Alerta de seguridad informática	9VSA-00061-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de octubre de 2019
Última revisión	3 de octubre 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.

Vulnerabilidad

CVE-2019-12698

Impacto

Una vulnerabilidad en la característica WebVPN del software Cisco Adaptive Security Appliance (ASA) y Cisco Firepower Threat Defense (FTD) podría permitir que un atacante remoto no autenticado provoque una mayor utilización de la CPU en un dispositivo afectado.

Productos Afectados

Esta vulnerabilidad afecta a los productos de Cisco que ejecutan el software Cisco Adaptive Security Appliance (ASA) y Cisco Firepower Threat Defense (FTD) cuando se configura para WebVPN.
Las versiones vulnerable son:

- Cisco ASA Software, desde la versión 9.4 (y anteriores) hasta 9.13
- Cisco FTD Software, desde la versión 6.1.0 (y anteriores) hasta 6.4

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Cisco ASA Software versiones 9.5 y anteriores, así como la Versión 9.7, han llegado al final del mantenimiento del software, esta situación también sucede con las versiones de Cisco FMC y FTD anteriores a 6.2.3. Se aconseja a los clientes que migren a una versión compatible que incluya la solución para esta vulnerabilidad.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-ftd-dos

---

Vulnerabilidad

CVE-2019-12693

Impacto

Una vulnerabilidad en la función de Copia segura (SCP) del software Cisco Adaptive Security Appliance (ASA) podría permitir que un atacante remoto autenticado cause una condición de denegación de servicio (DoS).

Productos Afectados

- Cisco ASA Software, desde la versión 9.4 (y anteriores) hasta 9.12

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Cisco ASA Software versiones 9.5 y anteriores, así como la Versión 9.7, han llegado al final del mantenimiento del software. Se aconseja a los clientes que migren a una versión compatible que incluya la solución para esta vulnerabilidad.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-scp-dos

---

Vulnerabilidad

CVE-2019-12695

Impacto

Una vulnerabilidad en Clientless SSL VPN (WebVPN) portal de Cisco Adaptive Security Appliance (ASA) y en el Software Cisco Firepower Threat Defense (FTD) podría permitir que un atacante remoto no autenticado realice un ataque de scripting entre sitios (XSS) contra un usuario de La interfaz web de un dispositivo afectado.

Productos Afectados

Esta vulnerabilidad afecta a los productos de Cisco que ejecutan el software Cisco Adaptive Security Appliance (ASA) y Cisco Firepower Threat Defense (FTD) cuando se configura para WebVPN.

Las versiones vulnerable son:

- Cisco ASA Software, desde la versión 9.4 (y anteriores) hasta 9.13
- Cisco FTD Software, desde la versión 6.1.0 (y anteriores) hasta 6.4

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Cisco ASA Software versiones 9.5 y anteriores, así como la Versión 9.7, han llegado al final del mantenimiento del software, esta situación también sucede con las versiones de Cisco FMC y FTD anteriores a 6.2.3. Se aconseja a los clientes que migren a una versión compatible que incluya la solución para esta vulnerabilidad.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-xss

---

Vulnerabilidad

CVE-2019-12710

Impacto

Una vulnerabilidad en la interfaz web de Cisco Unified Communications Manager y Cisco Unified Communications Manager Session Management Edition (SME) podría permitir que un atacante remoto autenticado afecte la confidencialidad de un sistema afectado mediante la ejecución de consultas SQL arbitrarias.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba las siguientes versiones de Cisco Unified Communications Manager y Cisco Unified Communications Manager SME:

- 10.5(2) y anteriores
- 11.5(1)SU5 y anteriores
- 12.0(1)SU2 y anteriores
- 12.5(1) y anteriores

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-cuc-inject

---

Vulnerabilidad

CVE-2019-12707

Impacto

Una vulnerabilidad en la interfaz web de múltiples productos de Cisco Unified Communications podría permitir que un atacante remoto no autenticado realice un ataque de scripting entre sitios (XSS) contra un usuario de la interfaz basada en web del software afectado.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a los siguientes productos y lanzamientos de Cisco:

