An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2607150226

NCSC Advisory

Multiple Vulnerabilities in SonicWall: SMA1000 Series Appliances

CVE-2026-15409 and CVE-2026-15410

15th, July 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 IDs: CVE-2026-15409 and CVE-2026-15410

Published: 2026-07-14

Vendor: SonicWall

Product: SMA1000

CVSS Score[1]: 10 and 7.2

Products Affected

Product	Version
SMA1000 models 6210, 7210, and 8200v	12.4.3-03245 <= 12.4.3-03434
SMA1000 models 6210, 7210, and 8200v	12.5.0-02283 <= 12.5.0-02800

Impact

CVE-2026-15409
A server-side request forgery (SSRF) vulnerability has been identified in the SMA1000 Appliance Work Place interface. A remote unauthenticated attacker could potentially cause the appliance to make requests to unintended location.

CVE-2026-15410
Post-authentication improper control of generation of code ('Code Injection') vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) which in specific conditions could potentially enable a remote authenticated attacker as administrator to execute arbitrary operating system commands.

Common Weakness Enumeration (CWE)[2]:

- **CVE-2026-15409**: CWE-918: Server-Side Request Forgery (SSRF)
- **CVE-2026-15410**: CWE-94: Improper Control of Gereration of Code ("Code Injection")

Known Exploited Vulnerability (KEV) catalog[3]: Yes

[1] https://www.first.org/cvss/
[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Used by Ransomware Operators: N/A

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://nvd.nist.gov/vuln/detail/CVE-2026-15409
- https://nvd.nist.gov/vuln/detail/CVE-2026-15410
- https://www.cve.org/CVERecord?id=CVE-2026-15409
- https://www.cve.org/CVERecord?id=CVE-2026-15410
- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-15409
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-15410