Boletín de alerta

Boletín Nro.: 66
Fecha de publicación: 06/08/2025
Tema: Alerta 2025-66 Vulnerabilidad Zero-Day en Gen 7 SonicWall
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Gen 7 SonicWall con SSLVPN enabled:

- Versiones de *firmware* 7.2.0-7015 y anteriores.

Descripción

Se ha reportado una vulnerabilidad de Día Cero (Zero-Day) crítica sin CVE aún asignado que afecta al componente SSLVPN de SonicWall Gen 7, la misma esta siendo explotado activamente por atacantes y ya se han publicado reportes que actores maliciosos como Akira estan explotandolo para la propagación de ransomware.

Las cadenas de ataque comienzan con la violación del dispositivo SonicWall, y luego los atacantes toman una ruta posterior a la explotación «muy utilizada» para realizar enumeración, evasión de detección, movimiento lateral y robo de credenciales.

Si bien el equipo de SonicWall ha publicado una la lista de medidas de seguridad adicionales que las organizaciones pueden implementarm en lugar de deshabilitar la VPN, se recomienda encarecidamente que las organizaciones inicien un proceso de respuesta a incidentes para determinar su exposición y si ya fueron comprometidos.

En un informe de GuidePoint Security publicado el 5 de agosto de 2025, se reveló que los actores del ransomware Akira aprovecharon dos controladores de Windows, rwdrv.sys y hlpdrv.sys, como parte de una cadena de explotación Bring Your Own Vulnerable Driver (BYOVD) para desarmar el software de seguridad.

El segundo controlador, hlpdrv.sys, también se registra como servicio. Al ejecutarse, modifica la configuración de DisableAntiSpyware de Windows Defender en \REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware. El malware logra esto mediante la ejecución de regedit.exe.

Mitigación:

Mientras SonicWall investiga más a fondo, se recomienda a las organizaciones que utilizan firewalls SonicWall Gen 7 que sigan los pasos a continuación hasta nuevo aviso:

- Deshabilite los servicios VPN SSL cuando sea posible
- Limite la conectividad VPN SSL a direcciones IP confiables
- Activar servicios como Botnet Protection y Geo-IP Filtering
- Aplicar la autenticación multifactor – MFA
- Elimine las cuentas de usuario locales inactivas o no utilizadas en el firewall, en particular aquellas con acceso VPN SSL
- Fomentar la actualización periódica de contraseñas en todas las cuentas de usuario

Información adicional:

- https://thehackernews.com/2025/08/sonicwall-investigating-potential-ssl.html
- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/vulnerabilidad-0day-en-firewalls-de-sonicwall-gen-7?sstc=u88504nl572772
- https://www.sonicwall.com/support/notices/gen-7-sonicwall-firewalls-sslvpn-recent-threat-activity/250804095336430
- https://www.huntress.com/blog/exploitation-of-sonicwall-vpn
- https://arcticwolf.com/resources/blog/arctic-wolf-observes-july-2025-uptick-in-akira-ransomware-activity-targeting-sonicwall-ssl-vpn/