Alerta de seguridad informática	9VSA20-00151-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de marzo de 2020
Última revisión	08 de marzo 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 diversas vulnerabilidades que afectan a sus productos.

Vulnerabilidad

CVE-2020-3164
CVE-2020-3157
CVE-2020-3193
CVE-2020-3192
CVE-2020-3176
CVE-2020-3185
CVE-2020-3182
CVE-2020-3127
CVE-2020-3128
CVE-2020-3148
CVE-2020-3155
CVE-2020-3181
CVE-2020-3166

Vulnerabilidad
CVE-2020-3164

Impacto

Una vulnerabilidad en la interfaz de administración web de Cisco AsyncOS para Cisco Email Security Appliance (ESA), Cisco Web Security Appliance (WSA) y Cisco Content Security Management Appliance (SMA), podría permitir que un atacante remoto no autenticado cause un alto uso de CPU en un dispositivo afectado, lo que resultaría en una condición de denegación de servicio (DoS).

La vulnerabilidad se debe a una validación incorrecta de encabezados de solicitud HTTP específicos. Un atacante podría aprovechar esta vulnerabilidad enviando una solicitud HTTP con formato incorrecto a un dispositivo afectado. Una explotación exitosa podría permitir al atacante activar un estado prolongado de alta utilización de la CPU en relación con los procesos de la GUI. Tras la explotación exitosa de esta vulnerabilidad, un dispositivo afectado seguirá operativo, pero su tiempo de respuesta y rendimiento general pueden verse degradados.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a los siguientes productos de Cisco si ejecutaban una versión de software afectada:

- Cisco ESA y Cisco Cloud Email Security versión 13.0.0-392 y anteriores
- Cisco WSA versión 12.0.1-268 y anterior
- Cisco SMA versiones anteriores a 13.6.0

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cont-sec-gui-dos-nJ625dXb

---

Vulnerabilidad

CVE-2020-3190

Una vulnerabilidad en el procesador de paquetes IPsec del software Cisco IOS XR podría permitir que un atacante remoto no autenticado cause una condición de denegación de servicio (DoS) para sesiones IPsec a un dispositivo afectado.

La vulnerabilidad se debe al manejo inadecuado de los paquetes por parte del procesador de paquetes IPsec. Un atacante podría aprovechar esta vulnerabilidad mediante el envío de mensajes de error ICMP maliciosos a un dispositivo afectado que se someterán al procesador de paquetes IPsec. Una explotación exitosa podría permitir que el atacante agote la memoria de IPsec, lo que resultaría en que todos los futuros paquetes de IPsec enviados a un dispositivo afectado sean descartados por el dispositivo. Se requiere intervención manual para recuperarse de esta situación.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afecta a la versión del software Cisco IOS XR anterior a 6.4.3, 6.6.3, 7.0.2 y 7.1.1, que tienen el proceso IPsec ipsec_mp o ipsec_pp ejecutándose. Ambos procesos IPsec se ejecutan en el software Cisco IOS XR de manera predeterminada.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-ipsec-dos-q8UPX6m

---

Vulnerabilidad

CVE-2020-3157

Una vulnerabilidad en la interfaz de administración web de Cisco Identity Services Engine (ISE) podría permitir que un atacante remoto autenticado realice un ataque cross-site scripting (XSS) contra un usuario de la interfaz web.

La vulnerabilidad se debe a una validación insuficiente de la entrada proporcionada por el usuario a la interfaz de administración web. Un atacante podría aprovechar esta vulnerabilidad creando una configuración maliciosa y guardándola en el sistema de destino. Un exploit 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 cuando un administrador ve la configuración. Un atacante necesitaría permisos de escritura para aprovechar esta vulnerabilidad con éxito.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones 2.7 y anteriores de Cisco ISE.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-BR7nEDjG

Vulnerabilidad

CVE-2020-3193

Una vulnerabilidad en la interfaz de administración web de Cisco Prime Collaboration Provisioning podría permitir que un atacante remoto no autenticado obtenga información confidencial sobre un dispositivo afectado.

