Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA21-00458-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	23 de junio de 2021
Última revisión	23 de junio 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 grave que afecta a productos de SonicWall. Esta vulnerabilidad fue descubierta en 2020, pero esta semana el proveedor presentó un nuevo parche para solucionar definitivamente problemas no resueltos por la actualización de seguridad original.

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

Vulnerabilidad

CVE-2020-5135

Impactos

La vulnerabilidad es considerada grave por el proveedor.

CVE-2020-5135 es una vulnerabilidad causada por un error de desbordamiento de buffer en SonicOS, que permite a un atacante remoto provocar denegación de servicio (DoS) y potencialmente ejecutar código arbitrario al enviar una solicitud maliciosa al firewall.

Productos Afectados

SonicOS 6.5.4.6-79n y anteriores
SonicOS 6.5.1.11-4n y anteriores
SonicOS 6.0.5.3-93o y anteriores
SonicOSv 6.5.4.4-44v-21-794 y anteriores

Mitigación

Instalar las respectivas actualizaciones desde el sitio web del proveedor.

Enlaces

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2020-0010
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5135

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.06.23 11:20:16 -04'00'