Boletín de alerta

Boletín Nro.: 2024-68
Fecha de publicación: 13/12/2024
Tema: Alerta 2024-68 Vulnerabilidades Críticas en SonicWall
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Los siguientes productos de la serie SMA 100 son vulnerables:

- Modelos: SMA 200, 210, 400, 410, 500v
- Versiones: 10.2.1.13-72sv y versiones anteriores

Descripción

Se han reportado dos vulnerabilidades importantes para productos afectando a productos SonicWall, especificamente al SMA100 SSLVPN, se han identificado CVE-2024-40763 y CVE-2024-45318 con una puntuación CVSSv3 7.5 y 8.1 respectivamente. Ambas están relacionadas con Desbordamiento de búfer (BoF) en la pila y head.

A continuación, se comparta la lista completa de las listas que afectan SonicWall:

- **CVE-2024-40763: Desbordamiento de búfer basado en memoria dinámica (Heap)**

Una vulnerabilidad en el manejo de cadenas de texto mediante la función strcpy permite a atacantes remotos autenticados provocar un desbordamiento de búfer basado en montón, lo que podría derivar en la ejecución de código malicioso.

Puntuación CVSS: 7,5 (Alta)

- **CVE-2024-45318: Desbordamiento de búfer basado en pila**

Un desbordamiento de búfer basado en pila en la interfaz de administración web podría permitir a atacantes remotos ejecutar código arbitrario.

Puntuación CVSS: 8,1 (Crítica)

- **CVE-2024-45319: Omisión de autenticación basada en certificados**

Esta falla permite que atacantes autenticados eviten el requisito de certificados durante el proceso de autenticación, comprometiendo la seguridad del acceso.

Puntuación CVSS: 6,3 (Media)

- **CVE-2024-53702: Aleatoriedad insegura**

El uso de un generador de números pseudoaleatorios criptográficamente débil (PRNG) puede permitir a un atacante predecir códigos de respaldo, exponiendo información sensible.

Puntuación CVSS: 5,3 (Media)

- **CVE-2024-53703: Desbordamiento de búfer basado en pila**

Una vulnerabilidad en la biblioteca mod_httprp utilizada por el servidor web Apache podría ser explotada por atacantes remotos para ejecutar código arbitrario.

Puntuación CVSS: 8,1 (Crítica)

Solución

SonicWall recomienda a todos los usuarios de la serie SMA100 actualizar a las versiones corregidas disponibles en su sitio oficial. Esto es crucial para mitigar las vulnerabilidades descritas y garantizar la seguridad de sus sistemas.

A continuación, se comparten enlaces de ayuda para realizar la actualización de sus dispositivos:

- **https://www.sonicwall.com/support**
- **https://www.sonicwall.com/support/technical-documentation/docs/sma_100-10-2-upgrade_guide/Content/sma-ug-intro.htm**
- https://www.sonicwall.com/support/technical-documentation/docs/sma_100-10-2-upgrade_guide/Content/sma-ug-obtaining-firmware.htm

Información adicional:

- **https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0018**
- https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2024-40763