SonicWall ha publicado actualizaciones para corregir tres vulnerabilidades de seguridad detectadas en los dispositivos Secure Mobile Access (SMA) 100, las cuales podrían ser aprovechadas para ejecutar código de manera remota.

Las fallas identificadas son las siguientes:

- CVE-2025-32819 (puntaje CVSS: 8.8): Esta vulnerabilidad en los dispositivos SMA100 permite que un atacante remoto autenticado con privilegios de usuario SSL-VPN eluda los controles de validación de rutas y elimine archivos arbitrarios, lo que podría llevar a un reinicio del equipo a su configuración de fábrica.
- CVE-2025-32820 (puntaje CVSS: 8.3): Esta falla permite que un atacante remoto autenticado con permisos de usuario SSL-VPN introduzca secuencias de recorrido de directorios, logrando así que cualquier carpeta del dispositivo SMA sea modificable.
- CVE-2025-32821 (puntaje CVSS: 6.7): En este caso, un atacante con acceso de administrador SSL-VPN podría inyectar argumentos de comandos de shell para cargar archivos en el dispositivo.

> *«Un atacante con acceso a una cuenta de usuario SSL-VPN en un equipo SMA puede encadenar estas vulnerabilidades para modificar un directorio sensible del sistema, escalar sus privilegios a administrador de SMA y escribir un archivo ejecutable en un directorio del sistema»*, explicó Rapid7 en un informe. «Esta cadena permite la ejecución remota de código con privilegios de root.»

Se estima que CVE-2025-32819 es una variante no corregida adecuadamente de una vulnerabilidad previamente descubierta por NCC Group en diciembre de 2021.

La firma de ciberseguridad también indicó que esta vulnerabilidad podría haber sido utilizada como un día cero, basándose en indicadores de compromiso conocidos y análisis de incidentes. No obstante, SonicWall no ha confirmado públicamente que esta falla haya sido explotada en ataques reales.

Estas vulnerabilidades afectan a la serie SMA 100, incluyendo los modelos SMA 200, 210, 400, 410 y 500v, y han sido solucionadas en la versión 10.2.1.15-81sv del software.

Estas correcciones se producen en un contexto en el que otras fallas de seguridad en dispositivos de la serie SMA 100 han sido aprovechadas activamente en las últimas semanas, como CVE-2021-20035, CVE-2023-44221 y CVE-2024-38475. Se recomienda a los usuarios actualizar a la versión más reciente para mantener una protección adecuada.