La empresa de ciberseguridad Huntress advirtió este viernes sobre una *"comprometida propagación generalizada"* que afecta a dispositivos SonicWall SSL VPN, permitiendo el acceso a múltiples entornos de clientes.

"Los actores maliciosos están iniciando sesión rápidamente en varias cuentas a través de dispositivos comprometidos", señaló la compañía. *"La velocidad y el alcance de estos accesos indican que los atacantes parecen tener credenciales legítimas, en lugar de recurrir a ataques de fuerza bruta."*

Se informa que gran parte de esta actividad comenzó el 4 de octubre de 2025, impactando a más de 100 cuentas de SonicWall SSL VPN pertenecientes a 16 organizaciones diferentes. En los casos analizados por Huntress, las conexiones a los dispositivos comprometidos se originaron desde la dirección IP 202.155.8[.]73.

La empresa también indicó que, en algunos incidentes, los atacantes no realizaron más acciones dentro de la red y finalizaron su conexión tras un corto periodo de tiempo. Sin embargo, en otros casos, se detectó que los actores realizaron escaneos internos y trataron de acceder a múltiples cuentas locales de Windows.

Esta revelación ocurre poco después de que SonicWall confirmara un incidente de seguridad que expuso sin autorización archivos de respaldo de configuraciones de firewall almacenados en cuentas de MySonicWall. Según la actualización más reciente, esta vulneración afecta a todos los clientes que utilizaron el servicio de respaldo en la nube de SonicWall.

"Los archivos de configuración de firewalls contienen información sensible que podría ser aprovechada por atacantes para vulnerar y obtener acceso a la red de una organización", afirmó Arctic Wolf. *"Estos archivos pueden incluir datos críticos como configuraciones de usuarios, grupos, dominios, ajustes de DNS y registro, así como certificados."*

No obstante, Huntress aclaró que hasta el momento *no existe evidencia que relacione directamente esta brecha con el reciente aumento de compromisos de seguridad*.

Dado que estos archivos pueden contener credenciales sensibles, se recomienda a las organizaciones que usan el servicio de respaldo en la nube de MySonicWall restablecer las credenciales en los firewalls activos para prevenir accesos no autorizados.

También se aconseja limitar la gestión vía WAN y el acceso remoto cuando sea posible, revocar claves API externas conectadas al firewall o sistemas de gestión, monitorear los inicios de sesión en busca de actividad sospechosa, y aplicar autenticación multifactor (MFA) para todas las cuentas administrativas y de acceso remoto.

Esta alerta coincide con un repunte de ataques de ransomware dirigidos a dispositivos firewall de SonicWall como punto inicial de acceso, utilizando vulnerabilidades conocidas (CVE-2024-40766) para infiltrarse en redes y desplegar el ransomware Akira.

En un informe publicado esta semana, Darktrace reveló que detectó una intrusión a finales de agosto de 2025 contra un cliente estadounidense no identificado, la cual incluyó escaneo de red, reconocimiento, movimiento lateral, escalamiento de privilegios mediante técnicas como *UnPAC the hash*, y exfiltración de datos.

"Uno de los dispositivos comprometidos fue identificado posteriormente como un servidor de red privada virtual (VPN) de SonicWall, lo que sugiere que el incidente forma parte de la campaña más amplia del ransomware Akira dirigida a tecnología de SonicWall", señaló el informe.

"Esta campaña llevada a cabo por los actores de Akira resalta la importancia crítica de mantener prácticas de parcheo actualizadas. Los atacantes continúan explotando vulnerabilidades ya conocidas, no sólo aquellas de día cero, lo que subraya la necesidad de una vigilancia constante incluso después de aplicar los parches."