Alerta de Seguridad Informática (9VSA-00012-001)

Nivel de Riesgo: Alto

Tipo: Vulnerabilidad

Fecha de lanzamiento original: 05 de Julio de 2019 | Última revisión 05 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

Cisco ha lanzado 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-2019-1855

CVE-2019-1884

CVE-2019-1886

CVE-2019-1889

CVE-2019-1890

Impacto

CVE-2019-1855

Una vulnerabilidad en el mecanismo de carga de bibliotecas de enlace dinámico específicas en Cisco Jabber para Windows podría permitir a un atacante local autenticado realizar un ataque de precarga de DLL. Para aprovechar esta vulnerabilidad, el atacante necesitaría tener credenciales válidas en el sistema de Windows.

CVE-2019-1884

Una vulnerabilidad en la funcionalidad de proxy web de Cisco AsyncOS Software para Cisco Web Security Appliance (WSA) podría permitir que un atacante remoto autenticado provoque una condición de denegación de servicio (DoS) en un dispositivo afectado.

CVE-2019-1886

Una vulnerabilidad en la función de descifrado HTTPS de Cisco Web Security Appliance (WSA) podría permitir que un atacante remoto no autenticado provoque una condición de denegación de servicio (DoS).

CVE-2019-1889

Una vulnerabilidad en la API REST para el software de administración de dispositivos en Cisco Application Policy Infrastructure Controller (APIC) podría permitir a un atacante remoto autenticado escalar privilegios root en un dispositivo afectado.

CVE-2019-1890

Una vulnerabilidad en el establecimiento de la conexión VLAN de la infraestructura de la estructura de Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software podría permitir a un atacante adyacente no autenticado eludir las validaciones de seguridad y conectar un servidor no autorizado a la infraestructura VLAN.

Productos afectados

CVE-2019-1855: Cisco Jabber para Windows software versiones anteriores a 12.6(0).

CVE-2019-1884: Cisco AsyncOS Software para Cisco Web Security Appliance, tanto dispositivos virtuales como de hardware.

CVE-2019-1886: Cisco AsyncOS Software para Cisco WSA, tanto dispositivos virtuales como de hardware.

CVE-2019-1889: Cisco APIC Software versiones anteriores a 4.1(2g).

CVE-2019-1890: Cisco Nexus 9000 Series Fabric Switches en modo ACI si está ejecutando Cisco Nexus 9000 Series ACI Mode Switch Software en versiones anteriores a 14.1(2g)

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-jabber-dll

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-asyncos-wsa

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-wsa-dos

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-ccapic-restapi

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-n9kaci-bypass

Contactos

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