| | |
|---|---|
| **Alerta de seguridad cibernética** | 9VSA23-00856-01 |
| **Clase de alerta** | Vulnerabilidad |
| **Tipo de incidente** | Sistema y/o Software Abierto |
| **Nivel de riesgo** | Alto |
| **TLP** | Blanco |
| **Fecha de lanzamiento original** | 6 de julio de 2023 |
| **Última revisión** | 6 de julio 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 de una nueva vulnerabilidad que afecta a Cisco ACI Multi-Site CloudSec. La empresa aún no entrega un parche ni mitigación para esta vulnerabilidad, llamando a las organizaciones que usen los switches afectados a apagar la función vulnerable.

## Vulnerabilidades

CVE-2023-20185

## Impacto

### Vulnerabilidades de riesgo alto

CVE-2023-20185: Vulnerabilidad en la función de cifrado de Cisco ACI Multi-Site CloudSec de Cisco Nexus 9000 Series Fabric Switches en modo ACI, que podría permitir a un atacante remoto no autenticado leer o modificar tráfico entre sitios cifrado.

### Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

### Productos afectados

Cisco Nexus 9332C, 9364C, y 9500 spine switches (los últimos equipados con Cisco Nexus N9K-X9736C-FX Line Card), solo si están en modo ACI.

### Enlaces

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20185

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.07.06 11:43:31 -04'00'