Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00639-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	17 de mayo de 2022
Última revisión	17 de mayo 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 CSIRT de Gobierno. 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 información sobre vulnerabilidades que afectan a los aparatos SonicWall SMA 1000.

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

Vulnerabilidades

CVE-2022-22282
CVE-2022-1701
CVE-2022-1702

Impacto

Vulnerabilidad de alto riesgo

CVE-2022-22282: Vulnerabilidad ocurrida debido a un error de evasión de control de acceso no autenticado, donde el acceso a un recurso específico está restringido incorrectamente.

Productos afectados

Serie SMA1000 firmware versiones 12.4.0, 12.4.1-02965 y anteriores.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor. La empresa advierte que no existen otras medidas de mitigación.

Enlaces

https://www.sonicwall.com/support/knowledge-base/security-notice-sma-1000-series-unauthenticated-access-control-bypass/220510172939820/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22282