Más de 178,000 firewalls SonicWall que se encuentran expuestos en Internet presentan vulnerabilidades que podrían ser explotadas para causar una denegación de servicio (DoS) y ejecución remota de código (RCE), al menos una de las dos, según informes recientes.

Jon Williams, un ingeniero senior de seguridad en Bishop Fox, señaló en un análisis técnico compartido, que ambas problemáticas son esencialmente idénticas, pero pueden ser explotadas en distintas rutas de URI HTTP debido a la reutilización de un patrón de código vulnerable.

Las vulnerabilidades mencionadas son las siguientes:

- CVE-2022-22274 (puntuación CVSS: 9.4) – Se trata de una vulnerabilidad de desbordamiento de búfer basada en la pila en SonicOS a través de solicitudes HTTP, lo que permite a un atacante remoto no autenticado provocar un DoS o, potencialmente, ejecutar código en el firewall.
- CVE-2023-0656 (puntuación CVSS: 7.5) – Esta vulnerabilidad, también de desbordamiento de búfer basada en la pila en SonicOS, posibilita a un atacante remoto no autenticado causar un DoS, lo que podría resultar en un bloqueo del sistema.

Aunque no se tienen informes de explotación en el entorno real, el equipo de SSD Secure Disclosure publicó un «proof-of-concept» (PoC) para CVE-2023-0656 en abril de 2023.

Devices Vulnerable To:	Count	Percent of Total
CVE-2022-22274	146,116	62%
CVE-2023-0656	178,608	76%
Both CVEs	146,087	62%
At least one CVE	178,637	76%

La firma de ciberseguridad reveló que estos problemas podrían ser aprovechados por actores malintencionados para generar bloqueos recurrentes y obligar al dispositivo a entrar en modo de mantenimiento, requiriendo así una intervención administrativa para restaurar el funcionamiento normal.

Williams destacó que resulta sorprendente descubrir que más de 146,000 dispositivos accesibles públicamente son vulnerables a un error que se hizo público hace casi dos años.

Este desarrollo se produce tras el descubrimiento de múltiples fallos de desbordamiento de búfer basados en la pila en la interfaz web de gestión de SonicOS y en el portal SSL VPN por parte de watchTowr Labs, los cuales podrían conducir a un bloqueo del firewall.

Para protegerse contra posibles amenazas, se recomienda actualizar a la última versión y

asegurarse de que la interfaz de gestión no esté expuesta a Internet.