# Alerta de Seguridad Cibernética

| | |
|---|---|
| Alerta de seguridad cibernética | 9VSA22-00631-01 |
| Clase de alerta | Vulnerabilidad |
| Tipo de incidente | Sistema y/o Software Abierto |
| Nivel de riesgo | Crítico |
| TLP | Blanco |
| Fecha de lanzamiento original | 9 de mayo de 2022 |
| Última revisión | 9 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 del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre nuevas vulnerabilidades (una de ellas críticas) informadas por Cisco para su Enterprise Network Function Virtualization Infrastructure Software (NFVIS).

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

## Vulnerabilidades

CVE-2022-20777
CVE-2022-20779
CVE-2022-20780

## Impacto

### Vulnerabilidad crítica

CVE-2022-20777: Vulnerabilidad que afecta la función NGIO de Enterprise NFVIS debido a restricciones insuficientes de los invitados.

### Productos afectados

Cisco Enterprise NFVIS

### Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

### Enlaces

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-NFVIS-MUL-7DySRX9
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20777
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20779
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20780