La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE.UU. (CISA) añadió el miércoles una vulnerabilidad de seguridad que afecta a los dispositivos SonicWall Secure Mobile Access (SMA) de la Serie 100 a su catálogo de Vulnerabilidades Conocidas como Explotadas (KEV, por sus siglas en inglés), debido a evidencias de explotación activa.

Esta vulnerabilidad, clasificada como de alta severidad y registrada como CVE-2021-20035 (con una puntuación CVSS de 7.2), se debe a una inyección de comandos del sistema operativo que puede permitir la ejecución remota de código.

Según una alerta emitida por SonicWall en septiembre de 2021, la falla ocurre por una inadecuada neutralización de ciertos caracteres especiales en la interfaz de administración de SMA100. Esto permitiría que un atacante remoto, ya autenticado, ejecute comandos arbitrarios bajo el usuario «nobody», lo que potencialmente podría derivar en la ejecución de código malicioso.

Los dispositivos afectados incluyen los modelos SMA 200, 210, 400, 410 y 500v (en plataformas ESX, KVM, AWS y Azure), que estén ejecutando alguna de las siguientes versiones:

- 10.2.1.0-17sv y anteriores (corregido en 10.2.1.1-19sv y posteriores)
- 10.2.0.7-34sv y anteriores (corregido en 10.2.0.8-37sv y posteriores)
- 9.0.0.10-28sv y anteriores (corregido en 9.0.0.11-31sv y posteriores)

Aunque aún no se conocen detalles técnicos precisos sobre cómo se está explotando esta vulnerabilidad, SonicWall actualizó su comunicado reconociendo que *«esta vulnerabilidad está siendo potencialmente explotada en el entorno real».*

Las agencias del Poder Ejecutivo Civil Federal (FCEB) deben aplicar las mitigaciones necesarias antes del 7 de mayo de 2025 para proteger sus redes frente a estas amenazas activas.