# Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Coordinación Nacional de Ciberseguridad Ministerio del Interior y Seguridad Pública Gobierno de Chile



Alerta de seguridad cibernética	9VSA23-00886-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
TLP	Blanco	
Fecha de lanzamiento original	23 de agosto de 2023	
Última revisión	23 de agosto de 2023	

#### 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 CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

## Resumen

El CSIRT de Gobierno comparte información sobre el parchado de varias vulnerabilidades que afectan a distintos productos de Cisco.

### Vulnerabilidades

CVE-2023-20168	CVE-2023-20200	CVE-2023-20234
CVE-2023-20169	CVE-2023-20115	CVE-2023-20230

## **Impacto**

#### Vulnerabilidades de riesgo alto

CVE-2023-20168: Vulnerabilidad de autenticación remota DE TACACS+ y RADIUS en el software de Cisco NX-OS. Podría permitir a un atacante local no autenticado el causar que un aparato afectado se reinicie inesperadamente, resultando en un condición de denegación de servicio (DoS).

CVE-2023-20169: Vulnerabilidad en el protocolo IS-IS del software Cisco NX-OS para los switches Nexus serie 3000 y Nexus serie 9000 en modo NX-OS standalone, que podría permitir a un atacante adyacente y no autenticado hacer que el proceso IS-IS se reinicie inesperadamente, lo que podría provocar que el dispositivo afectado se reinicie, resultando en una condición de denegación de servicio (DoS).

CVE-2023-20200: Vulnerabilidad en el servicio SNMP fel software Cisco FXOS para las Security appliances Firepower 4100 y Firepower 9300 y los Cisco UCS 6300 Series Fabric Interconnects, podría permitir a un atacante remoto autenticado causar una condición de denegación de servicio (DoS).

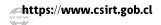
#### Mitigación

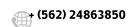
Instalar las respectivas actualizaciones entregadas por el proveedor.

#### Productos afectados

Cisco NX-OS Sofware

Ministerio del Interior y Seguridad Pública









# Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno Coordinación Nacional de Ciberseguridad Ministerio del Interior y Seguridad Pública Gobierno de Chile



Switches Cisco Nexus 3000 y 9000 series.

Cisco Firepower 4100 Series, Firepower 9300 Security Appliances y UCS 6300 Series Fabric Interconnects.

#### **Enlaces**

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxosremoteauth-dos-XB6pv74m

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-n3 9kisis-dos-FTCXB4Vb

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fp-ucsfisnmp-dos-qtv69NAO

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-sftpxVAp5Hfd

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fxosarbitrary-file-BLk6YupL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apic-uapa-F4TAShk

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20168

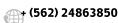
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20169

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20200

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20115

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20234

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20230





Ministerio del Interior y Seguridad Pública