- Unified Communications Manager y Unified Communications Manager Session Management Edition (SME) versiones:
  - 10.5(2) y anteriores
  - 11.5(1)SU5 y anteriores
  - 12.5(1) y anteriores
- Unified Communications Manager IM & Presence Service (IM&P) versiones:
  - 11.5(1)SU5 y anteriores
  - 12.5(1) y anteriores
- Unity Connection versiones
  - 11.5(1)SU5 y anteriores
  - 12.5(1) y anteriores

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-cuc-xss

---

Vulnerabilidad

CVE-2019-12715
CVE-2019-12716

Impacto

Una vulnerabilidad en la interfaz basada en la web de Cisco Unified Communications Manager y Cisco Unified Communications Manager Session Management Edition (SME) podría permitir que un atacante remoto no autenticado realice un ataque de scripting entre sitios (XSS) contra un usuario de la web interfaz del software afectado.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba las siguientes versiones de Cisco Unified Communications Manager y Cisco Unified Communications Manager SME:

- 10.5(2) y anteriores
- 11.5(1)SU5 y anteriores
- 12.0(1)SU2 y anteriores
- 12.5(1) y anteriores

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-cucm-xss-12715
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-cucm-xss-12716

Vulnerabilidad

CVE-2019-12711

Impacto

Una vulnerabilidad en la interfaz web de Cisco Unified Communications Manager y Cisco Unified Communications Manager Session Management Edition (SME) podría permitir que un atacante remoto no autenticado acceda a información confidencial o cause una condición de denegación de servicio (DoS).

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba las siguientes versiones de Cisco Unified Communications Manager y Cisco Unified Communications Manager SME:

- 10.5(2) y anteriores
- 11.5(1)SU5 y anteriores
- 12.0(1)SU2 y anteriores
- 12.5(1) y anteriores

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-cucm-xxe

---

Vulnerabilidad

CVE-2019-12706

Impacto

Una vulnerabilidad en la funcionalidad Sender Policy Framework (SPF) del software Cisco AsyncOS para Cisco Email Security Appliance (ESA) podría permitir que un atacante remoto no autenticado omita los filtros de usuario configurados en un dispositivo afectado.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba al software Cisco AsyncOS para las versiones del dispositivo de seguridad de correo electrónico de Cisco (ESA) anteriores a la versión 13.5.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-esa-bypass

---

Vulnerabilidad

CVE-2019-12701

Impacto

Una vulnerabilidad en la función de inspección de archivos y malware del software Cisco Firepower Management Center (FMC) podría permitir que un atacante remoto no autenticado omitiera las políticas de inspección de archivos y malware en un sistema afectado.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba al software Cisco FMC que ejecutaba versiones de Cisco VDB Fingerprint Database anteriores a 327.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fire-bypass

Vulnerabilidad

CVE-2019-12696
CVE-2019-12697

Impacto

Múltiples vulnerabilidades en el motor de detección de software del sistema Cisco Firepower podrían permitir que un atacante remoto no autenticado omitiera las políticas de malware y archivos configuradas para los tipos de archivos RTF y RAR.

Productos Afectados

Estas vulnerabilidades afectan los siguientes productos de Cisco si se ejecuta una versión vulnerable del software Cisco Firepower:

- 3000 Series Industrial Security Appliances (ISAs)
- Adaptive Security Appliance (ASA) 5500-X Series Firewalls
- ASA 5500-X Series with FirePOWER Services
- Advanced Malware Protection (AMP) for Networks for FirePOWER 7000 Series Appliances
- AMP for Networks for FirePOWER 8000 Series Appliances
- Firepower 2100 Series
- Firepower 4100 Series
- Firepower 1000 Series Appliances
- FirePOWER 7000 Series Appliances
- FirePOWER 8000 Series Appliances
- Firepower 9300 Security Appliances
- Firepower Threat Defense for Integrated Services Routers (ISRs)
- FTD Virtual (FTDv)
- Next-Generation Intrusion Prevention System (NGIPS)

