GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

15 July 2026

Advisory 166:

CVE-2026-15410_SonicWall SMA1000 Appliances Code Injection Vulnerability
CVE-2026-15409_ SonicWall SMA1000 Appliances Server-Side Request Forgery Vulnerability

Release Date: 14th July 2026
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-15409 is a critical server-side request forgery (SSRF) flaw in the SMA1000 Appliance Work Place interface, which may allow remote unauthenticated attackers to cause the appliance to make requests to unintended locations. This SSRF vulnerability in Stage 1 is used to establish access that is then leveraged to exploit the code injection vulnerability in Stage 2 (CVE-2026-15410).

CVE-2026-15410 is a post-authentication improper control of generation of code (Code Injection) vulnerability identified in the SonicWall SMA1000 Appliance Management Console (AMC), which in specific conditions could potentially enable a remote authenticated attacker as administrator to execute arbitrary OS commands.

This vulnerability does not exist in isolation. In attacks observed so far, CVE-2026-15410 and CVE-2026-15409 are being exploited in tandem. The two vulnerabilities forma two-stage attack chain.

What are the systems affected?

CVE-2026-15409 and CVE-2026-15410 affect SonicWall's SMA6210, SMA7210, and SMA8200v appliances.

The confirmed affected firmware versions are:

- SMA1000 version 12.4.3 from build 03245 through build 03434 (inclusive)
- SMA1000 version 12.5.0 from build 02283 through build 02800 (inclusive)

Application Model include:
SonicWall SMA6210 - (Affected)
SonicWall SMA7210 - (Affected)
SonicWall SMA8200v - (Affected)
SMA1000 firmware 12.4.3-03245 to 12.4.3-03434 - (Affected)
SMA1000 firmware 12.5.0-02283 to 12.5.0-02800 - (Affected)
SMA1000 firmware 12.4.3-03453 and above - (Patched)
SMA1000 firmware 12.5.0-02835 and above - (Patched)

What does this mean?

Step 1 — Reconnaissance
The attacker identifies an internet-facing SonicWall SMA1000 appliance running a vulnerable firmware version. SMA1000 appliances are SSL VPN gateways typically exposed to the internet for remote access, making them straightforward to discover via Shodan or Censys scanning.

Step 2 — Stage 1: Unauthenticated SSRF via CVE-2026-15409
The attacker exploits the SSRF vulnerability in the SMA1000 Appliance Work Place interface without any credentials. This allows the appliance to be manipulated into making requests to internal or unintended network locations — enabling the attacker to probe internal services or escalate their position on the network.

Step 3 — Stage 2: Code Injection via CVE-2026-15410
Using access or credentials obtained or leveraged through Stage 1, the attacker accesses the **Appliance Management Console (AMC)** with administrator-level credentials. Through the AMC interface, they submit crafted input containing injected OS commands. Due to insufficient input validation, the application passes the injected commands to the underlying Linux OS for execution.

Step 4 — Full OS Command Execution
The injected commands execute on the appliance with OS-level privileges, giving the attacker the ability to:

- Extract VPN credentials and session tokens
- Pivot into the internal network behind the SSL VPN gateway
- Install persistent backdoors or malware on the appliance

- Modify routing or access control configurations
- Intercept VPN traffic passing through the device

Mitigation process

CERTVU recommends the following:

Primary - Apply Emergency Firmware Patch Immediately

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-15410
3. https://www.cve.org/CVERecord?id=CVE-2026-15409

.