Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00601-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	29 de marzo de 2022
Última revisión	29 de marzo 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 una vulnerabilidad crítica en Sophos Firewall.

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

Vulnerabilidades

CVE-2022-1040

Impacto

Esta vulnerabilidad existe debido a una validación insuficiente del input del usuario en el User Portal y en Webadmin. Un atacante remoto puede enviar solicitudes especialmente diseñadas a la interfaz web y ejecutar código arbitrario en el sistema.

Su explotación exitosa podría permitir a un atacante comprometer el equipo afectado.

Productos afectados

Sophos Firewall de 17.0.0 a 18.5.3.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://www.sophos.com/en-us/security-advisories/sophos-sa-20220325-sfos-rce
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1040

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.03.29 15:11:35 -03'00'