Las versiones vulnerables de CISCO FTD van desde 6.1.0 a la 6.4.0

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Las versiones de software Cisco FMC y FTD 6.0.1 y anteriores han llegado al final del mantenimiento del software. Se aconseja a los clientes que migren a una versión compatible que incluya la solución para esta vulnerabilidad.
Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-firepwr-bypass

---

Vulnerabilidad

CVE-2019-12691

Impacto

Una vulnerabilidad en la interfaz de administración basada en la web del software Cisco Firepower Management Center (FMC) podría permitir que un atacante remoto autenticado realice un ataque transversal de directorio en un dispositivo afectado.

Productos Afectados

Esta vulnerabilidad afecta al software Cisco FMC, desde la versión 6.1.0 (y anteriores) hasta 6.2.3

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.
Las versiones de software Cisco FMC y FTD 6.0.1 y anteriores han llegado al final del mantenimiento del software. Se aconseja a los clientes que migren a una versión compatible que incluya la solución para esta vulnerabilidad.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fmc-dir-trav

---

Vulnerabilidad

CVE-2019-12694
Impacto

Una vulnerabilidad en la interfaz de línea de comando (CLI) del software Cisco Firepower Threat Defense (FTD) podría permitir que un atacante local autenticado con privilegios administrativos ejecute comandos en el sistema operativo subyacente con privilegios de root.

Productos Afectados

Esta vulnerabilidad afecta al software Cisco FTD, desde la versión 6.1.0 (y anteriores) hasta 6.4.0
Mitigación

Aplicar las actualizaciones publicadas por el fabricante.
Las versiones de software Cisco FMC y FTD 6.0.1 y anteriores han llegado al final del mantenimiento del software. Se aconseja a los clientes que migren a una versión compatible que incluya la solución para esta vulnerabilidad.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-ftd-cmdinj

---

Vulnerabilidad

CVE-2019-12714

Impacto

Una vulnerabilidad en la interfaz de administración basada en web de Cisco IC3000 Industrial Compute Gateway podría permitir que un atacante remoto autenticado cause una condición de denegación de servicio (DoS) en un dispositivo afectado.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones del software Cisco IC3000 Industrial Compute Gateway anteriores a la versión 1.1.1.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-ic3000-icg-dos

---

Vulnerabilidad

CVE-2019-12631

Impacto

Una vulnerabilidad en el portal de invitados basado en la web de Cisco Identity Services Engine (ISE) podría permitir que un atacante remoto no autenticado realice un ataque de scripting entre sitios (XSS) contra un usuario de la interfaz de administración basada en la web.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco ISE Software anteriores a:

- 2.4 Patch 10
- 2.6 Patch 3
- 2.7

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-ise-xss

---

Vulnerabilidad

CVE-2019-12712
CVE-2019-12713

Impacto

Una vulnerabilidad en la interfaz de administración basada en web de Cisco Prime Infrastructure podría permitir que un atacante remoto no autenticado realice un ataque de scripting entre sitios (XSS) contra un usuario de la interfaz de administración basada en web del software afectado.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones del software Cisco Prime Infrastructure anteriores a la versión 3.7.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-pi-xss-12712
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-pi-xss-12713

Vulnerabilidad

CVE-2019-12630

Impacto

Una vulnerabilidad en la función de deserialización de Java utilizada por Cisco Security Manager podría permitir que un atacante remoto no autenticado ejecute comandos arbitrarios en un dispositivo afectado.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones de Cisco Security Manager anteriores a la versión 4.18.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-sm-java-deserial

---

Vulnerabilidad

CVE-2019-15259

Impacto

Una vulnerabilidad en el software Cisco Unified Contact Center Express (UCCX) podría permitir que un atacante remoto no autenticado realice un ataque de división de respuesta HTTP.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba a las versiones del software Cisco UCCX anteriores a 11.6 (2).

