Alerta de seguridad cibernética	9VSA20-00322-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de noviembre de 2020
Última revisión	18 de noviembre de 2020

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 a 21 vulnerabilidades que afectan a sus productos, de las cuales 3 de ellas están clasificadas como Críticas, 5 como Altas y 13 como medias. El presente informe incluye las respectivas medidas de mitigación.

Vulnerabilidades

Críticas
CVE-2020-3531
CVE-2020-3586
CVE-2020-3470

Altas
CVE-2020-3392
CVE-2020-26072
CVE-2020-3367
CVE-2020-3284
CVE-2020-27131

Medias
CVE-2020-3482
CVE-2020-26077
CVE-2020-26078
CVE-2020-26079
CVE-2020-26075
CVE-2020-26076
CVE-2020-26080

CVE-2020-26081
CVE-2020-26068
CVE-2020-3419
CVE-2020-3471
CVE-2020-3441
CVE-2020-27126

CVE-2020-27131

Impacto
Varias vulnerabilidades en la función de deserialización de Java que utiliza Cisco Security Manager podrían permitir que un atacante remoto no autenticado ejecute comandos arbitrarios en un dispositivo afectado.

Estas vulnerabilidades se deben a la deserialización insegura del contenido proporcionado por el usuario por parte del software afectado. Un atacante podría aprovechar estas vulnerabilidades enviando un objeto Java serializado malicioso a un oyente específico en un sistema afectado. Un exploit exitoso podría permitir al atacante ejecutar comandos arbitrarios en el dispositivo con los privilegios de NT AUTHORITY\SYSTEM en el host de destino de Windows.

Productos Afectados
Estas vulnerabilidades afectan a las versiones 4.22 y anteriores de Cisco Security Manager.

Mitigación
Aplicar las actualizaciones publicadas por el fabricante.

Enlace
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csm-java-rce-mWJEedcD

CVE-2020-3284

Impacto
Una vulnerabilidad en el cargador de arranque mejorado Preboot eXecution Environment (PXE) para el software Cisco IOS XR de 64 bits podría permitir que un atacante remoto no autenticado ejecute código sin firmar durante el proceso de arranque PXE en un dispositivo afectado. El cargador de arranque PXE es parte del BIOS y se ejecuta en la interfaz de administración de las plataformas de hardware que ejecutan únicamente el software Cisco IOS XR.

La vulnerabilidad existe porque los comandos internos que se emiten cuando el proceso de inicio de la red PXE está cargando una imagen de software no se verifican correctamente. Un atacante podría aprovechar esta vulnerabilidad comprometiendo el servidor de arranque PXE y reemplazando una imagen de software válida por una maliciosa. Alternativamente, el atacante podría hacerse pasar por

el servidor de arranque PXE y enviar una respuesta de arranque PXE con un archivo malicioso. Un exploit exitoso podría permitir al atacante ejecutar código sin firmar en el dispositivo afectado.

Productos Afectados

Esta vulnerabilidad afecta a los dispositivos Cisco si ejecutan una versión vulnerable del software Cisco IOS XR de 64 bits y se cumplen las siguientes condiciones:

- El ID de producto (PID) del dispositivo coincide con uno de los PID enumerados en la sección Software fijo de este aviso.
- El dispositivo está ejecutando una versión de BIOS vulnerable.
- El dispositivo usa PXE para el inicio de la red.

El detalle de las versiones afectadas se puede revisar en el enlace.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-pxe-unsign-code-exec-qAa78fD2

CVE-2020-3482

Impacto

Una vulnerabilidad en el componente de servidor Traversal Using Relays around NAT (TURN) del software Cisco Expressway podría permitir que un atacante remoto no autenticado eluda los controles de seguridad y envíe tráfico de red a destinos restringidos.

