remoto no autenticado omita la autenticación del usuario y obtenga acceso como usuario administrativo.

La vulnerabilidad se debe a una validación insuficiente del encabezado de la solicitud durante el proceso de autenticación. Un atacante podría aprovechar esta vulnerabilidad enviando una serie de solicitudes maliciosas a un dispositivo afectado. Un exploit podría permitir al atacante obtener acceso administrativo completo al dispositivo afectado.

Productos Afectados

- Cisco IMC Supervisor versiones:
  - 2.1
  - 2.2.0.0 hasta 2.2.0.6
- Cisco UCS Director versiones:
  - 5.5.0.0 hasta 5.5.0.2
  - 6.0.0.0 hasta 6.0.1.3
  - 6.5.0.0 hasta 6.5.0.3
  - 6.6.0.0 y 6.6.1.0
  - 6.7.0.0 hasta 6.7.2.0
- Cisco UCS Director Express for Big Data versiones:
  - 2.1.0.0 hasta 2.1.0.2
  - 3.0.0.0 hasta 3.0.1.3
  - 3.5.0.0 hasta 3.5.0.3
  - 3.6.0.0 y 3.6.1.0
  - 3.7.0.0 hasta 3.7.2.0

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

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

---

Vulnerabilidad

CVE-2019-1936

Impacto

Una vulnerabilidad en la interfaz de administración basada en la 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.

La vulnerabilidad se debe a una validación insuficiente de la entrada proporcionada por el usuario por la interfaz de administración basada en la web. Un atacante podría aprovechar esta vulnerabilidad iniciando sesión en la interfaz de administración basada en la web con privilegios de administrador y luego enviando una solicitud maliciosa a cierta parte de la interfaz.

Productos Afectados

- Cisco IMC Supervisor versiones:
  - 2.1
  - 2.2.0.0 hasta 2.2.0.6
- Cisco UCS Director versiones:
  - 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 versiones:
  - 3.0
  - 3.5
  - 3.6
  - 3.7.0.0 y 3.7.1.0

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

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

---

Vulnerabilidad

CVE-2019-1935

Impacto

Una vulnerabilidad en 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 inicie sesión en la CLI de un sistema afectado utilizando la cuenta de usuario SCP (scpuser) , que tiene credenciales de usuario predeterminadas.

La vulnerabilidad se debe a la presencia de una cuenta predeterminada documentada con una contraseña predeterminada no documentada y una configuración de permisos incorrecta para esa cuenta. El cambio de la contraseña predeterminada para esta cuenta no se aplica durante la instalación del producto. Un atacante podría aprovechar esta vulnerabilidad utilizando la cuenta para iniciar sesión en un sistema afectado. Una explotación exitosa podría permitir al atacante ejecutar comandos arbitrarios con los privilegios de la cuenta scpuser. Esto incluye acceso completo de lectura y escritura a la base de datos del sistema.

Productos Afectados

- Cisco IMC Supervisor versiones:
  - 2.1
  - 2.2.0.0 hasta 2.2.0.6
- Cisco UCS Director versiones:
  - 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 versiones:
  - 3.0
  - 3.5
  - 3.6
  - 3.7.0.0 y 3.7.1.0

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

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

---

Vulnerabilidad

CVE-2019-12624

Impacto

Una vulnerabilidad en la interfaz de administración web deCisco IOS XE New Generation Wireless Controller (NGWC) podría permitir que un atacante remoto no autenticado realice un ataque de falsificación de solicitud entre sitios (CSRF) y realice acciones arbitrarias en un dispositivo afectado.

