مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in SonicWall SMA100 SSL-VPN

Tracking #:432316594

Date:05-12-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed SonicWall has disclosed multiple vulnerabilities affecting its SMA100 series SSL-VPN appliances.

TECHNICAL DETAILS:

SonicWall has disclosed multiple vulnerabilities affecting its SMA100 series SSL-VPN appliances. The vulnerabilities, which include path traversal, heap and stack-based buffer overflows, authentication bypass, and insecure randomness, present significant risks to users of affected devices. These vulnerabilities could allow attackers to execute arbitrary code, bypass authentication, or compromise sensitive information.

Vulnerability Details:

1. CVE-2024-38475: Path Traversal Vulnerability
   - CVSS Score: 7.5
   - Description: Allows attackers to map URLs to unintended file system locations
2. CVE-2024-40763: Heap-based Buffer Overflow
   - CVSS Score: 7.5
   - Description: Potential for remote code execution via heap-based buffer overflow
3. CVE-2024-45318: Stack-based Buffer Overflow
   - CVSS Score: 8.1
   - Description: Allows remote attackers to cause stack-based buffer overflow, potentially leading to code execution
4. CVE-2024-45319: Certificate-based Authentication Bypass
   - CVSS Score: 6.3
   - Description: Enables authenticated attackers to bypass certificate requirements during authentication
5. CVE-2024-53702: Insecure Randomness
   - CVSS Score: 5.3
   - Description: Weak pseudo-random number generation potentially exposing generated secrets.
6. CVE-2024-53703: Stack-based Buffer Overflow in mod_httprp
   - CVSS Score: 8.1
   - Description: Allows remote attackers to cause stack-based buffer overflow, potentially leading to code execution

Affected Versions:

- SMA 100 Series (SMA 200, 210, 400, 410, 500v): 10.2.1.13-72sv and earlier versions.

Fixed Versions:

- SMA 100 Series (SMA 200, 210, 400, 410, 500v): 10.2.1.14-75sv and higher versions.

RECOMMENDATIONS:

- Immediately update SonicWall SMA 100 Series to updated version to address these vulnerabilities.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0018