Alerta de seguridad cibernética	9VSA23-00800-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	3 de marzo de 2023
Última revisión	3 de marzo 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 Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre vulnerabilidad crítica en Cisco Application Policy Infrastructure Controller (APIC) y Cisco Cloud Network Controlle

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

Vulnerabilidad

CVE-2023-20011

Impacto

Esta vulnerabilidad podría permitir que un atacante remoto no autenticado realice un ataque de falsificación de solicitud entre sitios (CSRF) en un sistema afectado.

Productos afectados

Cisco APIC
Cisco Cloud Network Controller

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-csrfv-DMx6KSwV
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20011

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.03.03 10:30:13 -03'00'