SonicWall ha publicado actualizaciones de seguridad para corregir una falla crítica en sus firewalls que, si es explotada con éxito, podría permitir a actores maliciosos acceder a los dispositivos sin autorización.

La vulnerabilidad, conocida como CVE-2024-40766 (con una puntuación CVSS de 9.3), ha sido descrita como un problema de control de acceso inadecuado.

> *«Se ha detectado una vulnerabilidad de control de acceso inadecuado en el acceso de gestión de SonicOS de SonicWall, lo que podría resultar en acceso no autorizado a los recursos y, en circunstancias específicas, causar que el firewall se bloquee»,* informó la compañía en un aviso emitido la semana pasada.
>
> *«Este problema afecta a los dispositivos SonicWall Firewall de la Generación 5 y 6, así como a los dispositivos de la Generación 7 que ejecutan SonicOS 7.0.1-5035 y versiones anteriores».*

El problema ha sido solucionado en las siguientes versiones:

- SOHO (Firewalls Gen 5) – 5.9.2.14-13o
- Firewalls Gen 6 – 6.5.2.8-2n (para SM9800, NSsp 12400 y NSsp 12800) y 6.5.4.15.116n (para otros dispositivos Gen 6 Firewall)

SonicWall señaló que la vulnerabilidad no se puede reproducir en versiones de firmware SonicOS superiores a 7.0.1-5035, aunque se recomienda que los usuarios instalen la última versión del firmware.

El proveedor de equipos de red no menciona que la vulnerabilidad haya sido explotada activamente. No obstante, es fundamental que los usuarios apliquen los parches lo antes posible para protegerse de posibles amenazas.

El año pasado, Mandiant, una empresa propiedad de Google, reveló que un presunto grupo de amenazas vinculado a China, identificado como UNC4540, atacó dispositivos SonicWall Secure Mobile Access (SMA) 100 sin parchear para desplegar Tiny SHell y establecer una persistencia a largo plazo.

Varios grupos de actividades vinculados a China han cambiado su enfoque hacia la infraestructura perimetral, con el objetivo de comprometer objetivos y mantener el acceso remoto sin ser detectados.

Esto incluye un conjunto de intrusiones llamado Velvet Ant, que fue descubierto recientemente utilizando una vulnerabilidad de día cero contra dispositivos Cisco Switch para distribuir un nuevo malware llamado VELVETSHELL, una versión híbrida personalizada de Tiny SHell y 3proxy.