

Boletín de alerta

Boletín Nro.: 113

Fecha de publicación: 09/10/2026

Tema: Alerta 2026-113 Vulnerabilidad SSRF crítica en SonicWall SMA1000

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Producto	Versiones afectadas	Versión corregida
SonicWall SMA1000: modelos 6210, 7210 y 8200v, rama 12.4.3	12.4.3-03526 (platform-hotfix) y anteriores	12.4.3-03670 (platform-hotfix) o posterior de la rama correspondiente
SonicWall SMA1000: modelos 6210, 7210 y 8200v, rama 12.5.0	12.5.0-02952 (platform-hotfix) y anteriores	12.5.0-03082 (platform-hotfix) o posterior de la rama correspondiente

Descripción

Se identificó una vulnerabilidad de falsificación de solicitudes del lado del servidor identificada como CVE-2026-102255 CVSSv3 10 (crítica), conocida como SSRF, en la interfaz WorkPlace de sus dispositivos Secure Mobile Access (SMA) serie 1000. La falla permite que un atacante remoto, sin autenticación, fuerce al dispositivo a realizar solicitudes en su nombre, alcance funcionalidades internas y ejecute operaciones no autorizadas.

CVE-2026-102255 se origina en una ruta alternativa de acceso no prevista dentro de la interfaz WorkPlace. Un atacante puede aprovecharla para inducir al appliance a emitir solicitudes hacia funcionalidades internas y realizar operaciones que no deberían estar disponibles sin autorización. La explotación es remota, no requiere credenciales y presenta baja complejidad.

La vulnerabilidad afecta los modelos SMA 6210, 7210 y 8200v. No afecta la serie SMA 100 ni la funcionalidad SSL-VPN de los firewalls SonicWall. El fabricante publicó los hotfixes el 6 de octubre de 2026.

Dentro del boletín de seguridad publicado sobre la vulnerabilidad mencionada y la actualización, también se corrigen otras vulnerabilidades:

CVE	Vulnerabilidad	CVSS
CVE-2026-102256	Inyección de comandos del sistema operativo	7.8
CVE-2026-102257	Traversal de rutas de tipo Zip Slip	7.2

Solución

El fabricante ha publicado un hotfix, se recomienda actualizar a 12.4.3-03670 o 12.5.0-03082, o a una versión posterior corregida de la rama aplicable. Los paquetes están disponibles mediante MySonicWall.

<https://www.mysonicwall.com>

Información adicional:

- Portal de avisos de seguridad de SonicWall: <https://psirt.global.sonicwall.com/>
Consultar el aviso SNWLID-2026-0017, identificado en el análisis de Censys.
- Portal de descarga MySonicWall: <https://www.mysonicwall.com/>
Obtener el platform-hotfix correspondiente al equipo y a su rama de firmware.
- <https://www.bleepingcomputer.com/news/security/sonicwall-warns-of-max-severity-ssrf-flaw-in-sma1000-gateways/>