Vulnerabilidades en Cisco Integrated Management Controller

CYBERZAINTZA-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que la Agencia de Ciberseguridad Vasca considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso la Agencia de Ciberseguridad Vasca puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de la Agencia de Ciberseguridad Vasca como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de la Agencia de Ciberseguridad Vasca. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

1. Resumen ejecutivo

Cisco ha publicado avisos de seguridad para tratar **2 vulnerabilidades** de **severidad alta** cuyos identificadores son CVE-2024-20295 y CVE-2024-20356, que afectan a **Cisco Integrated Management Controller.** Su explotación supone una **amenaza de alta gravedad para la confidencialidad y la integridad** de los sistemas que se vean afectados.

El Equipo de Respuesta a Incidentes de Seguridad de Productos de Cisco (PSIRT) no tiene conocimiento de divulgación o uso malicioso de las vulnerabilidades descritas.

El fabricante ya ha publicado las actualizaciones y medidas de mitigación correspondientes, corrigiendo de esta manera el fallo destacado. Por lo que, para prevenir esta y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen los parches correspondientes.

2. Recursos afectados

Los recursos afectados por la vulnerabilidad CVE-2024-20356 son:

- 5000 Series Enterprise Network Compute Systems (ENCS).
- Catalyst 8300 Series Edge uCPE.
- UCS C-Series M5, M6, and M7 Rack Servers in standalone mode.
- UCS E-Series Servers.
- UCS S-Series Storage Servers in standalone mode.

Así mismo, según informa Cisco, también se ven afectados por esta vulnerabilidad los dispositivos de Cisco que se basan en una versión preconfigurada de uno de los Servidores de la Serie C de Cisco UCS que se encuentran en la lista anterior si exponen acceso a la interfaz de usuario de Cisco IMC. En el momento de la publicación, esto incluía los siguientes productos de Cisco:

- Application Policy Infrastructure Controller (APIC) Servers.
- Business Edition 6000 and 7000 Appliances.
- Catalyst Center Appliances, formerly DNA Center.
- Cloud Services Platform (CSP) 5000 Series.
- Common Services Platform Collector (CSPC) Appliances.
- Connected Mobile Experiences (CMX) Appliances.
- Connected Safety and Security UCS Platform Series Servers.
- Cyber Vision Center Appliances.
- Expressway Series Appliances.
- HyperFlex Edge Nodes.
- HyperFlex Nodes in HyperFlex Datacenter without Fabric Interconnect (DC-NO-FI) deployment mode.
- IEC6400 Edge Compute Appliances.
- IOS XRv 9000 Appliances.
- Meeting Server 1000 Appliances.
- Nexus Dashboard Appliances.
- Prime Infrastructure Appliances.
- Prime Network Registrar Jumpstart Appliances.
- Secure Email Gateways1.
- Secure Email and Web Manager1.
- Secure Endpoint Private Cloud Appliances.
- Secure Firewall Management Center Appliances, formerly Firepower Management Center.
- Secure Malware Analytics Appliances.
- Secure Network Analytics Appliances.
- Secure Network Server Appliances.
- Secure Web Appliances1.
- Secure Workload Servers.
- Telemetry Broker Appliances.

Los recursos afectados por la vulnerabilidad CVE-2024-20295 son los siguientes:

- 5000 Series Enterprise Network Compute Systems (ENCS).
- Catalyst 8300 Series Edge uCPE.
- UCS C-Series Rack Servers in standalone mode.
- UCS E-Series Servers.

Así mismo, cisco informa que los dispositivos de Cisco que se basan en una versión preconfigurada de un Servidor de la Serie C de Cisco UCS también se ven afectados si exponen acceso a la interfaz de línea de comandos (CLI) de Cisco IMC, los recursos afectados son:

