Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00556-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de enero de 2022
Última revisión	21 de enero de 2022

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 múltiples vulnerabilidades en Cisco Redundancy Configuration Manager (RCM) para el software Cisco StarOS.

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

Vulnerabilidades

CVE-2022-20649
CVE-2022-20648

Impactos

Vulnerabilidad de riesgo crítico

CVE-2022-20649: La vulnerabilidad podría permitir que un atacante remoto no autenticado realice la ejecución remota de código en la aplicación con privilegios de nivel raíz en el contexto del contenedor configurado.

CVE-2022-20648: La vulnerabilidad podría permitir que un atacante remoto no autenticado realice acciones de depuración que podrían resultar en la divulgación de información confidencial que debería estar restringida.

Productos afectados

Estas vulnerabilidades afectan a Cisco RCM para el software Cisco StarOS.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rcm-vuls-7cS3Nuq
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20649
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20648