Alerta de seguridad cibernética	9VSA23-00789-02
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	23 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 la actualización sobre una vulnerabilidad crítica en la biblioteca de escaneo de terceros ClamAV de Cisco.

Cisco informó que investigó su línea de productos, con el fin de determinar los productos pudieran verse afectados por esta vulnerabilidad.

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

Secure Endpoint, anteriormente Advanced Malware Protection (AMP) para Endpoints, para Linux (1.20.2)
Secure Endpoint, anteriormente Advanced Malware Protection (AMP) para Endpoints, para MacOS (1.21.1)
Secure Endpoint, anteriormente Advanced Malware Protection (AMP) para Endpoints, para Windows (7.5.9 y 8.1.5)
Nube privada segura para terminales (3.6.0 o posterior con conectores actualizados[2])
Dispositivo web seguro, anteriormente, dispositivo de seguridad web (12.5.6 (mayo de 2023), 14.0.4-005; 14.5.1-013 (marzo de 2023) y 15.0.0-254 (abril de 2023))

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-q8DThCy
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20032
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20052

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.02.23 12:43:48 -03'00'