- 5520 and 8540 Wireless Controllers.
- Application Policy Infrastructure Controller (APIC) Servers.
- Business Edition 6000 and 7000 Appliances.
- Catalyst Center Appliances, formerly DNA Center (DNAC).
- Cloud Services Platform (CSP) 5000 Series.
- Common Services Platform Collector (CSPC) Appliances.
- Connected Mobile Experiences (CMX) Appliances.
- Connected Safety and Security UCS Platform Series Servers.
- Cyber Vision Center Appliances.
- Expressway Series Appliances.
- HyperFlex Edge Nodes.
- HyperFlex Nodes in HyperFlex Datacenter without Fabric Interconnect (DC-NO-FI) deployment mode.
- IEC6400 Edge Compute Appliances.
- IOS XRv 9000 Appliances.
- Meeting Server 1000 Appliances.
- Nexus Dashboard Appliances.
- Prime Infrastructure Appliances.
- Prime Network Registrar Jumpstart Appliances.
- Secure Email Gateways1.
- Secure Email and Web Manager1.
- Secure Endpoint Private Cloud Appliances.
- Secure Firewall Management Center Appliances, formerly Firepower Management Center.
- Secure Malware Analytics Appliances.
- Secure Network Analytics Appliances.
- Secure Network Server Appliances.
- Secure Web Appliances 1.
- Secure Workload Servers.
- Telemetry Broker Appliances.

3. Análisis técnico

Los detalles de la vulnerabilidad tratada en este aviso son los siguientes:

CVE-2024-20295: vulnerabilidad en la interfaz de línea de comandos (CLI) del Controlador de Gestión Integrado (IMC) de Cisco que podría permitir a un atacante autenticado y local realizar ataques de inyección de comandos en el sistema operativo subyacente y elevar los privilegios a root. Para explotar esta vulnerabilidad, el atacante debe tener privilegios de solo lectura o superiores en un dispositivo afectado.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 78: Improper Neutralization of Special Elements used in an OS Command (OS Command Injection)

CVSS Base: **8.8**

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

- **Vector de ataque**: Local
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Bajos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2024-20356: vulnerabilidad en la interfaz de gestión basada en web del Controlador de Gestión Integrado (IMC) de Cisco que podría permitir a un atacante remoto autenticado con privilegios de administrador realizar ataques de inyección de comandos en un sistema afectado y elevar sus privilegios a root. Esta vulnerabilidad se debe a una validación insuficiente de la entrada del usuario. Un atacante podría explotar esta vulnerabilidad enviando comandos manipulados a la interfaz de gestión basada en web del software afectado. Un exploit exitoso podría permitir al atacante elevar sus privilegios a root.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 78: Improper Neutralization of Special Elements used in an OS Command (OS Command Injection)

CVSS Base: **8.7**

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos:** Altos

- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad:** Ninguno

4. Mitigación / Solución

Como es habitual, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

En el caso de la vulnerabilidad CVE-2024-20295 cisco recomienda actualizar a una versión corregida tal y como se indica a continuación:

Cisco 5000 Series ENCS and Catalyst 8300 Series Edge uCPE:

La actualización de Cisco IMC en Cisco 5000 Series ENCS y Cisco Catalyst 8300 Series Edge uCPE requiere la actualización del Software de Infraestructura de Virtualización de Funciones de Red (NFVIS) de Cisco en las plataformas. Cisco IMC se actualiza como parte del proceso de actualización automática del firmware.

- Cisco NFVIS 3.12 y anteriores, migrar a una versión corregida.
- Cisco NFVIS 4.13 y anterior, migrar a la versión 4.14.1.

Cisco UCS C-Series M4 Rack Server:

- Cisco IMC 4.0 y anteriores, se recomienda migrar a una versión corregida.
- Cisco IMC 4.1 se recomienda actualizar a la versión 4.1(2m)

Cisco UCS C-Series M5 Rack Server

- Cisco IMC 4.0 y anteriores, se recomienda migrar a una versión corregida.
- Cisco IMC 4.1 y anteriores migrar a la versión 4.1 (3m).
- Cisco IMC 4.2 y anteriores migrar a la versión 4.2 (3j).
- Cisco IMC 4.3 y anteriores migrar a la versión 4.3 (2.240002).

Cisco UCS C-Series M6 Rack Server

- Cisco IMC 4.2, se recomienda migrar a la versión corregida 4.2(3j).
- Cisco IMC 4.3, se recomienda migrar a la versión corregida 4.3(2.240002).