La vulnerabilidad se debe a una validación incorrecta de información de conexión específica por parte del servidor TURN dentro del software afectado. Un atacante podría aprovechar este problema enviando tráfico de red especialmente diseñado al software afectado. Un exploit exitoso podría permitirle al atacante enviar tráfico a través del software afectado a destinos más allá de la aplicación, posiblemente permitiendo que el atacante obtenga acceso no autorizado a la red.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a Cisco Expressway Series y Cisco TelePresence Video Communication Server (VCS) que ejecutaban una versión de software anterior a la versión X12.6.3.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-Expressway-8J3yZ7hV

CVE-2020-26077

Impacto

Una vulnerabilidad en la funcionalidad de control de acceso de Cisco IoT Field Network Director (FND) podría permitir que un atacante remoto autenticado vea listas de usuarios de diferentes dominios configurados en un sistema afectado.

La vulnerabilidad se debe a un control de acceso inadecuado. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud de API que modifique el dominio de una lista de usuarios solicitada en un sistema afectado. Un exploit exitoso podría permitir al atacante ver listas de usuarios de diferentes dominios en el sistema afectado.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco IoT FND anteriores a la 4.6.1.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-FND-LV-hE4Rntet

CVE-2020-26078

Impacto

Una vulnerabilidad en el sistema de archivos de Cisco IoT Field Network Director (FND) podría permitir a un atacante remoto autenticado sobrescribir archivos en un sistema afectado.

La vulnerabilidad se debe a una protección insuficiente del sistema de archivos. Un atacante podría aprovechar esta vulnerabilidad creando solicitudes de API y enviándolas a un sistema afectado. Un exploit exitoso podría permitir al atacante sobrescribir archivos en un sistema afectado.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco IoT FND anteriores a la 4.6.1.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-FND-OVW-SHzOE3Pd

CVE-2020-26079

Impacto

Una vulnerabilidad en la interfaz de usuario web de Cisco IoT Field Network Director (FND) podría permitir que un atacante remoto autenticado obtenga hash de las contraseñas de los usuarios en un dispositivo afectado.

La vulnerabilidad se debe a una protección insuficiente de las credenciales de usuario. Un atacante podría aprovechar esta vulnerabilidad iniciando sesión como usuario administrativo y creando una llamada para obtener información del usuario. Un exploit exitoso podría permitir al atacante obtener hash de las contraseñas de los usuarios en un dispositivo afectado.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco IoT FND anteriores a la 4.6.1.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-FND-PWH-yCA6M7p

CVE-2020-26075

Impacto

Una vulnerabilidad en la API REST de Cisco IoT Field Network Director (FND) podría permitir que un atacante remoto autenticado obtenga acceso a la base de datos back-end de un dispositivo afectado.

La vulnerabilidad se debe a una validación de entrada insuficiente de las solicitudes de API REST que se realizan a un dispositivo afectado. Un atacante podría aprovechar esta vulnerabilidad creando solicitudes de API maliciosas para el dispositivo afectado. Un exploit exitoso podría permitirle al atacante obtener acceso a la base de datos back-end del dispositivo afectado.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco IoT FND anteriores a la 4.6.1.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-FND-SQL-zEkBnL2h

CVE-2020-26076

Impacto

Una vulnerabilidad en Cisco IoT Field Network Director (FND) podría permitir que un atacante remoto no autenticado vea información confidencial de la base de datos en un dispositivo afectado.

La vulnerabilidad se debe a la ausencia de autenticación de información confidencial. Un atacante podría aprovechar esta vulnerabilidad enviando comandos curl diseñados a un dispositivo afectado. Un exploit exitoso podría permitir al atacante ver información confidencial de la base de datos en el dispositivo afectado.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco IoT FND anteriores a la 4.6.1.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-FND-SSI-V2myWX9y

CVE-2020-26080

Impacto

Una vulnerabilidad en la funcionalidad de administración de usuarios de Cisco IoT Field Network Director (FND) podría permitir que un atacante remoto autenticado administre la información de los usuarios en diferentes dominios en un sistema afectado.

