Alerta de seguridad informática	9VSA-00084-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de noviembre de 2019
Última revisión	11 de noviembre 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 a vulnerabilidades que afectan a sus productos.

Vulnerabilidades

CVE-2019-15270
CVE-2019-15973
CVE-2019-15974
CVE-2019-15959
CVE-2019-15967
CVE-2019-15960
CVE-2019-15969
CVE-2019-15958
CVE-2019-15957
CVE-2019-15283
CVE-2019-15284
CVE-2019-15285
CVE-2019-15286
CVE-2019-15287
CVE-2019-15276
CVE-2019-15271
CVE-2019-15956
CVE-2019-15289
CVE-2019-15288

Vulnerabilidad

CVE-2019-15270

Impacto

Una vulnerabilidad en la interfaz de administración web de Cisco Firepower Management Center (FMC) podría permitir que un atacante remoto autenticado realice un ataque cross-site scripting (XSS) contra un usuario de la interfaz de administración basada en web.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones del software Cisco FMC anteriores a la versión 6.5.0.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191016-firepwr-stored-xss

---

Vulnerabilidad

CVE-2019-15973

Impacto

Una vulnerabilidad en la interfaz de administración basada en la web de Cisco Industrial Network Director (IND) podría permitir que un atacante remoto no autenticado realice un ataque cross-site scripting (XSS) contra un usuario de la interfaz de una aplicación afectada.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco IND anteriores a la versión 1.7.1-45.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-idn-xss

---

Vulnerabilidad

CVE-2019-15974

Impacto

Una vulnerabilidad en la interfaz web de Cisco Managed Services Accelerator (MSX) podría permitir que un atacante remoto no autenticado redirija a un usuario a una página web maliciosa.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco MSX anteriores a la Versión 3.7.0.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-msa-open-redirect

---

Vulnerabilidad

CVE-2019-15959

Impacto

Una vulnerabilidad en los teléfonos IP Cisco Small Business serie SPA500 podría permitir que un atacante físicamente próximo ejecute comandos arbitrarios en el dispositivo.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de firmware de los teléfonos IP de la serie SPA500 de Cisco Small Business 7.6.2SR5 y anteriores.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-spa500-script

---

Vulnerabilidad

CVE-2019-15967

Impacto

Una vulnerabilidad en la CLI de Cisco TelePresence Collaboration Endpoint (CE) y el software Cisco RoomOS podría permitir que un atacante local autenticado habilite la grabación de audio sin notificar a los usuarios.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones del software Cisco TelePresence CE anteriores a la versión 9.8.1 y a las versiones del software Cisco RoomOS anteriores a la RoomOS September Drop 1 2019.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-telece-ros-eve

---

Vulnerabilidad

CVE-2019-15960

Impacto

Una vulnerabilidad en la página de administración de Webex Network Recording de Cisco Webex Meetings podría permitir a un atacante remoto autenticado elevar los privilegios en el contexto de la página afectada. Para aprovechar esta vulnerabilidad, el atacante debe iniciar sesión como administrador de bajo nivel.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco Webex Meetings anteriores a 39.7.0.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-wbs-privilege

---

Vulnerabilidad

CVE-2019-15969

Impacto

Una vulnerabilidad en la interfaz de administración basada en la web de Cisco Web Security Appliance (WSA) podría permitir que un atacante remoto no autenticado realice ataques de cross-site scripting (XSS) contra un usuario de la interfaz de un dispositivo afectado.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco WSA anteriores a la versión 11.8.0-332.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-wsa-xss

---

Vulnerabilidad

CVE-2019-15958

Impacto

Una vulnerabilidad en la API REST de Cisco Prime Infrastructure (PI) y Cisco Evolved Programmable Network Manager (EPNM) podría permitir que un atacante remoto no autenticado ejecute código arbitrario con privilegios de root en el sistema operativo subyacente.

Productos Afectados

Esta vulnerabilidad afecta a las versiones de Cisco PI Software anteriores a 3.4.2, 3.5.1, 3.6.0 Update 02 y a las versiones de Cisco EPNM anteriores a 3.0.2.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-pi-epn-codex

---

Vulnerabilidad

CVE-2019-15957

Impacto

Una vulnerabilidad en la interfaz de administración basada en la web de ciertos enrutadores Cisco Small Business RV Series podría permitir que un atacante remoto autenticado con privilegios administrativos inyecte comandos arbitrarios en el sistema operativo subyacente. Cuando se procesen, los comandos se ejecutarán con privilegios de root.