Cisco UCS C-Series M7 Rack Server

- Cisco IMC 4.3, se recomienda migrar a la versión 4.3(2.240002).

Cisco UCS E-Series M2 and M3

- Cisco IMC 3.2.4 y anteriores no son vulnerables.
- Cisco IMC 3.2.6 y posteriores, se recomienda migrar a la versión 3.2.15.

Cisco UCS E-Series M6

Cisco IMC 4.12 y anteriores, se recomienda migrar a la versión 4.12.2.

Para los dispositivos de Cisco que se basan en una versión preconfigurada de un Servidor de la Serie C de Cisco UCS, los administradores pueden realizar una actualización directa del software de Cisco IMC a una de las versiones corregidas mencionadas anteriormente.

No obstante, existen excepciones en el caso de algunos dispositivos, como es el caso de los que se enumeran a continuación:

IEC6400 Edge Compute Appliances

- La primera versión corregida de Cisco IMC es la 4.2 (3j), como medida de remediación cisco recomienda aplicar la actualización HUU utilizando **IEC6400-HUU-4.2.3j.img**.

Secure Email Gateways

- La primera versión corregida de Cisco IMC es la 4.2 (3j), como medida de remediación cisco recomienda Instalar el paquete de actualización de firmware (Mayo de 2024).

Secure Email and Web Manager

- La primera versión corregida de Cisco IMC es la 4.2 (3j), como medida de remediación cisco recomienda Instalar el paquete de actualización de firmware (Mayo de 2024).

Secure Endpoint Private Cloud Appliances

- La primera versión corregida de Cisco IMC es la 4.3(2.240009), como medida de remediación cisco recomienda Instalar el paquete de actualización de firmware **ucs-firmware-4.3.2.240009-1.rpm** (May 2024).

Secure Firewall Management Center Appliances

- La primera versión corregida de Cisco IMC es la 4.3(2.240009), como medida de remediación cisco recomienda aplicar Hotfix EZ.

Secure Malware Analytics Appliances

- La primera versión corregida de Cisco IMC es la 4.3(2.240009), como medida de remediación se recomienda actualizar a la versión 2.19.3 (Julio 2024).

Secure Network Analytics Appliances

- Para la versión corregida 4.1(2m)(M4) de Cisco IMC, cisco recomienda aplicar le actualización **ucs-c220m4-huu-4.1.2m-sna.iso** or **ucs-c240m4-huu-4.1.2m-sna.iso** (M4).

- Para versión corregida de Cisco IMC es la 4.3(2.240009), como medida de remediación se recomienda instalar el parche de actualización **patch-common-SNA-FIRMWARE-20240305-v2-01.swu**.

Secure Network Server Appliances

- La primera versión corregida de Cisco IMC es la 4.3(2.240009), como medida de remediación cisco recomienda aplicar la actualización del BIOS y HUU según lo documentado en la Guía de Actualización de Firmware para la Serie SNS 3700 o la Serie SNS 3600.

Secure Web Appliances

- La primera versión corregida de Cisco IMC es la 4.2 (3j), como medida de remediación cisco recomienda instalar el paquete de actualización de firmware (Mayo 2024).

Telemetry Broker Appliances

- La primera versión corregida de Cisco IMC es la 4.3(2.240009), como medida de remediación cisco recomienda aplicar el parche de actualización **patch-common-CTB-FIRMWARE-20240305.iso**.

En el caso de la vulnerabilidad CVE-2024-20356, se recomienda a los clientes actualizar a una versión de software corregida apropiada según se indica a continuación:

5000 Series ENCS and Catalyst 8300 Series Edge uCPE

- Cisco NFVIS 3.12 y anteriores, migrar a una versión corregida.
- Cisco NFVIS 4.13 y anterior, migrar a la versión 4.14.1.

UCS C-Series M5 Rack Server

- Cisco IMC 4.0 y anteriores, se recomienda migrar a una versión corregida.
- Cisco IMC 4.1 y anteriores migrar a la versión 4.1 (3m).
- Cisco IMC 4.2 y anteriores migrar a la versión 4.2 (3j).
- Cisco IMC 4.3 y anteriores migrar a la versión 4.3 (2.240002).

