Boletín de alerta

Boletín Nro.:
Fecha de publicación: 12/09/2025
Tema: Alerta 2025-75 Akira explota activamente SonicWall
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- SonicWall SMA100

Descripción

Un nuevo conjunto de vulnerabilidades en los dispositivos SonicWall de la serie SMA100 está siendo foco principal en los ataques de ransomware Akira dirigidos a la infraestructura VPN SSL de SonicWall. Estas vulnerabilidades son preocupantes, ya que podrían permitir a los atacantes ejecutar código de forma remota, lo que podría comprometer por completo el sistema.

El ransomware Akira surgió por primera vez en marzo de 2023 y desde entonces se ha convertido en una importante ciberamenaza. Akira opera bajo un modelo de ransomware como servicio (RaaS) y es conocido por usar técnicas de doble extorsión: exfiltrar datos confidenciales antes de cifrarlos y presionar a las víctimas con la exposición pública. Las demandas de rescate han oscilado entre 200.000 y 4 millones de dólares, con ganancias totales que superaron los 42 millones de dólares en 2024. A principios de 2025, más de 250 organizaciones se habían visto afectadas a nivel mundial

Información reciente sobre amenazas sugiere que las filiales de Akira podrían estar atacando la infraestructura VPN SSL de SonicWall, especialmente en entornos que carecen de autenticación multifactor o parches oportunos. Si bien las tácticas de Akira se alinean con la explotación de vulnerabilidades de internet, actualmente no hay avisos públicos que confirmen la explotación de las vulnerabilidades CVE-2025-40596 a CVE-2025-40599 por parte de Akira

CVE-2025-40599 – Carga de archivos arbitrarios autenticados

- Tipo: Atacantes autenticados por el administrador pueden cargar archivos arbitrarios a través de la interfaz de administración web.
- Impacto: Puede provocar la ejecución remota completa de código y su persistencia en el dispositivo.
- Puntuación DVE de Bitsight: 6,17 / 10
- Explotación: No se ha confirmado ninguna explotación; SonicWall advierte que esto podría ser objeto de abuso si las credenciales administrativas ya están comprometidas. Esta vulnerabilidad requiere

acceso a privilegios administrativos

CVE-2025-40596 – Desbordamiento de búfer basado en pila

- Tipo: Desbordamiento de búfer basado en pila en la interfaz web
- Impacto: Atacantes remotos no autenticados pueden bloquear el sistema (denegación de servicio) o ejecutar código remoto
- Puntuación DVE de Bitsight: 5,89/10
- Explotación: No confirmada en la práctica al momento de escribir este artículo

CVE-2025-40597 – Desbordamiento de búfer basado en montón

- Tipo: Vulnerabilidad de desbordamiento de búfer basado en montón
- Impacto: Al igual que CVE-2025-40596, permite a atacantes no autenticados activar ataques de denegación de servicio (DoS) o potencialmente ejecutar código de forma remota.
- Puntuación DVE de Bitsight: 5,82/10
- Explotación: No confirmada en la práctica al momento de escribir este artículo

CVE-2025-40598 – Cross-Site Scripting (XSS) reflejado

- Tipo: XSS reflejado a través de la interfaz web
- Impacto: Permite la inyección de JavaScript, lo que podría provocar el secuestro de sesión o el robo de credenciales
- Puntuación DVE de Bitsight: 5,82/10
- Explotación: No confirmada; podría ser útil para reconocimiento o recopilación de credenciales

Mitigación:

- Aplique todas las actualizaciones de firmware de SonicWall, incluidas las revisiones de julio de 2025 que abordan estos CVE.
- Desactive el acceso público a las interfaces web del SMA100.
- Utilice la segmentación de red y la lista blanca de IP para el acceso remoto.
- Habilite la autenticación multifactor (MFA) para todas las cuentas administrativas.
- Rote y audite las credenciales administrativas

Información adicional:

- https://www.truesec.com/hub/blog/akira-ransomware-exploiting-potential-zero-day-in-sonicwall-ssl-vpn
- https://www.threatlocker.com/blog/raas-meets-misconfiguration-how-akira-is-exploiting-sonicwall-sslvpn-weaknesses
- https://devel.group/blog/akira-ransomware-intensifica-ataques-explotando-vulnerabilidad-critica-en-sonicwall/
- https://www.bitsight.com/blog/akira-ransomware-exploits-sonicwall-sma100-vulnerabilities-what-you-need-know