Alerta de seguridad cibernética	9VSA21-00450-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de mayo de 2021
Última revisión	27 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 SonicWall NSM On-Prem.

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

Vulnerabilidad

CVE-2021-20026

Impactos

Esta vulnerabilidad permite a un atacante autenticado realizar inyección de comandos OS usando una solicitud HTTP especialmente diseñada.

Productos Afectados
Sonicwall NSM On-Prem 2.2.0-R10 y anteriores.

Mitigación
Instalar las respectivas actualizaciones desde el sitio web del proveedor.

Enlaces
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0014
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20026

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.05.27 18:53:51 -04'00'