Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00555-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de enero de 2022
Última revisión	20 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 vulnerabilidades en SolarWinds.

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

Vulnerabilidades

CVE-2021-35247

Impactos

Vulnerabilidad de riesgo medio

CVE-2021-35247: La vulnerabilidad de validación de entrada podría permitir a los atacantes crear una consulta dada alguna entrada y enviarla a través de la red sin saneamiento.

Productos afectados

15.2.5 y versiones anteriores

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35247
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35247