Productos Afectados

Los siguientes routers Cisco Small Business de la serie RV son vulnerables si están ejecutando una versión de firmware anterior a 4.2.3.10:

- RV016 Multi-WAN VPN Router[1]
- RV042 Dual WAN VPN Router
- RV042G Dual Gigabit WAN VPN Router
- RV082 Dual WAN VPN Router[1]

1. El router VPN WAN múltiple RV016 de Cisco y el router VPN WAN dual RV082 han llegado al final del mantenimiento del software.

Los enrutadores VPN VPN WAN duales Gigabit RV320 y RV325 son vulnerables si están ejecutando una versión de firmware anterior a 1.5.1.05.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-sbr-cominj

---

Vulnerabilidad

CVE-2019-15289

Impacto

Múltiples vulnerabilidades en el servicio de video de Cisco TelePresence Collaboration Endpoint (CE) y el software Cisco RoomOS podrían permitir que un atacante remoto no autenticado cause una condición de denegación de servicio (DoS) en un dispositivo afectado.

Productos Afectados

Estas vulnerabilidades afectan a los siguientes productos de Cisco si están ejecutando versiones del software Cisco TelePresence CE anteriores a la 9.8.0 o las versiones del software Cisco RoomOS anteriores a la RoomOS July Drop 1 2019:

- Webex Board 55
- Webex Board 55S
- Webex Board 70
- Webex Board 70S
- Webex Board 85S

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-telepres-roomos-dos

---

Vulnerabilidad

CVE-2019-15288

Impacto

Una vulnerabilidad en la CLI de Cisco TelePresence Collaboration Endpoint (CE), Cisco TelePresence Codec (TC) y Cisco RoomOS Software podría permitir que un atacante remoto autenticado escale privilegios a un usuario sin restricciones del shell restringido.

Productos Afectados

Esta vulnerabilidad afecta a las versiones del software Cisco TelePresence CE anteriores a 9.8.1, a las versiones de Cisco TC Software anteriores a 7.3.19 y a las versiones de Cisco RoomOS Software anteriores a RoomOS September Drop 1 2019 que tienen habilitada la función SSH.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-telepres-roomos-privesc

---

Vulnerabilidad

CVE-2019-15283
CVE-2019-15284
CVE-2019-15285
CVE-2019-15286
CVE-2019-15287

Impacto

Múltiples 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.

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 Cisco Webex Meetings Server:

- Sitios de Cisco Webex Meetings: todas las versiones de Webex Network Recording Player y Webex Player anteriores a la versión WBS 39.5.12
- Cisco Webex Meetings Online: todas las versiones de Webex Network Recording Player y Webex Player anteriores a la versión 1.3.44
- Cisco Webex Meetings Server: todas las versiones de Webex Network Recording Player anteriores a la versión 4.0MR2

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-webex-player

---

Vulnerabilidad

CVE-2019-15276

Impacto

Una vulnerabilidad en la interfaz web del software Cisco Wireless LAN Controller podría permitir que un atacante remoto, con pocos privilegios y autenticado, cause una condición de denegación de servicio (DoS) en un dispositivo afectado.

Productos Afectados

Esta vulnerabilidad afecta a los controladores de LAN inalámbrica de Cisco que ejecutan la versión de software 8.4 y posterior, y anterior a 8.10.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-wlc-dos

---

Vulnerabilidad

CVE-2019-15956

Impacto

Una vulnerabilidad en la interfaz de administración web del software Cisco AsyncOS para Cisco Web Security Appliance (WSA) podría permitir que un atacante remoto autenticado realice un reinicio no autorizado del sistema en un dispositivo afectado.

Productos Afectados

Esta vulnerabilidad afecta al dispositivo de seguridad de la red de Cisco (WSA), versiones 10.1, 10.5,.11.5 y 11.7

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-wsa-unauth-devreset

---

Vulnerabilidad

CVE-2019-15271

Impacto

Una vulnerabilidad en la interfaz de administración basada en la web de ciertos routers Cisco Small Business RV Series podría permitir que un atacante remoto autenticado ejecute comandos arbitrarios con privilegios de root. El atacante debe tener una credencial válida o un token de sesión activo.

Productos Afectados

Los siguientes routers Cisco Small Business de la serie RV son vulnerables si están ejecutando una versión de firmware anterior a 4.2.3.10:

- RV016 Multi-WAN VPN Router[1]
- RV042 Dual WAN VPN Router
- RV042G Dual Gigabit WAN VPN Router
- RV082 Dual WAN VPN Router[1]

1. El router VPN WAN múltiple RV016 de Cisco y el router VPN WAN dual RV082 han llegado al final del mantenimiento del software.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-sbrv-cmd-x

---

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.11.11 16:51:45 -03'00'