مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

SSRF Vulnerability in SonicWall Firewalls

Tracking #:432317273

Date:15-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a high- severity Server-Side Request Forgery (SSRF) vulnerability (CVE-2025-40595) has been disclosed in SonicWall SMA1000 appliances, specifically affecting the Work Place interface.

TECHNICAL DETAILS:

A high-severity Server-Side Request Forgery (SSRF) vulnerability (CVE-2025-40595) has been disclosed in SonicWall SMA1000 appliances, specifically affecting the Work Place interface. This flaw can be exploited by remote unauthenticated attackers using encoded URLs to trick the appliance into making unintended internal or external network requests.

Vulnerability Details:

- Vulnerability Type: Server-Side Request Forgery (SSRF)
- CVE ID: **CVE-2025-40595**
- CWE: CWE-918 - Server-Side Request Forgery (SSRF)
- CVSS v3 Score: 7.2 (High)
- CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N
- First Published: May 14, 2025
- Affected Product: SonicWall SMA1000
- Affected Versions: 12.4.3-02925 and earlier (platform-hotfix)
- Fixed Version: 12.4.3-02963 and later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade SMA1000 appliances to fixed or latest 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-2025-0010