مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in SonicWall AMC and CMC

Tracking #:432316778

Date:23-01-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in SonicWall Appliance Management Console (AMC) and Central Management Console (CMC) that could be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-23006**
- CVSS v3 Score: 9.8 (Critical)
- Critical vulnerability exists in SonicWall SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC). This pre-authentication deserialization of untrusted data vulnerability could allow a remote unauthenticated attacker to execute arbitrary OS commands.
- This vulnerability allows remote attackers to bypass authentication and potentially execute arbitrary OS commands on affected SonicWall SMA1000 installations

Affected Versions:

- 12.4.3-02804 (platform-hotfix) and earlier versions

Fixed Version:

- 12.4.3-02854 (platform-hotfix) and higher versions

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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