La vulnerabilidad existe porque las respuestas de la interfaz de administración web incluyen información innecesaria del servidor. Un atacante podría aprovechar esta vulnerabilidad al inspeccionar las respuestas recibidas de la interfaz de administración basada en la web. Una explotación exitosa podría permitir al atacante obtener detalles sobre el sistema operativo, incluida la versión del servidor web que se ejecuta en el dispositivo, que podría utilizarse para realizar más ataques.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco Prime Collaboration Provisioning 12.6 SU1 y anteriores.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-prim-collab-disclo-FAnX4DKB

Vulnerabilidad

CVE-2020-3192

Una vulnerabilidad en la interfaz de administración web de Cisco Prime Collaboration Provisioning podría permitir que un atacante remoto no autenticado realice un ataque de cross-site scripting (XSS) contra un usuario de la interfaz de administración web.

La vulnerabilidad se debe a una validación insuficiente de la entrada proporcionada por el usuario por la interfaz de administración web. 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 o acceder a información confidencial basada en el navegador.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco Prime Collaboration Provisioning 12.6 SU1 y anteriores.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.
Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-prime-collab-xss-RjRCe9n7

Vulnerabilidad

CVE-2020-3176

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 existe porque el software afectado no desinfecta adecuadamente la entrada proporcionada por el usuario. Un atacante que tenga acceso válido de administrador a un dispositivo afectado podría aprovechar esta vulnerabilidad al proporcionar ciertos comandos CLI con argumentos diseñados. Una explotación exitosa podría permitir al atacante ejecutar comandos arbitrarios como usuario root, lo que podría resultar en un compromiso completo del sistema.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las siguientes versiones de software de Cisco con configuración predeterminada:

- Remote PHY 120: anterior a la versión 7.7

- Remote PHY 220: todos los lanzamientos
- Remote PHY Shelf 7200: todas las versiones

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

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

Vulnerabilidad

CVE-2020-3185
Una vulnerabilidad en la interfaz de administración web de Cisco TelePresence Management Suite (TMS) podría permitir que un atacante remoto autenticado realice un ataque de cross-site scripting (XSS) contra un usuario de la interfaz de administración web.

La vulnerabilidad se debe a una validación de entrada insuficiente por parte de la interfaz de administración web. Un atacante podría aprovechar esta vulnerabilidad insertando datos maliciosos en un campo de datos específico en la interfaz. Una explotación exitosa podría permitir al atacante ejecutar código de script arbitrario en el contexto de la interfaz de administración web afectada o acceder a información confidencial basada en el navegador.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco TMS 15.9.0 y anteriores.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tms-xss-4VXKdLO

Vulnerabilidad

CVE-2020-3182

Una vulnerabilidad en la configuración del protocolo multicast DNS (mDNS) de Cisco Webex Meetings Client para MacOS podría permitir que un atacante adyacente no autenticado obtenga información confidencial sobre el dispositivo en el que se ejecuta el cliente Webex.

La vulnerabilidad existe porque la información confidencial se incluye en la respuesta mDNS. Un atacante podría aprovechar esta vulnerabilidad haciendo una consulta mDNS para un servicio en particular contra un dispositivo afectado. Una explotación exitosa podría permitir al atacante obtener acceso a información confidencial.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a Cisco Webex Meetings Client para MacOS versiones 40.1.8.5 y anteriores.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-info-disc-OHqg982

Vulnerabilidad

CVE-2020-3127
CVE-2020-3128

Dos vulnerabilidades en Cisco Webex Network Recording Player para Microsoft Windows y Cisco Webex Player para Microsoft Windows podrían permitir que un atacante ejecute código arbitrario en un sistema afectado.

Las vulnerabilidades se deben a una validación insuficiente de ciertos elementos dentro de una grabación de Webex que se almacena en el Formato de grabación avanzado (ARF) o el Formato de grabación de Webex (WRF). Un atacante podría explotar estas vulnerabilidades enviando un archivo ARF o WRF malicioso a un usuario a través de un enlace o archivo adjunto de correo electrónico y persuadiendo al usuario para que abra el archivo en el sistema local. Una explotación exitosa podría permitir al atacante ejecutar código arbitrario en el sistema afectado con los privilegios del usuario objetivo.

