مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in SonicWall SSL-VPN

Tracking #:432317231

Date:08-05-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in SonicWall SMA100 SSL-VPN appliances. These flaws allow authenticated attackers to delete files, modify directory access, and execute remote commands, potentially compromising device integrity and security.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-32819 - Arbitrary File Deletion (CVSS: 8.8 High)**
  - A remote authenticated attacker with SSLVPN user privileges can bypass path traversal checks, enabling the deletion of arbitrary system files—potentially triggering a factory reset.
- **CVE-2025-32820 - Path Traversal Vulnerability (CVSS: 8.3 High)**
  - An attacker can inject a path traversal sequence, making any directory on the SMA appliance writable, potentially allowing unauthorized modifications.
- **CVE-2025-32821 - Remote Command Injection (CVSS: 6.7 Medium)**
  - A remote attacker with admin privileges can inject shell command arguments to upload a file onto the appliance, creating a risk of unauthorized command execution.

Affected Products and Versions:

- **Affected Product:** SonicWall SMA 100 Series (SMA 200, 210, 400, 410, 500v)
- **Affected Versions:** 10.2.1.14-75sv and earlier

Fixed Versions:

- 10.2.1.15-81sv and later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released 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-2025-0011