

Alert Bulletin

Bulletin N.: 113

Publication Date: 09/10/2026

Subject: Alert 2026-113 Critical SSRF Vulnerability in SonicWall SMA1000

Traffic Light Protocol (TLP): White

Affected product(s):

Product	Affected versions	Fixed version
SonicWall SMA1000: models 6210, 7210 and 8200v, branch 12.4.3	12.4.3-03526 (platform-hotfix) and earlier	12.4.3-03670 (platform-hotfix) or later of the corresponding branch
SonicWall SMA1000: models 6210, 7210 and 8200v, branch 12.5.0	12.5.0-02952 (platform-hotfix) and earlier	12.5.0-03082 (platform-hotfix) or later of the corresponding branch

Description

A server-side request forgery vulnerability identified as CVE-2026-102255 CVSSv3 10 (critical), known as SSRF, was identified in the WorkPlace interface of its Secure Mobile Access (SMA) 1000 series devices. The flaw allows a remote, unauthenticated attacker to force the device to make requests on their behalf, reach internal functionalities, and execute unauthorized operations.

CVE-2026-102255 originates in an unanticipated access side channel within the WorkPlace interface. An attacker can leverage it to induce the appliance to issue requests toward internal functionalities and perform operations that should not be available without authorization. Exploitation is remote, does not require credentials, and presents low complexity.

The vulnerability affects SMA models 6210, 7210, and 8200v. It does not affect the SMA 100 series or the SSL-VPN functionality of SonicWall firewalls. The vendor released the hotfixes on October 6, 2026.

Within the security bulletin published about the mentioned vulnerability and update, other vulnerabilities are also fixed:

CVE	Vulnerability	CVSS
CVE-2026-102256	Operating system command injection	7.8

CVE-2026-102257 Zip Slip path traversal	7.2
CVE-2026-102258 Stored cross-site scripting	5.5

Solution

The vendor has released a hotfix; it is recommended to update to 12.4.3-03670 or 12.5.0-03082, or to a later fixed version of the applicable branch. The packages are available through MySonicWall.

<https://www.mysonicwall.com>

Additional information:

- SonicWall security advisories portal: <https://psirt.global.sonicwall.com/>
Consult advisory SNWLID-2026-0017, identified in Censys analysis.
- MySonicWall download portal: <https://www.mysonicwall.com/>
Obtain the platform-hotfix corresponding to the device and its firmware branch.
- <https://www.bleepingcomputer.com/news/security/sonicwall-warns-of-max-severity-ssrf-flaw-in-sma1000-gateways/>