SonicWall ha informado que una vulnerabilidad crítica de seguridad recientemente corregida en SonicOS podría haber sido explotada activamente, lo que hace crucial que los usuarios apliquen los parches lo antes posible.

La falla de seguridad, identificada como CVE-2024-40766, tiene una puntuación CVSS de 9.3 sobre 10.

«Se ha detectado una vulnerabilidad de control de acceso inadecuado en el acceso de gestión de SonicWall SonicOS y en SSLVPN, lo que podría permitir el acceso no autorizado a recursos y, bajo ciertas condiciones, provocar un fallo en el firewall», explicó SonicWall en un aviso actualizado.

En la actualización más reciente, la compañía reveló que la vulnerabilidad CVE-2024-40766 también afecta la funcionalidad SSLVPN del firewall. El problema se ha corregido 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)

El proveedor de seguridad de red ha ajustado el boletín para reflejar que la vulnerabilidad puede haber sido explotada activamente.

«Es probable que esta vulnerabilidad esté siendo explotada en el entorno», añadió SonicWall. «Se recomienda aplicar el parche lo más pronto posible en los productos afectados.»

Como medidas provisionales, se sugiere restringir el acceso de gestión del firewall a fuentes confiables o desactivar la administración WAN del firewall desde el acceso a Internet. Para SSLVPN, se recomienda limitar el acceso a fuentes seguras o deshabilitar completamente el acceso a Internet.

Otras medidas incluyen activar la autenticación multifactor (MFA) para todos los usuarios de

SSLVPN utilizando contraseñas de un solo uso (OTP) y aconsejar a los clientes que utilicen firewalls GEN5 y GEN6 con cuentas gestionadas localmente que actualicen sus contraseñas inmediatamente para evitar accesos no autorizados.

No se han revelado detalles sobre cómo podría haberse explotado la vulnerabilidad en la práctica, pero actores maliciosos chinos han aprovechado en el pasado dispositivos SonicWall Secure Mobile Access (SMA) 100 sin parches para mantener acceso persistente a largo plazo.