Alerta

Técnica

Vulnerabilidades Críticas Detectadas

COLCERT AL-20250806-070

TLP:CLEAR

Una posible vulnerabilidad zero-day en los dispositivos Secure Mobile Access (SMA) VPN y firewalls de SonicWall podría estar siendo activamente explotada, permitiendo a ciberdelincuentes evadir la autenticación multifactor (MFA) y desplegar ransomware en cuestión de horas. Múltiples firmas de seguridad han reportado una ola de incidentes que comprometen redes corporativas a través de estos dispositivos, afectando incluso sistemas completamente actualizados.

El ataque implica movimientos laterales rápidos, uso de cuentas privilegiadas, eliminación de defensas y despliegue de ransomware Akira. Como medida urgente, se recomienda deshabilitar el acceso VPN de SonicWall hasta que exista un parche oficial, restringiendo severamente el acceso si esto no es posible.

SONICWALL

¿Cómo se explota esta vulnerabilidad?

- En los ataques reportados los ciberdelincuentes acceden al dispositivo SonicWall, incluso en entornos donde la autenticación multifactor (MFA) está activada, aprovechando la posible vulnerabilidad aún no parcheada.
- Tras la brecha inicial, el atacante utiliza cuentas con privilegios para escalar privilegios y obtener control sobre la red.
- Se despliegan tecnologías para la creación de túneles como Cloudflare Tunnel y OpenSSH, que permiten un acceso persistente y oculto a la red comprometida (Backdoor).
- Utilizando scripts automatizados, el atacante se encarga de extraer las credenciales en el equipo por medio del archivo NTDS.dit, almacenando las contraseñas del dispositivo de manera cifrada.
- Antes de desplegar el *ransomware*, los atacantes eliminan defensas (Antivirus) y alteran las reglas de firewall para asegurar el acceso.
- Posteriormente, eliminan las copias de seguridad para dificultar la recuperación y es entonces cuando despliegan el *ransomware* **Akira**.

El ataque es sofisticado, rápido y automatizado, apuntando a la persistencia, la escalada de privilegios y el cifrado de la mayor cantidad de sistemas, todo mientras logran evadir controles de seguridad y facilitar el impacto.

NIVEL DE RIESGO

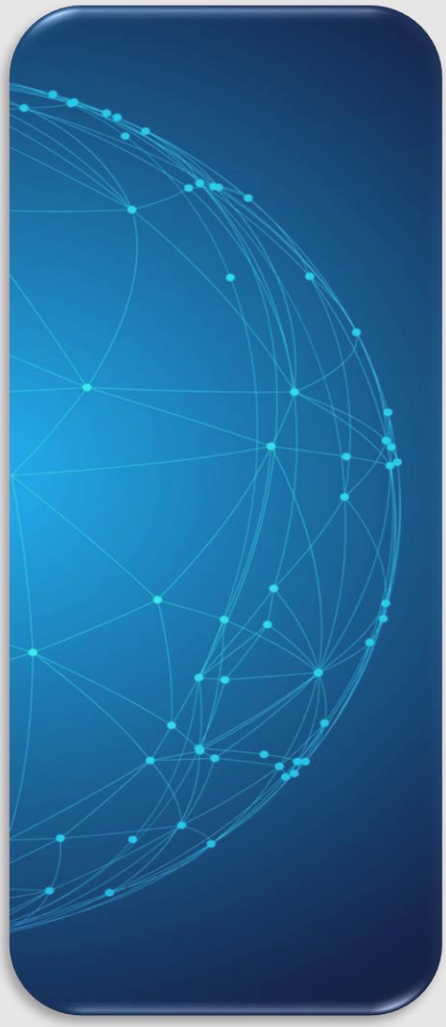
ALTO

Técnicas MITRE ATT&CK Asociadas

TÉCNICA	CÓDIGO	DESCRIPCIÓN
Explotación para ejecución remota	T1203	Los atacantes explotan vulnerabilidades en aplicaciones expuestas (como la interfaz web de SonicWall VPN) para ejecutar código arbitrario de forma remota en el equipo.
Explotación para escalamiento de privilegios	T1068	Utilizan fallos en el sistema para obtener permisos más altos de los que ya poseen, logrando el control administrativo sobre el dispositivo y, posteriormente, la red.
Recolección de datos del sistema local	T1005	El atacante accede y extrae información almacenada localmente en la red y dispositivos comprometidos, como credenciales, backups y bases de datos de Active Directory.
Uso de cuentas válidas	T1078	Se aprovechan cuentas legítimas, incluidas cuentas de servicio privilegiadas (ej. LDAP, Administrador) para moverse lateralmente y mantener acceso persistente.
Manipulación de defensas	T1562	Desactivan o evitan mecanismos de seguridad (ej. antivirus, firewalls, copias de seguridad) para facilitar la ejecución del *ransomware* y dificultar la recuperación.
Movimiento lateral	T1021	Emplean técnicas para desplazarse entre sistemas dentro de la red y expandir el alcance del compromiso

