



An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NCSC #2610070242

NCSC Advisory

Critical Vulnerability in SonicWall: SMA1000

CVE-2026-102255

7th, October 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see <https://www.first.org/tlp/>. Please treat this document in accordance with the TLP assigned.



Description

CVE ID: CVE-2026-102255

Published: 2026-10-07

Vendor: SonicWall

Product: SMA1000

CVSS Score: 10.0

Products Affected

Product	Version
SMA1000	12.4.3-03526 (platform-hotfix) and older versions
SMA1000	12.5.0-02952 (platform-hotfix) and older versions

Impact

A Pre-authentication SSRF vulnerability exists in the SMA1000 Appliance Work Place interface due to an unintended alternate access path. By abusing this path, a remote unauthenticated attacker could potentially exploit this vulnerability to direct the appliance to issue requests on their behalf and reach internal functionality and perform unauthorized operations.

Common Weakness Enumeration (CWE)¹: CWE-918: Server-Side request forgery (SSRF), CWE-441: Unintended Proxy or Intermediary ('Confused Deputy')

Known Exploited Vulnerability (KEV) catalog²: No

Used by Ransomware Operators: N/A

¹ <https://cwe.mitre.org>

² <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>



Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from SonicWall.

- <https://www.cve.org/CVERecord?id=CVE-2026-102255>
- <https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0017>

