Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

AKIRA RANSOMWARE INTENSIFICA ATAQUES EXPLOTANDO VULNERABILIDAD CRÍTICA EN SONICWALL

11/ 09 / 2025

CONTENIDO

INTRODUCCIÓN 3

RESUMEN 5

NOTICIA COMPLETA 5

CONTACTOS DE SOPORTE 6

INTRODUCCIÓN

El ransomware continúa posicionándose como una de las mayores amenazas para las organizaciones, aprovechando vulnerabilidades en dispositivos críticos de red para infiltrarse en entornos corporativos. En las últimas semanas, el grupo Akira, activo desde 2023, ha intensificado sus campañas explotando una falla grave en los firewalls de SonicWall, combinando además otras superficies de ataque que aumentan el riesgo para empresas de distintos sectores.

La vulnerabilidad CVE-2024-40766, con una severidad de 9.3 en la escala CVSS, sigue siendo explotada más de un año después de su divulgación. Los ataques recientes confirman que, aunque existan parches y recomendaciones disponibles, la falta de actualización y configuración adecuada continúa dejando expuestos a miles de dispositivos, abriendo la puerta a robos de datos, eliminación de respaldos y despliegue de ransomware a gran escala.

AKIRA RANSOMWARE INTENSIFICA ATAQUES EXPLOTANDO VULNERABILIDAD CRÍTICA EN SONICWALL

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_09_12_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	12/09/2025
Es día cero (0 day):	No

RESUMEN

La vulnerabilidad CVE-2024-40766, con puntaje CVSS de 9.3, afecta a dispositivos firewall de SonicWall. Se trata de un problema de control de acceso inadecuado, que puede permitir a atacantes acceder a recursos restringidos e incluso provocar la caída del dispositivo. Aunque la compañía publicó un aviso en agosto de 2024 y ha emitido recomendaciones adicionales, el fallo continúa siendo explotado en nuevas campañas.

Akira combina múltiples vectores de ataque

De acuerdo con investigadores, el grupo de ransomware Akira no solo aprovecha esta vulnerabilidad, sino que también se apoya en otras dos superficies de ataque:

- El SSLVPN Default Users Group, que permite conexiones no autorizadas a la VPN.
- El acceso al Virtual Office Portal, que a menudo está configurado como público.

La combinación de estas tres vías incrementa la efectividad de los ataques, permitiendo a los atacantes obtener acceso inicial, escalar privilegios, sustraer información sensible y desplegar ransomware a nivel de hipervisor.

Riesgos para las organizaciones

Activos desde 2023, los operadores de Akira se enfocan en dispositivos de borde para penetrar en las redes corporativas. Una vez dentro, eliminan respaldos, roban archivos críticos y ejecutan cifrado masivo, interrumpiendo operaciones de negocio y exigiendo rescates millonarios.

Recomendaciones de seguridad

SonicWall recomienda a las organizaciones:

- Aplicar de inmediato los parches de seguridad disponibles.
- Rotar contraseñas en todas las cuentas de SonicWall y habilitar la opción “User must change password”.
- Implementar MFA en servicios SSLVPN.
- Mitigar el riesgo del SSLVPN Default Group.
- Restringir el acceso al Virtual Office Portal.

Conclusión

El caso de Akira y SonicWall refleja una realidad crítica: las vulnerabilidades conocidas, aunque tengan más de un año, siguen siendo una de las puertas favoritas de los atacantes. La combinación de parches, controles de acceso robustos y monitoreo constante resulta esencial para mitigar el riesgo de ransomware en entornos empresariales.

NOTICIA COMPLETA

https://devel.group/blog/akira-ransomware-intensifica-ataques-explotando-vulnerabilidad-critica-en-sonicwall/

CONTACTOS DE SOPORTE

Correo electrónico: teamcti@devel.group

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group/