Alerta de seguridad cibernética	9VSA23-00783-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de febrero de 2023
Última revisión	3 de febrero 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 una vulnerabilidad de alto riesgo que afecta a algunos productos de Cisco, y para la cual la empresa ha hecho disponible un parche.

Vulnerabilidades

CVE-2023-20076

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-20076: Vulnerabilidad en aparatos que corren software Cisco IOS XE con la función Cisco IOx activada, como también a los 800 Series Industrial ISRs, Catalyst Access Points, CGR1000 Compute Modules, IC3000 Industrial Compute Gateways, IR510 WPAN Industrial Routers.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

Aparatos Cisco que corran software Cisco IOS XE, si tienen activada la función Cisco IOx.
800 Series Industrial ISRs
Catalyst Access Points
CGR1000 Compute Modules
IC3000 Industrial Compute Gateways
IR510 WPAN Industrial Routers

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.02.03 14:37:04 -03'00'

Enlaces

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-8whGn5dL
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20076

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