

## Boletín de alerta

**Boletín Nro.:**

**Fecha de publicación:** 09/01/2025

**Tema:** Alert 2025-01-SonicWall publica Parches para Fallas Críticas de Seguridad

**Traffic Light Protocol (TLP):** Amber

## Producto(s) afectado(s):

- Múltiples productos SonicWall

## Descripción

SonicWall ha emitido parches para múltiples vulnerabilidades críticas en sus firewalls SonicOS. Entre las fallas más importantes se incluyen problemas de autenticación, escalación de privilegios y falsificación de solicitudes.

### **CVE-2024-53704: Omisión de autenticación en SSLVPN**

Una vulnerabilidad en el mecanismo de autenticación SSLVPN permite a atacantes remotos eludir la autenticación. Este problema, con una puntuación CVSS de 8.2, afecta la administración de SSLVPN y SSH, lo que lo hace susceptible de explotación activa. SonicWall recomienda actualizar al firmware más reciente para mitigar este riesgo.

### **CVE-2024-40762: Generador de tokens predecible**

El generador de tokens de autenticación en versiones afectadas de SonicOS utiliza un generador de números pseudoaleatorios (PRNG) débil, que podría ser predicho por atacantes, comprometiendo la autenticación.

### **CVE-2024-53705: Vulnerabilidad SSRF en la interfaz de administración SSH**

Una falla de falsificación de solicitudes del lado del servidor (SSRF) permite a un atacante remoto establecer conexiones TCP arbitrarias a direcciones IP y puertos específicos. Para explotar esta vulnerabilidad, el atacante debe haber iniciado sesión en el firewall.

### **CVE-2024-53706: Escalación de privilegios en SonicOS Cloud NSv**

Una falla específica en Gen7 SonicOS Cloud NSv, que afecta las ediciones de AWS y Azure, permite que un atacante autenticado con privilegios limitados eleve sus privilegios a nivel root, potencialmente

ejecutando código malicioso.

## Solución

Actualice su firmware: Instale las versiones más recientes del firmware de SonicWall para mitigar las vulnerabilidades.

## Información adicional:

- <https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0003>
- <https://www.bleepingcomputer.com/news/security/sonicwall-urges-admins-to-patch-exploitable-sslvpn-bug-immediately/>