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-uccx-http

---

Vulnerabilidad

CVE-2019-15272

Impacto

Una vulnerabilidad en la interfaz basada en la web de Cisco Unified Communications Manager y Cisco Unified Communications Manager Session Management Edition (SME) podría permitir que un atacante remoto no autenticado eluda las restricciones de seguridad.

Productos Afectados

En el momento de la publicación, esta vulnerabilidad afectaba las siguientes versiones de Cisco Unified Communications Manager y Cisco Unified Communications Manager SME:

- 10.5 (2) y anterior
- 11.5 (1) SU5 y anterior
- 12.0 (1) SU2 y anterior
- 12.5 (1) y anterior

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-ucm-secbypass

---

Vulnerabilidad

CVE-2019-12673

Impacto

Una vulnerabilidad en el motor de inspección FTP del software Cisco Adaptive Security (ASA) y el software Cisco Firepower Threat Defense (FTD) podría permitir que un atacante remoto no autenticado cause una condición de denegación de servicio (DoS) en un dispositivo afectado.

Productos Afectados

Esta vulnerabilidad afecta a los productos de Cisco si están ejecutando una versión vulnerable del software Cisco ASA o del software Cisco FTD que está configurado para realizar una inspección FTP.

Las versiones vulnerables son:

- Cisco ASA Software, desde la versión 9.4 (y anteriores) hasta 9.12
- Cisco FTD Software, desde la versión 6.1.0 (y anteriores) hasta 6.4

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-dos

---

Vulnerabilidad

CVE-2019-15256

Impacto

Una vulnerabilidad en la función de Internet Key Exchange versión 1 (IKEv1) del software del dispositivo de seguridad adaptable de Cisco (ASA) y el software Cisco Firepower Threat Defense (FTD) podría permitir que un atacante remoto no autenticado desencadene una recarga de un dispositivo afectado, resultando en un condición de denegación de servicio (DoS).

Productos Afectados

Esta vulnerabilidad afecta a los siguientes productos de Cisco cuando se ejecuta una versión vulnerable de Cisco ASA Software o Cisco FTD Software en interfaces que tienen el protocolo IKEv1 habilitado para conexiones LAN a LAN o VPN de acceso remoto Ipsec:

- Adaptive Security Virtual Appliance (ASAv)
- Firepower 2100 Series Appliances

- Firepower Threat Defense Virtual (FTDv)

Las versiones afectadas son:

- Cisco ASA Software, desde la versión 9.7 hasta la 9.12
- Cisco FTD Software, desde la versión 6.2 hasta la 6.3

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-ftd-ikev1-dos

---

Vulnerabilidad

CVE-2019-12678

Impacto

Una vulnerabilidad en el módulo de Session Initiation Protocol (SIP) inspection del Software de Cisco Adaptive Security Appliance (ASA) y del Software de Cisco Firepower Threat Defense (FTD) podría permitir que un atacante remoto no autenticado cause una condición de denegación de servicio (DoS) en un afectado dispositivo.

Productos Afectados

Esta vulnerabilidad afecta a los productos de Cisco que ejecutan una versión vulnerable de Cisco ASA Software o Cisco FTD Software y que tienen habilitada la función de inspección SIP. La inspección SIP está habilitada de forma predeterminada en el software Cisco ASA y el software FTD. Versiones afectadas:

- Cisco ASA Software, versiones desde 9.4 (y anteriores) hasta 9.12
- Cisco FTD Software, versiones desde 6.1.0 (y anteriores) hasta 6.4.0

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Cisco ASA Software versiones 9.5 y anteriores, así como la Versión 9.7, han llegado al final del mantenimiento del software, esta situación también sucede con las versiones de Cisco FMC y FTD anteriores a 6.2.3. Se aconseja a los clientes que migren a una versión compatible que incluya la solución para esta vulnerabilidad.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-ftd-sip-dos

---

Vulnerabilidad

CVE-2019-12676

Impacto

Una vulnerabilidad en la implementación Open Shortest Path First (OSPF) del software Cisco Adaptive Security Appliance (ASA) y del Software Cisco Firepower Threat Defense (FTD) podría permitir que un atacante adyacente no autenticado provoque una recarga de un dispositivo afectado, lo que resultaría en una negación Condición de servicio (DoS).

