BEACON LAB
C S I R T

CYBOLT

Boletín de alerta

Boletín Nro.: 2024-28
Fecha de publicación: 09/09/2024
Tema: Alerta 2024-28 Vulnerabilidad crítica en SonicWall explotada por los autores del ransomware Akira
Traffic Light Protocol (TLP): White

Una vulnerabilidad crítica, identificada como **CVE-2024-40766** con una puntuación CVSS de **9,3**, ha sido revelada por **SonicWall**, y afecta a sus cortafuegos que ejecutan **SonicOS** en las generaciones 5, 6 y algunas versiones de 7. Esta vulnerabilidad surge de un control de acceso inadecuado a la interfaz de gestión de SonicOS y a la funcionalidad SSLVPN. El fallo permite a los atacantes obtener acceso no autorizado a recursos o provocar el fallo del cortafuegos.

Los **actores del ransomware Akira** han estado explotando activamente esta vulnerabilidad como vector de acceso inicial, comprometiendo **cuentas de usuario SSLVPN** locales, especialmente cuando **la autenticación multifactor (MFA**) está desactivada.

Recientemente, se ha observado la explotación activa de esta vulnerabilidad en varias organizaciones de **México**, por lo que urge tomar medidas inmediatas.