Productos Afectados

Estas vulnerabilidades afectan las siguientes versiones de Cisco Webex Network Recording Player para Microsoft Windows y Cisco Webex Player para Microsoft Windows, que están disponibles en los sitios de Cisco Webex Meetings, los sitios de Cisco Webex Meetings Online y el Cisco Webex Meetings Server:

- Cisco Webex Meetings: todas las versiones de Webex Network Recording Player y Webex Player anteriores a la versión WBS 39.5.17 o WBS 39.11.0
- Cisco Webex Meetings Online: todas las versiones de Webex Network Recording Player y Webex Player anteriores a la versión 1.3.49
- Cisco Webex Meetings Server: todas las versiones de Webex Network Recording Player anteriores a la versión 3.0MR3SecurityPatch1 y 4.0MR2SecurityPatch2

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200304-webex-player

---

Vulnerabilidad

CVE-2020-3148

Una vulnerabilidad en la interfaz web de Cisco Prime Network Registrar (CPNR) podría permitir que un atacante remoto no autenticado realice un ataque de falsificación de solicitudes entre sitios (CSRF) en un sistema afectado.

La vulnerabilidad se debe a insuficientes protecciones CSRF en la interfaz basada en web. Un atacante podría aprovechar esta vulnerabilidad persuadiendo a un usuario objetivo, con una sesión administrativa activa en el dispositivo afectado, para que haga clic en un enlace malicioso. Una explotación exitosa podría permitir a un atacante cambiar la configuración del dispositivo, lo que podría incluir la capacidad de editar o crear cuentas de usuario de cualquier nivel de privilegio. Algunos cambios en la configuración del dispositivo podrían afectar negativamente la disponibilidad de servicios de red para otros dispositivos en redes administradas por CPNR.

Productos Afectados

Esta vulnerabilidad afecta a las versiones de Cisco Prime Network Registrar anteriores a 10.1.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cpnr-csrf-WWTrDkyL

Vulnerabilidad

CVE-2020-3155

Una vulnerabilidad en la implementación SSL de la solución Cisco Intelligent Proximity podría permitir que un atacante remoto no autenticado vea o modifique la información compartida en los dispositivos de video Cisco Webex y los puntos finales de colaboración de Cisco.

La vulnerabilidad se debe a la falta de validación del certificado del servidor SSL recibido al establecer una conexión a un dispositivo de video Cisco Webex o un punto final de colaboración de Cisco. Un atacante podría aprovechar esta vulnerabilidad al usar técnicas de hombre en el medio (MITM) para interceptar el tráfico entre el cliente afectado y un punto final, y luego usar un certificado falsificado para suplantar el punto final. Dependiendo de la configuración del punto final, un exploit podría permitir al atacante ver el contenido de presentación compartido en él, modificar cualquier contenido presentado por la víctima o tener acceso a los controles de llamadas.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco si están ejecutando una versión de software vulnerable, tienen habilitada la función de proximidad y se utilizan para conectarse a dispositivos locales:

- Cisco Intelligent Proximity application
- Cisco Jabber
- Cisco Webex Meetings
- Cisco Webex Teams
- Cisco Meeting App

Mitigación

Cisco no ha publicado actualizaciones de software que aborden esta vulnerabilidad. Todas las versiones de software están afectadas, por lo que se recomienda consultar en el link como determinar si algún cliente cuenta con la función de proximidad para deshabilitarla.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-proximity-ssl-cert-gBBu3RB

Vulnerabilidad

CVE-2020-3181

Una vulnerabilidad en la funcionalidad de detección de malware en Cisco Advanced Malware Protection (AMP) en Cisco AsyncOS software para dispositivos de seguridad de correo electrónico de Cisco (ESA) podría permitir que un atacante remoto no autenticado agote los recursos en un dispositivo afectado.

