Boletín de alerta

Boletín Nro.:

Fecha de publicación: 25/07/2025

Tema: Alerta 2025-65 Vulnerabilidad Grave en SonicWall SMA Serie 100

Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- SonicWall Secure Mobile Access (SMA) Serie 100
- Modelos: SMA 210, SMA 410, SMA 500v
- Versiones: 10.2.1.15-81sv y anteriores

Esta vulnerabilidad no afecta a los productos de la serie SonicWall SSL VPN SMA1000 ni a SSL-VPN que se ejecutan en firewalls SonicWall.

Descripción

Se ha identificado una **vulnerabilidad crítica** (CVE-2025-40599) en la interfaz de administración web de los dispositivos SonicWall SMA 100.
Esta falla permite a un atacante con privilegios administrativos **subir archivos maliciosos** al dispositivo, lo que podría llevar a una **ejecución remota de código (RCE)**.

Aunque **no se ha confirmado su explotación activa**, existe riesgo elevado debido a recientes ataques que, se sospechan, aprovecharon otras fallas anteriores y así como también **credenciales robadas** para comprometer dispositivos SMA 100 que habían estado completamente parcheados para implantar backdoors (“puertas traseras»).

Solución:

Actualizar inmediatamente los dispositivos a la versión **10.2.2.1-90sv o superior**.

Información adicional:

- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0014
- https://cloud.google.com/blog/topics/threat-intelligence/sonicwall-secure-mobile-access-exploitation-overstep-backdoor
- https://www.securityweek.com/sonicwall-patches-critical-sma-100-vulnerability-warns-of-recent-malware-attack/