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 242: SonicWall SMA1000 Pre-Authentication Server-Side Request Forgery Zero-Day (CVE-2026-83548).

Release Date: 2nd September 2026
Impact: 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, 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-2026-83548 is a critical, actively-exploited zero-day, pre-authentication Server-Side Request Forgery (SSRF) vulnerability in SonicWall SMA1000 series appliances - SSL VPN secure remote access gateways widely deployed by medium to large enterprises, government agencies, and managed security service providers. The flaw exists in the appliance's Work Place interface, where an unintended alternate access path allows an unauthenticated remote attacker to reach sensitive internal functionality and perform unauthorized operations without ever presenting valid credentials. This CVE was disclosed alongside a companion vulnerability, CVE-2026-83549 (an OS command injection flaw in the SMA1000 Management Console requiring administrator-level authentication) - these advisory covers CVE-2026-83548 specifically; organizations should be aware both were patched together in the same SonicWall security bulletin.

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.

SMA1000 appliances are self-managed and do not update automatically, so this fix will not reach an existing deployment on its own. Because this is a zero-day that was actively exploited before organizations had an opportunity to patch, 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. **Reach the Work Place interface's unintended alternate access path**
    - An unauthenticated attacker sends a crafted request to a reachable SMA1000 appliance's Work Place interface, using an unintended alternate access path that bypasses the authentication normally required to reach it.
2. **Abuse the SSRF to reach sensitive internal functionality**
    - Using the same unauthenticated access, the attacker forces the appliance to make server-side requests on their behalf, reaching sensitive internal functionality and performing unauthorized operations that should only be reachable by an authenticated administrator.

Attack vectors:

- A network-based, unauthenticated request against any internet- or network-reachable SMA1000 appliance running an affected firmware version.
- No user interaction, no privileges, and no special access conditions are required (CVSS AV:N/AC:L/PR:N/UI:N) — confirmed active exploitation in the wild, prior to widespread patching, demonstrates this is being exploited in practice as a genuine zero-day.

Successful exploitation may allow attackers to:

- Gain unauthorized access to sensitive internal functionality on the SMA1000 appliance without ever presenting valid credentials, undermining the very authentication boundary the appliance exists to enforce for remote access.
- Use the compromised remote-access gateway as a foothold into the internal network it was deployed to protect, and — per SonicWall's own remediation guidance recommending full re-imaging, password resets, and TOTP reinitialization for confirmed-compromised

appliances — potentially achieve a deeper compromise of stored credentials and authentication material.

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). SonicWall has described this as a hotfix requiring immediate action given the confirmed zero-day exploitation.

2. Contact SonicWall Technical Support for a compromise assessment, since this vulnerability was actively exploited before a patch was available
3. Audit the estate for SMA1000 deployments
4. Treat any internet-reachable, unpatched appliance as potentially compromised
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-2026-83548
2. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0016