UCS C-Series M6 Rack Server

- Cisco IMC 4.2, se recomienda migrar a la versión corregida 4.2(3j).
- Cisco IMC 4.3, se recomienda migrar a la versión corregida 4.3(2.240002).

UCS C-Series M7 Rack Server

- Cisco IMC 4.3, se recomienda migrar a la versión 4.3(2.240002).

UCS E-Series M2 and M3 Server

- Para Cisco IMC 3.1 y versiones anteriores, se recomienda migrar a una versión corregida.
- Para la versión 3.2 de Cisco IMC, se recomienda migrar a la versión 3.2.15.3.

UCS E-Series M6 Server

- En el caso de la versión 4.12 de Cisco IMC y anteriores, se recomienda migrar a la versión 4.12.2.

UCS S-Series Storage Server

- En el caso de la versión 4.0 de Cisco IMC se recomienda migrar a una versión corregida.
- En el caso de la versión 4.1 de Cisco IMC, la primera versión corregida es la 4.1(3n).
- En el caso de la versión 4.2 de Cisco IMC, la primera versión corregida es la 4.2(3k).
- En el caso de la versión 4.3 de Cisco IMC, las versiones corregidas son la 4.3(2.240009) y la versión 4.3(3.240041).

Para los dispositivos de Cisco que se basan en una versión preconfigurada de uno de los Servidores de la Serie C de Cisco UCS mostrados anteriormente, los administradores pueden realizar una actualización directa del software de Cisco IMC a una de las versiones corregidas mencionadas. Para obtener instrucciones, consultar la Guía del usuario de la Utilidad de Actualización de Host de Cisco. Las excepciones son los dispositivos que se enumeran a continuación:

IEC6400 Edge Compute Appliances

- La primera versión corregida de Cisco IMC es la 4.2 (3j), como medida de remediación cisco recomienda aplicar la actualización HUU utilizando **IEC6400-HUU-4.2.3j.img**.

Secure Email Gateways

- La primera versión corregida de Cisco IMC es la 4.2 (3j), como medida de remediación cisco recomienda Instalar el paquete de actualización de firmware (Mayo de 2024).

Secure Email and Web Manager

- La primera versión corregida de Cisco IMC es la 4.2 (3j), como medida de remediación cisco recomienda Instalar el paquete de actualización de firmware (Mayo de 2024).

Secure Endpoint Private Cloud Appliances

- La primera versión corregida de Cisco IMC es la 4.3(2.240009), como medida de remediación cisco recomienda Instalar el paquete de actualización de firmware **ucs-firmware-4.3.2.240009-1.rpm** (May 2024).

Secure Firewall Management Center Appliances

- La primera versión corregida de Cisco IMC es la 4.3(2.240009), como medida de remediación cisco recomienda aplicar Hotfix EZ.

Secure Malware Analytics Appliances

- La primera versión corregida de Cisco IMC es la 4.3(2.240009), como medida de remediación se recomienda actualizar a la versión 2.19.3 (Julio 2024).

Secure Network Analytics Appliances

- Para versión corregida de Cisco IMC es la 4.3(2.240009), como medida de remediación se recomienda instalar el parche de actualización **patch-common-SNA-FIRMWARE-20240305-v2-01.swu**.

Secure Network Server Appliances

- La primera versión corregida de Cisco IMC es la 4.3(2.240009), como medida de remediación cisco recomienda aplicar la actualización del BIOS y HUU según lo documentado en la Guía de Actualización de Firmware para la Serie SNS 3700 o la Serie SNS 3600.

Secure Web Appliances

- La primera versión corregida de Cisco IMC es la 4.2 (3j), como medida de remediación cisco recomienda instalar el paquete de actualización de firmware (Mayo 2024).

Telemetry Broker Appliances

- La primera versión corregida de Cisco IMC es la 4.3(2.240009), como medida de remediación cisco recomienda aplicar el parche de actualización **patch-common-CTB-FIRMWARE-20240305.iso**.

5. Referencias Adicionales

- Avisos de seguridad.
- CVE-2024-20356.
- CVE-2024-20295


cyber
zaintza
BASQUE CYBERSECURITY AGENCY