An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2501230151

NCSC Advisory

Critical Vulnerability in SonicWall: SMA1000 CVE-2025-23006

(CVSS:9.8)

23rd, January 2025

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-2025-23006

Published: 2025-01-22

Vendor: SonicWall

Products: SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC)

CVSS Score[1]: 9.8

Products Affected

Products	Version
SMA1000 Appliance AMC and CMC	12.4.3-02804 (platform-hotfix) and earlier versions.

Impact

Pre-authentication deserialization of untrusted data vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC), which in specific conditions could potentially enable a remote unauthenticated attacker to execute arbitrary OS commands.

Note: SonicWall PSIRT has been notified of possible active exploitation of the referenced vulnerability by threat actors.

Common Weakness Enumeration (CWE)[2]: CWE-502: CWE-502 Deserialization of Untrusted Data

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

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/v3.0/specification-document

[2] https://cwe.mitre.org

[3] 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://nvd.nist.gov/vuln/detail/CVE-2025-23006
- https://www.cve.org/CVERecord?id=CVE-2025-23006
- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002