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

3 September 2026

Advisory 243: SonicWall SMA1000 Appliance Management Console Post-Authentication OS Command Injection (CVE-2026-83549).

Release Date: 2nd September 2026
Impact: HIGH
TLP: CLEAR

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

This alert is relevant to Organizations, System/Network administrators, and remote-access/VPN engineering teams that deploy or operate SonicWall SMA1000 series secure remote access appliances. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-83549 is a high-severity, post-authentication Operating System (OS) command injection vulnerability in the Appliance Management Console (AMC) of SonicWall SMA1000 series appliances - SSL VPN secure remote access gateways widely deployed by medium to large enterprises, government agencies, and managed security service providers. Under specific conditions, a remote attacker who has already authenticated to the AMC with administrator-level privileges can submit crafted input that is passed to an underlying operating-system command without proper sanitization, allowing them to execute arbitrary OS commands and achieve remote code execution on the appliance. This CVE was disclosed alongside a companion vulnerability, CVE-2026-83548 (an unauthenticated, pre-authentication Server-Side Request Forgery flaw in the SMA1000 Work Place interface, covered separately in CERTVU Advisory 242).

What are the systems affected?

The following version(s) are affected:

- SonicWall SMA1000 firmware 12.4.3-03453 (platform-hotfix) and earlier - (Affected)
- SonicWall SMA1000 firmware 12.5.0-02835 (platform-hotfix) and earlier - (Affected)

SonicWall SMA1000 firmware 12.4.3-03526 and later, and 12.5.0-02952 and later - (Not affected, patched). Affected hardware models are the SMA 6210 and 7210 physical appliances and the SMA 8200v virtual appliance; SMA 100 series appliances and SonicWall firewalls are not affected by this CVE. The same hotfix that resolves this vulnerability also resolves the companion CVE-2026-83548.

SMA1000 appliances are self-managed and do not update automatically, so this fix will not reach an existing deployment on its own. Because real-world attackers have been observed chaining this vulnerability with the unauthenticated companion flaw (CVE-2026-83548), SonicWall recommends that administrators contact SonicWall Technical Support to review their systems for indicators of compromise, in addition to applying the hotfix.

What does this mean?

Typical attack flow:

1. **Obtain administrator-level access to the Appliance Management Console**
    - The attacker first needs valid administrator credentials for the SMA1000 Appliance Management Console (AMC) - obtained independently (e.g. phished, brute-forced, or reused/purchased credentials), or, as observed in real-world attacks, by first exploiting the unauthenticated companion vulnerability CVE-2026-83548 to gain an initial foothold on the appliance.
2. **Inject and execute arbitrary OS commands via the AMC**
    - Using the authenticated administrator session, the attacker submits crafted input to a specific AMC function whose input is passed to an underlying operating-system command without proper sanitization, executing arbitrary OS commands under specific conditions and achieving remote code execution on the appliance.

Attack vectors:

- A network-based request against any internet- or network-reachable SMA1000 appliance running an affected firmware version - but, unlike the companion CVE-2026-83548, only exploitable by an attacker who already holds administrator-level credentials to the Appliance Management Console (CVSS PR:L).
- No user interaction is required (CVSS UI:N), and real-world attackers have been observed obtaining the needed administrator-level access by first chaining the unauthenticated SSRF vulnerability in CVE-2026-83548 - making this a practical escalation step in an observed real-world attack chain, rather than a purely theoretical post-authentication risk.

Successful exploitation may allow attackers to:

- Execute arbitrary operating-system commands on the SMA1000 appliance with administrator-level privileges, achieving full remote code execution on the underlying appliance.
- When chained with the companion unauthenticated SSRF vulnerability (CVE-2026-83548), progress from no prior credentials at all to full remote code execution on the appliance — the combination that has been observed in real-world attacks — and from there use the compromised remote-access gateway as a foothold into the internal network it was deployed to protect.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor hotfix without delay

- Upgrade SMA1000 firmware to 12.4.3-03526 or 12.5.0-02952 (whichever branch applies to your deployment), where this vulnerability is fixed (SonicWall Security Bulletin SNWLID-2026-0016). This is the same hotfix that also resolves the companion CVE-2026-83548, so a single upgrade addresses both.

2. Contact SonicWall Technical Support for a compromise assessment, since real-world attackers have chained this vulnerability with the unauthenticated companion flaw to achieve full remote code execution
3. Audit the estate for SMA1000 deployments
4. Review Appliance Management Console access and credentials
5. Rotate credentials and review connected systems

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-83549
2. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0016