Productos Afectados

Esta vulnerabilidad afecta a los productos de Cisco que ejecutan una versión vulnerable del software Cisco ASA o del software Cisco FTD que está configurado para admitir el enrutamiento OSPF.
Versiones afectadas:

- Cisco ASA Software, versiones desde 9.4 (y anteriores) hasta 9.12
- Cisco FTD Software, versiones desde 6.1.0 (y anteriores) hasta 6.4.0

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Cisco ASA Software versiones 9.5 y anteriores, así como la Versión 9.7, han llegado al final del mantenimiento del software, esta situación también sucede con las versiones de Cisco FMC y FTD anteriores a 6.2.3. Se aconseja a los clientes que migren a una versión compatible que incluya la solución para esta vulnerabilidad.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-ospf-lsa-dos

---

Vulnerabilidad

CVE-2019-12677

Impacto

Una vulnerabilidad en la función Secure Sockets Layer (SSL) VPN del software de Cisco dispositivo Adaptive Security Appliance (ASA) podría permitir que un atacante remoto autenticado cause una condición de denegación de servicio (DoS) que impida la creación de una nueva conexión SSL/ Transport Layer Security (TLS) a un dispositivo afectado.

Productos Afectados

Esta vulnerabilidad afecta a los productos de Cisco que ejecutan una versión vulnerable del software Cisco ASA y que tienen habilitada la VPN SSL sin cliente o la VPN SSL AnyConnect.

Versiones afectadas:

- Cisco ASA Software, desde las versiones 9.1 (y anteriores) hasta 9.6

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.
Cisco ASA Software versiones 9.5 y anteriores, así como la Versión 9.7, han llegado al final del mantenimiento del software. Se aconseja a los clientes que migren a una versión compatible que incluya la solución para esta vulnerabilidad.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-asa-ssl-vpn-dos

---

Vulnerabilidad

CVE-2019-1915

Impacto

Una vulnerabilidad en la interfaz web de Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition (SME), Cisco Unified Communications Manager IM y Presence (Unified CM IM&P) y Cisco Unity Connection podría permitir a un atacante remoto no autenticado llevar a cabo un ataque de falsificación de solicitud entre sitios (CSRF) en un sistema afectado.

Productos Afectados

Esta vulnerabilidad afecta a Cisco Unified Communications Manager, Cisco Unified Communications Manager SME, Cisco Unified CM IM&P Service y Cisco Unity Connection.

Versiones afectadas:

- Unified Communications Manager y Unified Communications Manager Session Management Edition, desde la versión 10.5(2) (y anteriores) hasta 12.5
- Unified Communications Manager IM y Presence Service, desde la version 10.5(2) (y anteriores) hasta 12.5
- Unity Connection, desde la versión 10.5(2) (y anteriores) hasta 12.5

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-cucm-csrf

---

Vulnerabilidad

CVE-2019-12690

Impacto

Una vulnerabilidad en la interfaz de usuario web de Cisco Firepower Management Center (FMC) podría permitir que un atacante remoto autenticado inyecte comandos arbitrarios que se ejecutan con los privilegios del usuario root del sistema operativo subyacente.

Productos Afectados

Esta vulnerabilidad afecta al software Cisco FMC., desde la versión 6.1.0 hasta 6.0.0

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fmc-com-inj

---

Vulnerabilidad

CVE-2019-12687
CVE-2019-12688

Impacto

Una vulnerabilidad en la interfaz de usuario web de Cisco Firepower Management Center (FMC) podría permitir que un atacante remoto autenticado ejecute comandos arbitrarios en un dispositivo afectado.

