BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2025-37
Fecha de publicación: 9/05/2025
Tema: Escalación de privilegios en SonicWall SMA
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Las vulnerabilidades afectan a la serie SMA 100, incluidos SMA 200, 210, 400, 410 y 500v:

- En 10.2.1.14-75sv y anteriores versiones.

Descripción

Se han reportado varias vulnerabilidades importantes en productos SonicWall SMA denominadas como **CVE-2025-32819 (CVSS: 8.8), CVE-2025-32820 (CVSS: 8,3) y CVE-2025-32821 (CVSS: 6,7)** todas estas vulnerabilidades permiten a atacantes autenticados inyectar comandos con privilegios administrativos.

Las vulnerabilidades se enumeran a continuación:

- **CVE-2025-32819 (puntuación CVSS: 8.8)**: una vulnerabilidad en SMA100 permite a un atacante remoto autenticado con privilegios de usuario SSL-VPN eludir las comprobaciones de recorrido de ruta y eliminar un archivo arbitrario, lo que potencialmente puede provocar un reinicio a la configuración predeterminada de fábrica.
- **CVE-2025-32820 (puntuación CVSS: 8,3)**: una vulnerabilidad en SMA100 permite que un atacante remoto autenticado con privilegios de usuario SSL-VPN pueda inyectar una secuencia de recorrido de ruta para hacer que cualquier directorio en el dispositivo SMA sea escribible.
- **CVE-2025-32821 (puntuación CVSS: 6,7)**: una vulnerabilidad en SMA100 permite que un atacante remoto autenticado con privilegios de administrador de SSL-VPN pueda inyectar argumentos de comando de shell para cargar un archivo en el dispositivo.

Un atacante con acceso a una cuenta de usuario SSL-VPN de SMA puede encadenar estas vulnerabilidades para permitir la escritura en un directorio sensible del sistema, elevar sus

privilegios a administrador de SMA y escribir un archivo ejecutable en un directorio del sistema. Esta cadena resulta en la ejecución remota de código a nivel raíz.

También se ha reportado explotación activa de múltiples vulnerabilidades de seguridad en los dispositivos de la serie SMA 100 en las últimas semanas, incluyendo CVE-2021-20035, CVE-2023-44221 y CVE-2024-38475.

Se recomienda a los administradores de sistemas de estos dispositivos actualizar sus instancias a la última versión para una protección óptima.

Solución

El proveedor a lanzado parches de seguridad para los productos SMA 100 Series *(incluyendo SMA 200, 210, 400, 410, 500v)* que corrigen estas vulnerabilidades en las versiones 10.2.1.15-81sv y superiores.

Para mas información sobre el reporte de seguridad oficial puede ir al siguiente enlace:

- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0011

Puede encontrar información de como actualizar sus dispositivos en los siguientes enlaces:

- https://www.sonicwall.com/support/technical-documentation/docs/sma_100-10-2-upgrade_guide/Content/sma-ug-obtaining-firmware.htm
- https://www.sonicwall.com/support/knowledge-base/how-to-upgrade-firmware-on-sma-100-series-in-high-availability-hardware-failover-pair/170502253823254

Información adicional:

- https://thehackernews.com/2025/05/sonicwall-patches-3-flaws-in-sma-100.html
- https://www.rapid7.com/blog/post/2025/05/07/multiple-vulnerabilities-in-sonicwall-sma-100-series-2025/
- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0011

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com