

Alerta de Seguridad Cibernética

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



Alerta de seguridad cibernética	9VSA23-00769-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de enero de 2023
Última revisión	12 de enero 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 afectada a actualizaciones.

Resumen

El CSIRT de Gobierno comparte la información entregada por Cisco sobre nuevas vulnerabilidades que afectan a varios de sus productos, y para las cuales pusieron a disposición actualizaciones de seguridad.

Vulnerabilidades

CVE-2023-20025
CVE-2023-20020
CVE-2023-20026
CVE-2023-20002
CVE-2023-20018
CVE-2023-20037

CVE-2023-20008
CVE-2023-20045
CVE-2023-20040
CVE-2023-20047
CVE-2023-20038
CVE-2023-20007

CVE-2023-20043
CVE-2023-20044
CVE-2023-20058
CVE-2023-20019

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-20025 y CVE-2023-20026: Vulnerabilidades críticas en routers Cisco Small Business RV016, RV042, RV042G, and RV082. Podrían permitir a un atacante remoto evadir autenticación o ejecutar comandos arbitrarios en el sistema operativo subyacente en un dispositivo afectado.

Productos afectados

Routers Cisco Small Business RV016, RV042, RV042G, and RV082.
Cisco IP Phone 7800 y 8800 series web management interface.
Cisco BroadWorks Application Server.
Cisco BroadWorks Application Delivery Platform.
Cisco BroadWorks Xtended Services Platform.
Cisco RV340, RV340W, RV345 y RV345P Dual WAN Gigabit VPN routers.
Cisco TelePresence Collaboration Endpoint (CE) Software.
Cisco Network Services Orchestrator (NSO)

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

<https://www.csirt.gob.cl>

Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl

[@csirtgob](#)

<https://www.linkedin.com/company/csirt-gob>

Cisco RoomOS Software.
Cisco Webex Room Phone y Cisco Webex Share.
Cisco Unified Intelligence Center

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ip-phone-auth-bypass-pSqxZRPR>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ind-fZyVjJtG>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-dos-HpkeYzp>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-rce-dos-7HjP74jD>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-dkjGFgRK>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-path-trvsl-zjBeMkZg>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ldp-memlk-McOecPT>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cxagent-gOq9QjqZ>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuis-xss-Omm8jyBX>
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-xss-EzqDXqG4>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20025>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20020>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20026>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20002>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20008>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20045>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20040>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20047>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20043>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20044>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20058>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20019>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20018>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20037>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20038>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20007>