Mitigaciones MITRE

MITIGACIÓN	CÓDIGO	RELEVANCIA
Protección contra explotación	M1050	Aplicar los parches oficiales de SonicWall tan pronto como estén disponibles para corregir vulnerabilidades críticas y reducir el riesgo de explotación.
Gestión de cuentas privilegiadas	M1026	Limitar los privilegios de las cuentas de servicio y administrativas usadas por el dispositivo, aplicando el principio de menor privilegio y auditando su uso.
Segmentación de red	M1030	Restringir el acceso a la VPN y segmentos críticos de la red solo a IPs de confianza y separar lógicamente los dispositivos vulnerables para minimizar el impacto.
Monitoreo de actividad y búsqueda de IoC	M1031	Implementar monitoreo constante y búsqueda activa de Indicadores de Compromiso (IoCs) para detectar actividad sospechosa tempranamente y contener incidentes rápido.
Fortalecimiento de autenticación	M1032	Revisar y reforzar métodos de autenticación, eliminando credenciales predeterminadas o débiles y deshabilitando servicios no esenciales en los dispositivos.



Impacto para Colombia y la región

Sectores afectados: gobierno, salud, financiero, educación e infraestructura crítica, así como empresas privadas que utilicen dispositivos SonicWall para acceso remoto seguro.

Riesgo alto de ciberataques: elevada probabilidad de incidentes con ransomware (Akira), exfiltración de datos, control total de redes internas y propagación de *malware* utilizando la vulnerabilidad explotada en los dispositivos VPN.

Consecuencias: posible acceso a información sensible (bases de datos, credenciales, archivos confidenciales), interrupción de servicios operativos esenciales, afectación de la productividad y pérdida de confianza en infraestructuras críticas; además, riesgo de movimiento lateral hacia otros activos de red.

Implicaciones en seguridad digital:

- Violación de la confidencialidad, integridad y disponibilidad de la información.
- Eventual incumplimiento de normativas y regulaciones en materia de protección de datos.
- Riesgo de espionaje, robo de propiedad intelectual y afectación a la soberanía digital de organizaciones e instituciones clave.

Comunicado SonicWall

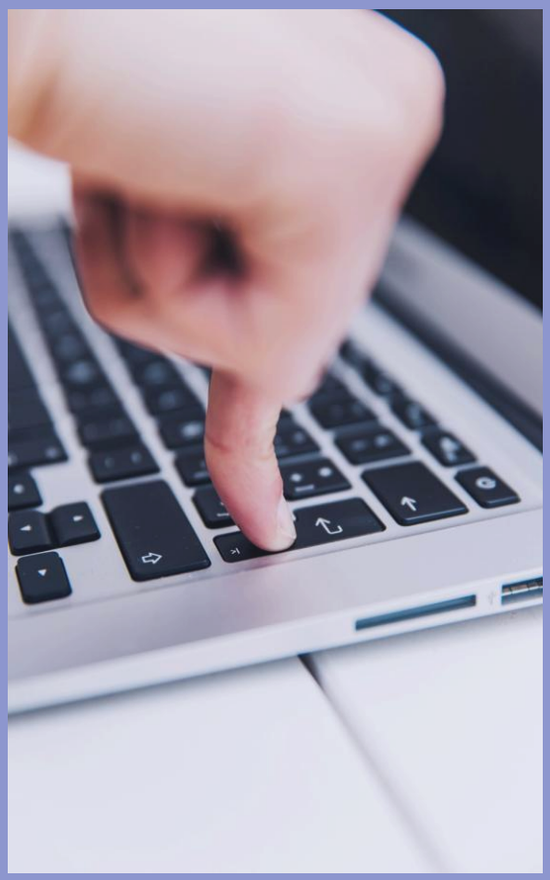
Por su parte **SonicWall emitido una advertencia URGENTE** tras el aumento significativo de los ciberataques dirigidos a sus dispositivos. La compañía y diversas firmas de seguridad se encuentran investigando si estos incidentes están relacionados con una vulnerabilidad ya conocida o si se trata de un nuevo fallo zero-day. Mientras tanto recomiendan a todos los usuarios deshabilitar el servicio de SSL VPN siempre que sea posible, limitar el acceso a IP confiables y fortalecer la autenticación para reducir la exposición mientras continúan las investigaciones.