La vulnerabilidad se debe a un control insuficiente sobre la asignación de memoria del sistema. Un atacante podría aprovechar esta vulnerabilidad enviando un correo electrónico diseñado a través del dispositivo de destino. Una explotación exitosa podría permitir que el atacante provoque la entrega de un archivo adjunto de correo electrónico que contiene malware a un usuario y ocasione demoras en el procesamiento del correo electrónico.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba al software Cisco AsyncOS para las versiones de Cisco ESA anteriores a la versión 13.0.0.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-resource-exhaust-D7RQAhnD

Vulnerabilidad

CVE-2020-3166

Una vulnerabilidad en la CLI del software Cisco FXOS podría permitir que un atacante local autenticado lea o escriba archivos arbitrarios en el sistema operativo (SO) subyacente.

La vulnerabilidad se debe a una validación de entrada insuficiente. Un atacante podría aprovechar esta vulnerabilidad al incluir argumentos diseñados para un comando CLI específico. Una explotación exitosa podría permitir al atacante leer o escribir en archivos arbitrarios en el sistema operativo subyacente.

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 FXOS:

- Firepower 1000 Series
- Firepower 2100 Series
- Firepower 4100 Series
- Firepower 9300 Security Appliances

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200226-fxos-cli-file

---

Vulnerabilidad

CVE-2020-3167

Una vulnerabilidad en la CLI del software Cisco FXOS y del software Cisco UCS Manager podría permitir que un atacante local autenticado ejecute comandos arbitrarios en el sistema operativo (SO) subyacente.

La vulnerabilidad se debe a una validación de entrada insuficiente. Un atacante podría explotar esta vulnerabilidad al incluir argumentos diseñados para comandos específicos. Una explotación exitosa podría permitir al atacante ejecutar comandos arbitrarios en el sistema operativo subyacente con los privilegios del usuario actualmente conectado para todas las plataformas

afectadas, excluyendo las interconexiones Fabric Cisco UCS 6400 Series. En las interconexiones Fabric de Cisco UCS 6400 Series, los comandos inyectados se ejecutan con privilegios de root.

Productos Afectados

- Esta vulnerabilidad afecta a los siguientes productos de Cisco si están ejecutando una versión vulnerable del software Cisco FXOS o del software Cisco UCS Manager:
- 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 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches
- Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode
- Nexus 9000 Series Switches in standalone NX-OS mode

En el enlace se presenta una matriz con las versiones afectadas.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200226-fxos-ucs-cmdinj

---

Vulnerabilidad

CVE-2020-3172

Una vulnerabilidad en la función de Cisco Discovery Protocol del software Cisco FXOS y el software Cisco NX-OS podría permitir que un atacante adyacente no autenticado ejecute código arbitrario como root o cause una condición de denegación de servicio (DoS) en un dispositivo afectado.

La vulnerabilidad existe debido a los encabezados de paquetes de Cisco Discovery Protocol insuficientemente validados. Un atacante podría aprovechar esta vulnerabilidad enviando un paquete de Cisco Discovery Protocol diseñado a un dispositivo afectado adyacente a la Capa 2. Una explotación exitosa podría permitir al atacante causar un desbordamiento del búfer que

podría permitirle ejecutar código arbitrario como root o causar una condición DoS en el dispositivo afectado.

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco si están ejecutando una versión vulnerable del software Cisco FXOS o del software Cisco NX-OS y si están configurados para usar el Protocolo de descubrimiento de Cisco:

Firepower 4100 Series (CSCvr37151)
Firepower 9300 Security Appliances (CSCvr37151)
MDS 9000 Series Multilayer Switches (CSCux07556)
Nexus 1000 Virtual Edge for VMware vSphere (CSCvr37146)
Nexus 1000V Switch for Microsoft Hyper-V (CSCvr37146)
Nexus 1000V Switch for VMware vSphere (CSCvr37146)
Nexus 3000 Series Switches (CSCux58226)
Nexus 5500 Platform Switches (CSCvr37148)
Nexus 5600 Platform Switches (CSCvr37148)
Nexus 6000 Series Switches (CSCvr37148)
Nexus 7000 Series Switches (CSCux07556)
Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode (CSCvr31410)
Nexus 9000 Series Switches in standalone NX-OS mode (CSCux58226)
UCS 6200 Series Fabric Interconnects (CSCvr37150)
UCS 6300 Series Fabric Interconnects (CSCvr37150)

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200226-fxos-nxos-cdp