Alerta de Seguridad Informática (9VSA-00021-001)

Nivel de Riesgo: Alto

Tipo: Vulnerabilidad

Fecha de lanzamiento original: 18 de Julio de 2019 | Última revisión 18 de Julio 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 liberado por Cisco que contiene actualizaciones de seguridad para abordar las vulnerabilidades en varios de sus productos. Un atacante podría explotar algunas de estas vulnerabilidades para tomar el control de un sistema afectado o bien realizar ataques de denegación de servicio.

Vulnerabilidad

Múltiples vulnerabilidades en productos CISCO

CVE-2019-1894	CVE-2019-1909
CVE-2019-1893	CVE-2019-1933
CVE-2019-1932	CVE-2019-1911
CVE-2019-1931	CVE-2019-1892
CVE-2019-1922	CVE-2019-1891
CVE-2019-1921	CVE-2019-1887
CVE-2019-1930	CVE-2019-1873

Impacto

CVE-2019-1894

Una vulnerabilidad en Cisco Enterprise NFV Infrastructure Software (NFVIS) podría permitir que un atacante remoto autenticado con privilegios de administrador sobrescriba o lea archivos arbitrarios en el sistema operativo subyacente (OS) de un dispositivo afectado.

CVE-2019-1893

Una vulnerabilidad en Cisco Enterprise NFV Infrastructure Software (NFVIS) podría permitir que un atacante local autenticado ejecutara comandos arbitrarios en el sistema operativo (SO) subyacente de un dispositivo afectado como root.

CVE-2019-1932

Una vulnerabilidad en Cisco Advanced Malware Protection (AMP) para puntos finales para Windows podría permitir a un atacante local autenticado con privilegios de administrador ejecutar código arbitrario.

CVE-2019-1931

Múltiples vulnerabilidades en el panel de control RSS en la interfaz de administración basada en web del Centro de administración de Cisco Firepower (FMC) podrían permitir que un atacante remoto no autenticado realice un ataque de scripts entre sitios (XSS) contra un usuario de la interfaz de administración basada en web de Un dispositivo afectado.

CVE-2019-1922

Una vulnerabilidad en el software Cisco SIP IP Phone para Cisco IP Phone 7800 Series y 8800 Series podría permitir que un atacante remoto no autenticado provoque una condición de denegación de servicio (DoS) en un teléfono afectado.

CVE-2019-1921

Una vulnerabilidad en el análisis de archivos adjuntos del software Cisco AsyncOS para Cisco Email Security Appliance (ESA) podría permitir que un atacante remoto no autenticado omita los filtros de contenido configurados en el dispositivo.

CVE-2019-1930

Múltiples vulnerabilidades en el panel de control RSS en la interfaz de administración basada en web del Centro de administración de Cisco Firepower (FMC) podrían permitir que un atacante remoto no autenticado realice un ataque de scripts entre sitios (XSS) contra un usuario de la interfaz de administración basada en web de Un dispositivo afectado.

CVE-2019-1909

Una vulnerabilidad en la implementación de la funcionalidad Border Gateway Protocol (BGP) en el software Cisco IOS XR podría permitir que un atacante remoto no autenticado provoque una condición de denegación de servicio (DoS) en un sistema afectado.

CVE-2019-1933

Una vulnerabilidad en el análisis de mensajes de correo electrónico del software Cisco AsyncOS para Cisco Email Security Appliance (ESA) podría permitir que un atacante remoto no autenticado omita los filtros configurados en el dispositivo.

CVE-2019-1911

Una vulnerabilidad en la CLI del software Cisco Unified Communications Domain Manager (Cisco Unified CDM) podría permitir a un atacante local autenticado escapar del shell restringido.

CVE-2019-1892

Una vulnerabilidad en el procesador de paquetes de entrada Secure Sockets Layer (SSL) de los switches administrados de las series 200, 300 y 500 de Cisco Small Business podría permitir que un atacante remoto no autenticado cause daños en la memoria de un dispositivo afectado.

CVE-2019-1891

Una vulnerabilidad en la interfaz web de los switches administrados de las series 200, 300 y 500 de Cisco Small Business podría permitir que un atacante remoto no autenticado provoque una condición de denegación de servicio (DoS) en un dispositivo afectado.

CVE-2019-1887

Una vulnerabilidad en la implementación del protocolo SIP (Session Initiation Protocol) de Cisco Unified Communications Manager y Unified Communications Manager Session Management Edition podría permitir que un atacante remoto no autenticado provoque una condición de denegación de servicio (DoS).

Productos afectados

CVE-2019-1894: Cisco Enterprise NFV Infrastructure Software (NFVIS)

CVE-2019-1893: Cisco Enterprise NFV Infrastructure Software (NFVIS)

CVE-2019-1932: Cisco Advanced Malware Protection (AMP)

CVE-2019-1931: Cisco Firepower Management Center

CVE-2019-1922: Cisco SIP IP Phone

CVE-2019-1921: Cisco Email Security Appliance.

CVE-2019-1930: Cisco Firepower Management Center

CVE-2019-1909: Cisco IOS XR

CVE-2019-1933: Cisco Email Security Appliance

CVE-2019-1911: Cisco Unified CDM

CVE-2019-1892: Cisco Small Business 200, 300, and 500 Series Managed Switches

CVE-2019-1891: Cisco Small Business 200, 300, and 500 Series Managed Switches

CVE-2019-1887: Cisco Unified Communications Manager y Unified Communications Manager Session Management Edition

Mitigación

Se recomienda actualizar los productos afectados de manera urgente, siguiendo los pasos provistos por el fabricante.

Enlace

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-nfvis-file-readwrite
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-nfvis-commandinj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-amp-commandinj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-fmc-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-ip-phone-sip-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-esa-bypass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-fmc-xss
https://tools.ciscohttps://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-esa-filterpass.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-iosxr-bgp-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-esa-filterpass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-cucdm-rsh
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-sbss-memcorrupt
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-sbss-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-cucm-dos

Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.07.19 19:11:30 -04'00'