Alerta de seguridad cibernética	9VSA21-00469-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de julio de 2021
Última revisión	19 de julio 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 una vulnerabilidad que afecta a productos VPN de SonicWall.

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

Vulnerabilidad

CVE-2019-7481

Impactos

Esta vulnerabilidad permite a usuarios no autenticados ganar acceso de lectura a recursos no autorizados.

Productos Afectados

SonicWall Secure Mobile Access (SMA) 100 series
SonicWall Secure Remote Access (SRA) secure VPN appliances

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor. El mismo recomendó "desconectar inmediatamente" productos legacy, incluyendo SRA 4600/1600 (EoL 2019), SRA 4200/1200 (EoL 2016) y SSL-VPN 200/2000/400 (EoL 2013/2014).

Enlaces

https://www.sonicwall.com/support/product-notification/urgent-security-notice-critical-risk-to-unpatched-end-of-life-sra-sma-8-x-remote-access-devices/210713105333210/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7481

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.07.19 12:52:53 -04'00'