La vulnerabilidad se debe a las insuficientes protecciones CSRF para la interfaz de administración basada en web del software afectado. Un atacante podría aprovechar esta vulnerabilidad persuadiendo a un usuario de la interfaz para que siga un enlace diseñado. Una explotación exitosa podría permitir al atacante realizar acciones arbitrarias en un dispositivo afectado mediante el uso de un navegador web y con los privilegios del usuario.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a los siguientes productos de Cisco si ejecutaban alguna de las versiones 3.xE del software Cisco IOS XE:

- 5760 Wireless LAN Controllers
- Catalyst 3650 Series Switches
- Catalyst 3850 Series Switches
- Catalyst 4500E Supervisor Engine 8-E (Wireless) Switches

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-iosxe-ngwc-csrf

---

Vulnerabilidad

CVE-2019-12623

Impacto
Una vulnerabilidad en la funcionalidad del servidor web de Cisco Enterprise Network Functions Virtualization Infrastructure Software (NFVIS) podría permitir que un atacante remoto autenticado realice una enumeración de archivos en un sistema afectado.

La vulnerabilidad se debe a que el servidor web responde con diferentes códigos de error para archivos existentes y no existentes. Un atacante podría aprovechar esta vulnerabilidad enviando solicitudes GET para diferentes nombres de archivo. Una explotación exitosa podría permitir al atacante enumerar los archivos que residen en el sistema.

Productos Afectados
Cisco Enterprise Network Compute Systems que estén corriendo NFVIS versiones anteriores a 3.12.1.

Mitigación

Instalar las actualizaciones indicadas por el fabricante.
Enlace
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-nfv-enumeration

---

Vulnerabilidad

CVE-2019-1984

Impacto

Una vulnerabilidad en Cisco Enterprise Network Functions Virtualization Infrastructure Software (NFVIS) podría permitir que un atacante remoto autenticado con privilegios de administrador sobrescriba archivos en el sistema operativo (SO) subyacente de un dispositivo afectado.

La vulnerabilidad se debe a una validación de entrada incorrecta en un comando del sistema de archivos NFVIS. Un atacante podría aprovechar esta vulnerabilidad mediante el uso de variables diseñadas durante la ejecución de un comando afectado. Una explotación exitosa podría permitir al atacante sobrescribir archivos arbitrarios en el sistema operativo subyacente.

Productos Afectados

Cisco Enterprise Network Compute Systems que estén corriendo NFVIS versiones anteriores a 3.12.1.

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-nfv-filewrite

---

Vulnerabilidad

CVE-2019-12622

Impacto

Una vulnerabilidad en el software Cisco RoomOS podría permitir que un atacante local autenticado escriba archivos en el sistema de archivos subyacente con privilegios de root.

La vulnerabilidad se debe a restricciones de permisos insuficientes en un proceso específico. Un atacante podría aprovechar esta vulnerabilidad iniciando sesión en un dispositivo afectado con credenciales de soporte remoto e iniciando el proceso específico en el dispositivo y enviando datos diseñados a ese proceso. Una explotación exitosa podría permitir al atacante escribir archivos en el sistema de archivos subyacente con privilegios de root.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones del software Cisco RoomOS anteriores a la versión ce-9.7.3

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-roomos-privesc

---

Vulnerabilidad

CVE-2019-1839

Impacto

Una vulnerabilidad en el software del dispositivo Cisco Remote PHY podría permitir que un atacante local autenticado ejecute comandos en el shell Linux subyacente de un dispositivo afectado con privilegios de root.

La vulnerabilidad se produce porque el software afectado desinfecta incorrectamente las entradas proporcionadas por el usuario. Un atacante que tenga acceso válido de administrador a un dispositivo afectado podría aprovechar esta vulnerabilidad al proporcionar varios comandos CLI con argumentos diseñados. Un exploit exitoso podría permitir al atacante ejecutar comandos arbitrarios como usuario root, lo que permitiría un compromiso total del sistema.

Productos Afectados

- Remote PHY 120 versiones anterior a 6.4
- Remote PHY 220 versiones anterior a 3.1
- Remote PHY Shelf 7200 versiones anterior a 1.2

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

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

---

Vulnerabilidad

CVE-2019-1885

Impacto
Una vulnerabilidad en el protocolo Redfish de Cisco Integrated Management Controller (IMC) podría permitir que un atacante remoto autenticado inyecte y ejecute comandos arbitrarios con privilegios de root en un dispositivo afectado.

