Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00554-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de enero de 2022
Última revisión	19 de enero 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 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 múltiples vulnerabilidades en Trend Micro Deep Security Agent.

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

Vulnerabilidades

CVE-2022-23119
CVE-2022-23120

Impactos

Vulnerabilidades de riesgo bajo

CVE-2022-23119: Un usuario local con acceso a Deep Security Manager (DSM) antes de la activación del agente puede crear un archivo especialmente diseñado y ejecutar código arbitrario en el sistema con privilegios elevados.

CVE-2022-23120: La vulnerabilidad permite que un usuario local aumente los privilegios en el sistema.

Productos afectados

10.0, 10.0 U1, 10.0 U2, 10.0 U3, 10.0 U4, 10.0 U5, 10.0 U6, 10.0 U7, 10.0 U8, 10.0 U9, 10.0 U10, 10.0 U11, 10.0 U12, 10.0 U13, 10.0 U14, 10.0 U14 10.0 U16, 10.0 U17, 10.0 U18, 10.0 U19, 10.0 U20, 10.0 U21, 10.0 U22, 10.0 U23, 10.0 U24, 10.0 U28, 10.0 U26, 10.0 U27, 10.0 U28, 10.0 U29, 10.0 U30, 10.0 U31, 10.1 (Versión de funciones), 11.0, 11.0 U1, 11.0 U2, 11.0 U3, 11.0 U4, 11.0 U5, 11.0 U6, 11.0 U7, 11.0 U8, 11.0 U9, 11.0 U10, 11.0 U11, 11.0 U12, 11.0 U13, 11.0 U014, 11.0 11.0 U16, 11.0 U17, 11.0 U18, 11.0 U19, 11.0 U20, 11.0 U21, 11.0 U22, 11.0 U23, 11.0 U24, 11.0 U25, 11.0 U26, 11.0 U27, 12.0, 12.0 U0.10, 12.0 U0. , 12.0 U5, 12.0 U6, 12.0 U7, 12.0 U8, 12.0 U9, 12.0 U10, 12.0 U11, 12.0 U12, 12.0 U13, 12.0 U14, 12.0 U15, 12.0 U16, 12.0 U17, 12.0 U18, 1.0, 12.0 U21, 20,0 LTS

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://success.trendmicro.com/solution/000290104
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23119
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23120