La vulnerabilidad se debe a un control de acceso al dominio inadecuado. Un atacante podría aprovechar esta vulnerabilidad manipulando cargas útiles JSON para apuntar a diferentes dominios en un sistema afectado. Un exploit exitoso podría permitir al atacante administrar la información del usuario para usuarios en diferentes dominios en un sistema afectado.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco IoT FND anteriores a la 4.6.1.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-FND-UPWD-dCRPuQ78

CVE-2020-26081

Impacto

Varias vulnerabilidades en la interfaz de usuario web de Cisco IoT Field Network Director (FND) podrían permitir que un atacante remoto no autenticado lleve a cabo ataques cross-site scripting (XSS) contra usuarios en un sistema afectado.

Las vulnerabilidades se deben a una validación insuficiente de la entrada proporcionada por el usuario que es procesada por la interfaz de usuario web. Un atacante podría aprovechar estas vulnerabilidades persuadiendo a un usuario para que haga clic en un enlace creado. Un exploit exitoso podría permitir al atacante ejecutar código de secuencia de comandos arbitrario en el contexto de la interfaz o acceder a información confidencial basada en el navegador en un sistema afectado.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco IoT FND anteriores a la 4.6.1.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-FND-XSS-NzOPCGEc

CVE-2020-26068

Impacto

Una vulnerabilidad en el servicio xAPI del software Cisco Telepresence CE y el software Cisco RoomOS podría permitir a un atacante remoto autenticado generar un token de acceso para un dispositivo afectado.

La vulnerabilidad se debe a una autorización de acceso insuficiente. Un atacante podría aprovechar esta vulnerabilidad mediante el servicio xAPI para generar un token específico. Un exploit exitoso podría permitir al atacante usar el token generado para habilitar funciones experimentales en el dispositivo que no deberían estar disponibles para los usuarios.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones 9.10 y 9.12 del software Cisco Telepresence CE, en cuanto al software Cisco RoomOS, Cisco ha abordado esta vulnerabilidad en Cisco RoomOS Software RoomOS July Drop 1 2020, que está basado en la nube. No se requiere ninguna acción por parte del usuario. Los clientes pueden determinar el estado actual de la corrección o la versión del software utilizando la función de Ayuda en la GUI del servicio.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tp-uathracc-jWNESUfM

CVE-2020-3419

Impacto

Una vulnerabilidad en Cisco Webex Meetings y Cisco Webex Meetings Server podría permitir que un atacante remoto no autenticado se una a una sesión de Webex sin aparecer en la lista de participantes.

Esta vulnerabilidad se debe al manejo inadecuado de los tokens de autenticación por parte de un sitio de Webex vulnerable. Un atacante podría aprovechar esta vulnerabilidad enviando solicitudes diseñadas a un sitio vulnerable de Cisco Webex Meetings o Cisco Webex Meetings Server. Un exploit exitoso requiere que el atacante tenga acceso para unirse a una reunión de Webex, incluidos los vínculos y las contraseñas correspondientes para unirse a la reunión. El atacante podría aprovechar esta vulnerabilidad para unirse a las reuniones, sin aparecer en la lista de participantes, mientras tiene acceso completo a las capacidades de audio, video, chat y uso compartido de pantalla.

Productos Afectados

Esta vulnerabilidad afectó a todos los sitios de Cisco Webex Meetings antes del 17 de noviembre de 2020. Webex Meetings se basa en la nube.

En el momento de la publicación, esta vulnerabilidad también afectaba a todas las versiones 40.10.9 y anteriores de las aplicaciones de Cisco Webex Meetings para iOS y Android.

En el momento de la publicación, esta vulnerabilidad también afectó a las siguientes versiones de Cisco Webex Meetings Server, que se encuentra en las instalaciones:

- 3.0MR Security Patch 4 y versiones anteriores
- 4.0MR3 Security Patch 3 y versiones anteriores

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-auth-token-3vg57A5r

CVE-2020-3471

Impacto

Una vulnerabilidad en Cisco Webex Meetings y Cisco Webex Meetings Server podría permitir que un atacante remoto no autenticado mantuviera el audio bidireccional a pesar de haber sido expulsado de una sesión activa de Webex.

