

Alerta de seguridad cibernética	9VSA21-00448-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de mayo de 2021
Última revisión	25 de mayo 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, CSIRT de Gobierno, comparte vulnerabilidades que afectan a Trend Micro Home Network Security.

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

Vulnerabilidades

CVE-2021-32457
CVE-2021-32458
CVE-2021-32459

Impactos

Son consideradas como graves las siguientes dos vulnerabilidades:

CVE-2021-32457: Esta es una vulnerabilidad de escalamiento de privilegios en la función de `tdts.ko chrdev_ioctl_handle` en Trend Micro Home Network Security 6.1.567. Un atacante puede elevar privilegios detonando esta vulnerabilidad.

CVE-2021-32458: Esta es una vulnerabilidad de escalamiento de privilegios en la función de `tdts.ko chrdev_ioctl_handle` en Trend Micro Home Network Security 6.1.567. Un atacante puede elevar privilegios detonando esta vulnerabilidad.

Productos Afectados

Trend Micro Home Network Security 6.1.567

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor.

Enlaces

https://www.trendmicro.com/en_us/forHome/products/homenetworksecurity.html

https://talosintelligence.com/vulnerability_reports/TALOS-2021-1230

https://talosintelligence.com/vulnerability_reports/TALOS-2021-1231

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-32457>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-32458>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-32459>