Security Advisory 2025-004

Critical Vulnerability in SonicWall Products

2025-01-27 — v1.0

TLP:CLEAR

History:

- *27/01/2025 — v1.0 – Initial publication*

Summary

On January 22, 2025, SonicWall issued an advisory regarding a critical vulnerability in the Appliance Management Console (AMC) and Central Management Console (CMC) of the SonicWall SMA 1000. An unauthenticated, remote attacker could exploit this vulnerability to execute arbitrary code on the affected appliance. This vulnerability is being exploited in the wild [1].

It is recommended applying update as soon as possible.

Technical Details

The vulnerability `CVE-2025-23006`, with a CVSS score of 9.8, is a deserialisation of untrusted data vulnerability in the Appliance Management Console (AMC) and Central Management Console (CMC) of the SonicWall SMA 1000. An unauthenticated, remote attacker could exploit this vulnerability to execute arbitrary code and gain control over affected systems.

Products Affected

The vulnerability affects all firmware versions of the SMA1000 appliance up to 12.4.3-02804 (platform-hotfix).

Recommendations

It is strongly recommended applying updates and check for any suspicious configuration change on affected assets.

Mitigation

It is strongly recommended restricting access to the Appliance Management Console (AMC) and Central Management Console (CMC) to only trusted networks [2].

References

[1] https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002

[2] https://www.sonicwall.com/techdocs/pdf/sma_1000-12-4-admin_guide.pdf#page=653