La vulnerabilidad se debe a un problema de sincronización entre los servicios de reuniones y de medios en un sitio de Webex vulnerable. Un atacante podría aprovechar esta vulnerabilidad enviando solicitudes diseñadas a un sitio vulnerable de Cisco Webex Meetings o Cisco Webex Meetings Server. Un exploit exitoso podría permitir al atacante mantener la conexión de audio de una sesión de Webex a pesar de haber sido expulsado.

Productos Afectados

Esta vulnerabilidad afecta a las siguientes versiones de los sitios de Cisco Webex Meetings. Webex Meetings está basado en la nube.

- WBS 39.5.25 y anteriores
- WBS 40.6.10 y anteriores
- WBS 40.9.5

En el momento de la publicación, esta vulnerabilidad también afectó a las siguientes versiones de Cisco Webex Meetings Server, que se encuentra en las instalaciones:

- 3.0MR3 Security Patch 4 y versiones anteriores
- 4.0MR3 Security Patch 3 y versiones anteriores

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-info-leak-PhpzB3sG

CVE-2020-3441

Impacto

Una vulnerabilidad en Cisco Webex Meetings y Cisco Webex Meetings Server podría permitir que un atacante remoto no autenticado vea información confidencial desde el vestíbulo de la sala de reuniones.

Esta vulnerabilidad se debe a la protección insuficiente de la información confidencial de los participantes. Un atacante podría aprovechar esta vulnerabilidad examinando la lista de Webex. Un exploit exitoso podría permitir al atacante recopilar información sobre otros participantes de Webex, como la dirección de correo electrónico y la dirección IP, mientras espera en el vestíbulo.

Productos Afectados

Esta vulnerabilidad afectó a todos los sitios de Cisco Webex Meetings antes del 17 de noviembre de 2020. Webex Meetings se basa en la nube.

En el momento de la publicación, esta vulnerabilidad también afectó a las siguientes versiones de Cisco Webex Meetings Server, que se encuentra en las instalaciones:

- 3.0MR3 Security Patch 4 y versiones anteriores
- 4.0MR3 Security Patch 3 y versiones anteriores

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-infodisc-4tvQzn4

CVE-2020-27126

Impacto

Una vulnerabilidad en una API de Cisco Webex Meetings podría permitir que un atacante remoto no autenticado lleve a cabo ataques de secuencias de comandos entre sitios.

La vulnerabilidad se debe a una validación incorrecta de la entrada proporcionada por el usuario a una interfaz de programación de aplicaciones (API) dentro de Cisco Webex Meetings. Un atacante podría aprovechar esta vulnerabilidad convenciendo a un usuario objetivo de que siga un vínculo diseñado para enviar información maliciosa a la API utilizada por Cisco Webex Meetings. Un exploit exitoso podría permitir al atacante realizar ataques cross-site scripting y potencialmente obtener acceso a información confidencial basada en el navegador del sistema de un usuario objetivo.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco IoT FND anteriores a la 4.6.1.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-meetings-xss-MX56prER

CVE-2020-3392

Impacto

Una vulnerabilidad en la API de Cisco IoT Field Network Director (FND) podría permitir que un atacante remoto no autenticado vea información confidencial en un sistema afectado.

La vulnerabilidad existe porque el software afectado no autentica correctamente las llamadas a la API. Un atacante podría aprovechar esta vulnerabilidad enviando solicitudes de API a un sistema afectado. Un exploit exitoso podría permitir al atacante ver información confidencial en el sistema afectado, incluida información sobre los dispositivos que administra el sistema, sin autenticación.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco IoT FND anteriores a la 4.6.1.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-FND-APIA-xZntFS2V

CVE-2020-26072

Impacto

Una vulnerabilidad en la API SOAP de Cisco IoT Field Network Director (FND) podría permitir que un atacante remoto autenticado acceda y modifique información en dispositivos que pertenecen a un dominio diferente.