Conclusiones

- La posible vulnerabilidad zero-day en los dispositivos SonicWall representa un riesgo crítico y real de intrusión, escalamiento de privilegios y despliegue de ransomware, incluso en entornos con autenticación multifactor activa.
- El vector de ataque permite a actores maliciosos evadir los controles de autenticación y obtener acceso remoto no autorizado, pudiendo comprometer información sensible y la continuidad operativa de sectores clave.
- La explotación activa de esta vulnerabilidad en las últimas horas evidencia que existen campañas organizadas, automatizadas y dirigidas contra organizaciones públicas y privadas en la región, afectando infraestructura crítica.
- No existe por el momento un parche definitivo debido a que aún no se determina el tipo de vulnerabilidad, por lo que la exposición de las organizaciones dependerá de la implementación inmediata de controles de mitigación.

Recomendaciones

- **Deshabilitar de inmediato el servicio SSL VPN en dispositivos SonicWall si es posible, o restringirlo únicamente a IP autorizadas y de total confianza mientras se publica un parche oficial.**
- **Auditar y limitar los privilegios de las cuentas administrativas y de servicio; eliminar credenciales y cuentas innecesarias y reforzar la gestión de accesos privilegiados.**
- **Monitorizar de forma activa la red en busca de indicadores de compromiso (IoCs) asociados a estas campañas, fortaleciendo la capacidad de detección y respuesta temprana.**
- **Segmentar adecuadamente la red para evitar movimientos laterales del atacante y garantizar que servicios y sistemas críticos se encuentren lo más aislados posible.**
- **Revisar las políticas de respaldo y recuperación, asegurando la existencia de copias fuera de línea y mecanismos de restauración rápida ante un eventual incidente de ransomware.**
- **Concienciar al personal técnico y usuarios sobre la situación de riesgo y las mejores prácticas frente a ciberataques dirigidos a la infraestructura de acceso remoto.**



Indicadores de compromiso

Item	Descripción
42.252.99[.]59	IP de atacante ubicada en Shenyang, China.
45.86.208[.]240	IP de atacante ubicada en Phoenix,, Estados Unidos.
77.247.126[.]239	IP de atacante ubicada en Las Vegas, Estados Unidos.
104.238.205[.]105	IP de atacante ubicada en Miami, Estados unidos.
104.238.220[.]216	IP de atacante ubicada en Los Angeles, Estados Unidos.
181.215.182[.]64	IP de atacante ubicada en Dallas, Estados Unidos.
193.163.194[.]7	IP de atacante ubicada en New York, Estados Unidos.
193.239.236[.]149	IP de atacante ubicada en Chicago, Estados Unidos
194.33.45[.]155	IP de atacante ubicada en Orangeburg, Estados Unidos.
w.exe SHA256: d080f553c9b1276317441894ec6861573fa64fb1fae46165a55302e782b1614d	Ejecutable de ransomware
backupSQL lockadmin	Usuarios creados por el atacante
Password123$ Msnc?42da VRT83g$%ce	Contraseñas utilizadas por el atacante
AS24863 – LINK-NET – 45.242.96.0/22 AS62240 – Clouvider – 45.86.208.0/22 AS62240 – Clouvider – 77.247.126.0/24 AS23470 – ReliableSite LLC – 104.238.204.0/22 AS23470 – ReliableSite LLC – 104.238.220.0/22 AS174 – COGENT-174 – 181.215.182.0/24 AS62240 – Clouvider – 193.163.194.0/24 AS62240 – Clouvider – 193.239.236.0/23 AS62240 – Clouvider – 194.33.45.0/24	Rangos de Red/Proveedores (ASN/CIDR)

Fuentes Oficiales

- **SonicWall, 4 de agosto de 2025, "Gen 7 SonicWall Firewalls SSL VPN Recent Threat Activity", Fuente oficial del proveedor de VPNs afectado.**
  https://www.sonicwall.com/support/notices/gen-7-sonicwall-firewalls-sslvpn-recent-threat-activity/250804095336430

- **The Record, 4 de agosto de 2025, "SonicWall urges customers to take VPN devices offline after ransomware campaign", Web de noticias de tecnología.**
  https://therecord.media/sonicwall-possible-zero-day-gen-7-firewalls-ssl-vpn

- **Cyber Security News, 4 de agosto de 2025, "SonicWall VPNs Actively Exploited for 0-Day Vulnerability to Bypass MFA and Deploy Ransomware", Web de noticias de ciberseguridad.**
  https://cybersecuritynews.com/sonicwall-vpns-exploited-for-0-day-vulnerability/

- **Cyber Security News, 5 de agosto de 2025, "SonicWall Warns of Escalating Cyberattacks Targeting Gen 7 Firewalls in Last 72 Hours", Web de noticias de ciberseguridad.**
  https://cybersecuritynews.com/gen-7-sonicwall-firewalls-attacked/

- **Huntress, "Threat Advisory: Active Exploitation of SonicWall VPNs", Sitio web de proveedor de soluciones de ciberseguridad.**
  https://www.huntress.com/blog/exploitation-of-sonicwall-vpn