



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



SSRF Vulnerability in SonicWall Firewalls

Tracking #:432317153

Date:01-05-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a high-severity Server-Side Request Forgery (SSRF) vulnerability, tracked as CVE-2025-2170, has been identified in the SonicWall SMA1000 Appliance Work Place interface.

TECHNICAL DETAILS:

A high-severity Server-Side Request Forgery (SSRF) vulnerability, tracked as CVE-2025-2170, has been identified in the SonicWall SMA1000 Appliance Work Place interface. This flaw allows a remote, unauthenticated attacker to manipulate the appliance into making unauthorized requests to unintended locations under specific conditions.

Vulnerability Details:

- Advisory ID: SNWLID-2025-0008
- CVE: CVE-2025-2170
- CWE: CWE-918 – Server-Side Request Forgery (SSRF)
- CVSS v3 Base 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
- Publication Date: April 30, 2025
- Affected Product: SonicWall SMA1000
- Affected Versions: 12.4.3-02907 and earlier
- Fixed Versions: 12.4.3-02925 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-2025-0008>