

ADVISORY !

TLP : CLEAR

DATE : 14th October 2026

REF NO : CERT-NCSOC-0231

SonicWall SMA1000 — Pre-authentication Server-Side Request Forgery (SSRF)

Severity Level: **Critical**

Components Affected

- **Product:** SonicWall Secure Mobile Access (SMA) 1000 Series.
- **Hardware models:** SMA 6210 and SMA 7210
- **Virtual appliance:** SMA 8200v, across supported hypervisor deployments.
- **Affected software branch:** Platform-hotfix version 12.4.3-03526 and earlier versions.
- **Affected software branch:** Platform-hotfix version 12.5.0-02952 and earlier versions.
- **Vulnerable interface:** Appliance WorkPlace web interface, used to provide users with secure remote access to organizational resources.

Overview

A critical pre-authentication Server-Side Request Forgery (SSRF) vulnerability has been identified in the Appliance WorkPlace interface of SonicWall Secure Mobile Access (SMA) 1000 Series appliances. The vulnerability, tracked as CVE-2026-102255, has a CVSS severity score of 10.0 (**Critical**).

The flaw results from an unintended alternate access path that may allow a remote, unauthenticated attacker to direct the affected appliance to issue requests on their behalf. Successful exploitation could enable access to internal functionality and unauthorized operations without requiring valid credentials or user interaction.

SonicWall published security advisory SNWLID-2026-0017 on 6 October 2026 and released hotfixes for the affected software branches. On 9 October 2026, subsequent security reporting described exploitation attempts consistent with this vulnerability being observed by a security researcher's honeypot network. This reporting should be distinguished from a confirmed compromise of a specific organization. SonicWall's original advisory stated that there was no evidence of exploitation in the wild at the time of publication.

ADVISORY !

TLP : CLEAR

DATE : 14th October 2026

REF NO : CERT-NCSOC-0231

Description

Server-Side Request Forgery (SSRF) is a vulnerability in which an attacker can manipulate a server-side application into sending requests to unintended destinations or internal services. Because these requests originate from the vulnerable server, they may reach functionality that is not directly accessible to the attacker.

In CVE-2026-102255, the weakness exists in the Appliance WorkPlace interface of SMA1000 appliances because of an unintended alternate access path. A remote attacker without authentication may abuse this path to cause the appliance to issue requests on the attacker's behalf and reach internal functionality, potentially performing unauthorized operations.

The principal characteristics of the vulnerability are as follows:

- **CVE-2026-102255 (CVSS 10.0 — Critical):** A pre-authentication SSRF vulnerability in the SMA1000 Appliance WorkPlace interface. A remote, unauthenticated attacker may direct the appliance to issue requests on their behalf, potentially accessing internal functionality and performing unauthorized operations.
- **Attack prerequisites:** The attacker does not require authentication or user interaction. The published CVSS vector indicates network accessibility and low attack complexity.
- **Affected software:** Platform-hotfix versions 12.4.3-03526 and earlier, and 12.5.0-02952 and earlier.
- **Exploitation status:** Security reporting dated 9 October 2026 described honeypot observations consistent with exploitation attempts. This does not independently establish successful compromise of a particular production appliance.
- **Vendor response:** SonicWall released fixed platform-hotfix versions on 6 October 2026 under advisory SNWLID-2026-0017.

ADVISORY !

TLP : CLEAR

DATE : 14th October 2026

REF NO : CERT-NCSOC-0231

Impact

- Unauthorized access to internal functionality
- Unauthorized operations
- Potential information disclosure
- Potential compromise of security boundaries
- Increased risk to remote-access infrastructure

Solution/ Workarounds

Upgrade affected appliances to the fixed platform-hotfix version for the applicable software branch:

- **12.4.3 branch:** Upgrade to 12.4.3-03670 or a later version.
- **12.5.0 branch:** Upgrade to 12.5.0-03082 or a later version.

Obtain the applicable hotfix from SonicWall's official support resources and follow the vendor's upgrade instructions. Confirm the installed version after the upgrade and verify that the remote-access service and required business functions operate correctly.

Recommended hardening and monitoring measures:

- Identify all physical and virtual SMA1000 appliances deployed across the organization, including appliances hosted on supported hypervisors.
- Review the installed platform-hotfix version on every appliance and prioritize systems running affected versions.
- Restrict administrative and remote-access interfaces to approved networks and trusted access paths wherever operationally feasible.

Reference

- <https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0017>
- <https://www.sonicwall.com/support/notices/kA1VN000002QP3G0AW>
- <https://www.cve.org/CVERecord?id=CVE-2026-102255>
- <https://www.bleepingcomputer.com/news/security/sonicwall-warns-of-max-severity-ssrf-flaw-in-sma1000-gateways>

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.