Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00644-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	23 de mayo de 2022
Última revisión	23 de mayo 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 CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comparte información sobre una vulnerabilidad que afecta a Cisco IOS XR.

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

Vulnerabilidades

CVE-2022-20821

Impacto

CVE-2022-20821: Una vulnerabilidad en el RPM de chequeo de salud del software Cisco IOS XR podría permitir a un atacante remoto no autenticado acceder a la instancia Redis que corre dentro del container NOSi.

Productos afectados

Routers Cisco de la serie 8000 con software Cisco IOS XR 7.3.3.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-redis-ABJyE5xK#fs
https://kb.isc.org/docs/cve-2022-1183
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20821