Alerta de seguridad cibernética	9VSA21-00484-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de agosto de 2021
Última revisión	26 de agosto de 2021

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 del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre vulnerabilidades en varios productos de Cisco.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2021-1577
CVE-2021-1586
CVE-2021-1523
CVE-2021-1583
CVE-2021-1584
CVE-2021-1591

Impactos

Nivel de riesgo crítico.

CVE-2021-1577: Una vulnerabilidad en un endpoint API de Cisco Application Policy Infrastructure Controller (APIC) permite a un usuario no autenticado y remoto leer o escribir archivos arbitrarios en un sistema afectado.

Nivel de riesgo alto.

CVE-2021-1586: Una vulnerabilidad en las configuraciones de red Multi-Pod o Multi-Site para switches Cisco Nexus 9000 Series Fabric en modo Application Centric Infrastructure (ACI) permiten a un atacante remoto no autenticado reiniciar inesperadamente el aparato, resultando en una condición de denegación de servicio (DoS).

CVE-2021-1523: Esta vulnerabilidad en los switches Cisco Nexus 9000 Series Fabric en modo Application Centric Infrastructure (ACI) permite a un atacante remoto no autenticado generar una condición de denegación de servicio (DoS).

Productos Afectados

Cisco APIC
Cisco Cloud APIC
Cisco Nexus 9000 Series Fabric Switches en modo ACI
Cisco Nexus 9500 Series Switches

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-frw-Nt3RYxR2
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n9kaci-tcp-dos-YXukt6gM
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n9kaci-queue-wedge-cLDDEfKF
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nexus-acl-vrvQYPVe
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-naci-mdvul-vrKVgNU
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-naci-afr-UtjfO2D7
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1577
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1586
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1523
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1583
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1584
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1591

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.08.26 17:04:45 -04'00'