La vulnerabilidad se debe a una autorización insuficiente en la API SOAP. Un atacante podría aprovechar esta vulnerabilidad enviando solicitudes de API SOAP a los dispositivos afectados para dispositivos que están fuera de su dominio autorizado. Un exploit exitoso podría permitir al atacante acceder y modificar información en dispositivos que pertenecen a un dominio diferente.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco IoT FND anteriores a la 4.6.1.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-FND-AUTH-vEypBmmR

CVE-2020-3367

Impacto

Una vulnerabilidad en el subsistema de suscripción de registros de Cisco AsyncOS para Cisco Secure Web Appliance (anteriormente Web Security Appliance) podría permitir a un atacante local autenticado realizar la inyección de comandos y elevar los privilegios a la raíz.

Esta vulnerabilidad se debe a una validación insuficiente de la entrada proporcionada por el usuario para la interfaz web y CLI. Un atacante podría aprovechar esta vulnerabilidad al autenticarse en el dispositivo afectado e inyectar comandos de secuencias de comandos en el ámbito del subsistema de suscripción de registros. Un exploit exitoso podría permitir al atacante ejecutar comandos arbitrarios en el sistema operativo subyacente y elevar los privilegios a root.

Productos Afectados

This vulnerability affects Cisco AsyncOS for the Secure Web Appliance, both virtual and hardware appliances, para ver el detalle de las versiones afectadas se puede consultar en el enlace.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-prv-esc-nPzWZrQj

CVE-2020-3531

Impacto

Una vulnerabilidad en la API REST de Cisco IoT Field Network Director (FND) podría permitir que un atacante remoto no autenticado acceda a la base de datos back-end de un sistema afectado.

La vulnerabilidad existe porque el software afectado no autentica correctamente las llamadas a la API REST. Un atacante podría aprovechar esta vulnerabilidad al obtener un token de falsificación de solicitud entre sitios (CSRF) y luego usar el token con solicitudes de API REST. Un exploit exitoso podría permitir al atacante acceder a la base de datos back-end del dispositivo afectado y leer, alterar o eliminar información.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco IoT FND anteriores a la 4.6.1.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-FND-BCK-GHkPNZ5F

CVE-2020-3586

Impacto

Una vulnerabilidad en la interfaz de administración basada en la web de Cisco DNA Spaces Connector podría permitir que un atacante remoto no autenticado ejecute comandos arbitrarios en un dispositivo afectado.

La vulnerabilidad se debe a una validación insuficiente de la entrada proporcionada por el usuario en la interfaz de administración basada en web. Un atacante podría aprovechar esta vulnerabilidad enviando solicitudes HTTP creadas a la interfaz de administración basada en web. Un exploit exitoso podría permitir al atacante ejecutar comandos arbitrarios en el sistema operativo subyacente con privilegios de la aplicación de administración basada en web, que se ejecuta como un usuario restringido. Esto podría provocar que se realicen cambios en las páginas atendidas por la aplicación de administración basada en web que afecten a la integridad o disponibilidad de la aplicación de administración basada en web.

Productos Afectados

Esta vulnerabilidad afecta a las versiones 2.2 y anteriores del software Cisco DNA Spaces Connector.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dna-cmd-injection-rrAYzOwc

CVE-2020-3470

Impacto

Varias vulnerabilidades en el subsistema API de Cisco Integrated Management Controller (IMC) podrían permitir que un atacante remoto no autenticado ejecute código arbitrario con privilegios de root.

Las vulnerabilidades se deben a comprobaciones de límites inadecuadas para determinadas entradas proporcionadas por el usuario. Un atacante podría aprovechar estas vulnerabilidades enviando una solicitud HTTP diseñada al subsistema API de un sistema afectado. Cuando se procesa esta solicitud, puede ocurrir una condición de desbordamiento de búfer explotable. Un exploit exitoso podría permitir al atacante ejecutar código arbitrario con privilegios de root en el sistema operativo subyacente (SO).

Productos Afectados

Estas vulnerabilidades afectan a los siguientes productos de Cisco si ejecutan una versión vulnerable de Cisco IMC:

- 5000 Series Enterprise Network Compute System (ENCS) Platforms
- UCS C-Series Rack Servers in standalone mode
- UCS E-Series Servers
- UCS S-Series Servers in standalone mode

El detalle del softare afectado se puede consultar en el enlace.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-api-rce-UXwpeDHd