La vulnerabilidad se debe a una validación insuficiente de las entradas proporcionadas por el usuario por el software afectado. Un atacante podría aprovechar esta vulnerabilidad enviando comandos autenticados diseñados a la interfaz de administración basada en web del software afectado. Una explotación exitosa podría permitir al atacante inyectar y ejecutar comandos arbitrarios en un dispositivo afectado con privilegios de root.

Productos Afectados

Esta vulnerabilidad afecta a los servidores Cisco UCS C-Series y S-Series en modo independiente que ejecutan el software Cisco IMC antes de las primeras versiones fijas de 3.0 y 4.0.

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

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

---

Vulnerabilidad

CVE-2019-12634

Impacto

Una vulnerabilidad en la interfaz de administración web de Cisco Integrated Management Controller (IMC) Supervisor, Cisco UCS Director, and Cisco UCS Director Express para Big Data podría permitir que un atacante remoto no autenticado cause una condición de denegación de servicio (DoS).

La vulnerabilidad se debe a una falta de verificación de autenticación en una llamada a la API. Un atacante que puede enviar una solicitud a un sistema afectado podría hacer que todos los usuarios autenticados actualmente cierren sesión. La explotación repetida podría causar la incapacidad de mantener una sesión en el portal de administración basado en la web.

Productos Afectados

- Versiones de Cisco IMC Supervisor:
  - 2.2.0.3 a 2.2.0.6
- Versiones de Cisco UCS Director:
  - 6.6.0.0 y 6.6.1.0

    - 6.7.0.0 a 6.7.2.0
- Cisco UCS Director Express para versiones de Big Data:
    - 3.6.0.0 y 3.6.1.0
    - 3.7.0.0 a 3.7.2.0

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-ucs-imc-dos

---

Vulnerabilidad

CVE-2019-1938

Impacto

Una vulnerabilidad en la interfaz de administración web de Cisco UCS Director y Cisco UCS Director Express para Big Data podría permitir que un atacante remoto no autenticado omita la autenticación y ejecute acciones arbitrarias con privilegios de administrador en un sistema afectado.

La vulnerabilidad se debe al manejo incorrecto de la solicitud de autenticación. Un atacante podría aprovechar esta vulnerabilidad enviando solicitudes HTTP diseñadas a un dispositivo afectado. Un exploit exitoso podría permitir que un atacante sin privilegios acceda y ejecute acciones arbitrarias a través de ciertas API.

Productos Afectados

- UCS Director versiones 6.7.0.0 y 6.7.1.0
- UCS Director Express for Big Data versiones 3.7.0.0 y 3.7.1.0

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-ucsd-authbypass

---

Vulnerabilidad

CVE-2019-1948

Impacto

Una vulnerabilidad en Cisco Webex Meetings Mobile (iOS) podría permitir que un atacante remoto no autenticado obtenga acceso de lectura no autorizado a datos confidenciales mediante el uso de un certificado SSL (Secure Sockets Layer) no válido.

La vulnerabilidad se debe a una validación insuficiente del certificado SSL por parte del software afectado. Un atacante podría aprovechar esta vulnerabilidad al proporcionar un certificado SSL diseñado a un dispositivo afectado. Una explotación exitosa podría permitir al atacante realizar ataques de hombre en el medio para descifrar información confidencial sobre las conexiones de los usuarios con el software afectado.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco Webex Meetings Mobile (iOS) 11.3 a 39.5 si se ejecutaban en un iPhone, iPad o iPod touch.

Mitigación

Instalar las actualizaciones indicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-webex-ssl-cert

CSIRT
Gobierno
de Chile

Firmado
digitalmente por
CSIRT Gobierno de
Chile
Fecha: 2019.08.23
19:44:32 -04'00'