

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Ministerio del Interior y Seguridad Pública
Subsecretaría del Interior



Alerta de seguridad cibernética	9VSA23-00789-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	16 de febrero de 2023
Última revisión	16 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 Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre nuevas vulnerabilidades críticas en la biblioteca de escaneo de terceros ClamAV de Cisco.

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

Vulnerabilidad

CVE-2023-20032
CVE-2023-20052

Impacto

La explotación de las vulnerabilidades CVE-2023-20032 y CVE-2023-20052 podría permitir que el atacante ejecute código arbitrario con los privilegios del proceso de escaneo ClamAV, o bloquee el proceso, lo que resultaría en una condición de denegación de servicio (DoS).

Productos afectados

ClamAV versiones 1.0.0 y anteriores; 0.105.1 y anteriores; y 0.103.7 y anteriores

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

<https://blog.clamav.net/>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20032>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20052>