

Alerta de seguridad cibernética	9VSA21-00525-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de noviembre de 2021
Última revisión	30 de noviembre de 2021

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 equipo CSIRT. 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 vulnerabilidades en Trend Micro Security.

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

Vulnerabilidades

CVE-2021-43772

Impactos

Vulnerabilidad de riesgo medio:

CVE-2021-43772: La vulnerabilidad permite a un usuario local eludir las restricciones de seguridad implementadas, debido a un error no especificado en la función Folder Shield de Trend Micro Security.

Productos afectados

Trend Micro Security (consumer): 15, 16, 17, 17.1, 17.2, 17.3, 17.4, 17.5, 17.6

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

<https://helpcenter.trendmicro.com/en-us/article/TMKA-10855>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43772>