Alerta de seguridad cibernética	9VSA23-00772-01
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 afecta a actualizaciones.

Resumen

El CSIRT de Gobierno comparte información sobre dos vulnerabilidades críticas que afectan a algunos modelos de routers Cisco y que la empresa **no parchará**, por encontrarse ya estos productos más allá del límite de su vida útil.

Vulnerabilidades

CVE-2023-20025
CVE-2023-20026

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-20025 y CVE-2023-20026: Vulnerabilidades en la interfaz web de administración de routers Cisco Small Business RV016, RV042G y RV082, que podrían permitir a un atacante remoto evadir la autenticación o ejecutar comandos arbitrarios en el sistema operativo subyacente de un equipo afectado.

Productos afectados

Routers RV016 Multi-WAN VPN
Routers RV042 Dual WAN VPN
Routers RV042G Dual Gigabit WAN VPN
Routers RV082 Dual WAN VPN

Enlaces

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20025
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20026

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.01.16 16:41:21 -03'00'

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