مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates – SonicWall SSL-VPN

Tracking #:432317522

Date:24-07-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that SonicWall has released security updates to address multiple vulnerabilities, including a critical flaw in its SMA100 Series. These vulnerabilities could allow attackers to execute arbitrary code or trigger a Denial of Service (DoS) attack.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-40599** - Post-Authentication Arbitrary File Upload Vulnerability
  - **CVSS Score**: 9.1 - Critical
  - **Description:** An authenticated arbitrary file upload vulnerability exists in the SMA 100 series web management interface. A remote attacker with administrative privileges can exploit this flaw to upload arbitrary files to the system, potentially leading to remote code execution.

- **CVE-2025-40596** - Pre-Authentication Stack-Based Buffer Overflow Vulnerability
  - **CVSS Score**: 7.3 - High
  - **Description:** A Stack-based buffer overflow vulnerability in the SMA100 series web interface allows remote, unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution.

- **CVE-2025-40597** - Pre-Authentication Heap-Based Buffer Overflow Vulnerability
  - **CVSS Score**: 7.3 - High
  - **Description:** A Heap-based buffer overflow vulnerability in the SMA100 series web interface allows remote, unauthenticated attacker to cause Denial of Service (DoS) or potentially results in code execution.

- **CVE-2025-40598** - Reflected Cross-Site Scripting (XSS) Vulnerability
  - **CVSS Score**: 6.3 - Medium
  - **Description:** A Reflected cross-site scripting (XSS) vulnerability exists in the SMA100 series web interface, allowing a remote unauthenticated attacker to potentially execute arbitrary JavaScript code.

Affected Products:

- SMA 100 Series (SMA 210, 410, 500v) - 10.2.1.15-81sv and earlier versions.

Fixed Versions:

- SMA 100 Series (SMA 210, 410, 500v) - 10.2.2.1-90sv and higher versions.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by SonicWall.

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-2025-0012
- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0014