Productos Afectados

Esta vulnerabilidad afecta al software Cisco FMC desde la versión 6.1.0 (y anteriores) hasta 6.4.0

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fmc-rce

---

Vulnerabilidad

CVE-2019-12674
CVE-2019-12675

Impacto

Múltiples vulnerabilidades en la función de instancias múltiples del software Cisco Firepower Threat Defense (FTD) podrían permitir que un atacante local autenticado escape del contenedor para su instancia FTD y ejecute comandos con privilegios de root en el espacio de nombres del host.

Productos Afectados

Estas vulnerabilidades afectan los siguientes productos de Cisco si están ejecutando una versión vulnerable del software Cisco FTD que está configurado para operación de varias instancias:

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-ftd-container-esc

Vulnerabilidad

CVE-2019-12700

Impacto

Una vulnerabilidad en Pluggable Authentication Module (PAM) utilizado en Cisco Firepower Threat Defense (FTD) Software, Cisco Firepower Management Center (FMC) Software, y Cisco FXOS Software podría permitir que un atacante remoto autenticado cause una denegación de servicio (DoS).

Productos Afectados

Esta vulnerabilidad afecta Cisco FTD Software, FMC Software, and FXOS Software que se ejecutan en cualquier producto Cisco.
Las versiones afectadas son:

- Cisco FTD Software y FMC Software, desde la versión 6.1.0 (y anteriores) hasta 6.2.3
- Cisco FXOS Software, desde la versión 2.2 (y anteriores) hasta 2.6

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-ftd-fpmc-dos

Vulnerabilidad

CVE-2019-12699

Impacto

Múltiples vulnerabilidades en la CLI del software Cisco FXOS y del software Cisco Firepower Threat Defense (FTD) podrían permitir que un atacante local autenticado ejecute comandos en el sistema operativo (SO) subyacente con privilegios de root.

Productos Afectados

Estas vulnerabilidades afectan las versiones del software Cisco FXOS y Cisco FTD cuando se ejecutan en las siguientes plataformas:

- Cisco Firepower 1000 Series Appliances

- Cisco Firepower 2100 Series Appliances
- Cisco Firepower 4100 Series Appliances
- Cisco Firepower 9300 Series Appliances

Las versiones afectadas son:

- Cisco FTD Software para Cisco Firepower 1000/2100 Series Appliances, desde la versión 6.1.0 (y anteriores) hasta 6.3
- Cisco FXOS Software for Cisco Firepower 4100/9300 Series Appliances, desde la versión 2.0 hasta 2.4

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fxos-cmd-inject

---

Vulnerabilidad

CVE-2019-12679
CVE-2019-12680
CVE-2019-12681
CVE-2019-12682
CVE-2019-12683
CVE-2019-12684
CVE-2019-12685
CVE-2019-12686

Impacto

Múltiples vulnerabilidades en la interfaz de administración basada en web del software Cisco Firepower Management Center (FMC) podrían permitir que un atacante remoto autenticado ejecute inyecciones SQL arbitrarias en un dispositivo afectado.

Productos Afectados

Estas vulnerabilidades afectan al software Cisco FMC, desde la versión 6.1.0 (y anteriores) hasta 6.4

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fmc-sql-inj

---

Vulnerabilidad

CVE-2019-12689

Impacto

Una vulnerabilidad en la interfaz de administración basada en web del software Cisco Firepower Management Center (FMC) podría permitir que un atacante remoto autenticado ejecute código arbitrario en el sistema operativo subyacente de un dispositivo afectado.

Productos Afectados

Estas vulnerabilidades afectan al software Cisco FMC, desde la versión 6.1.0 (y anteriores) hasta 6.2

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191002-fmc-rce-12689

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.10.04 14:31:04 -03'00'