



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Security Updates – SonicWall Products**

Tracking #:432316179

Date:23-08-2024

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 SonicWall released security updates to address a vulnerability in its products.

## TECHNICAL DETAILS:

### Vulnerability Details:

- **CVE-2024-40766** | Base Score: 8.6 | Severity: High | Improper Access Control
  - An improper access control vulnerability exists in SonicWall SonicOS management access. This vulnerability may allow unauthorized access to resources and could potentially lead to a crash of the firewall under specific conditions.
  - Successful exploitation of this vulnerability can result in unauthorized access to sensitive management functions of the firewall, potentially leading to information compromise or service disruption.

### Impacted Versions and Respective Fixes:

Impacted Platforms	Impacted Versions	Fixed Versions
SOHO (Gen 5)	5.9.2.14-12o and older versions	5.9.2.14-13o
Gen6 Firewalls -SOHOW, TZ 300, TZ 300W, TZ 400, TZ 400W, TZ 500, TZ 500W, TZ 600, NSA 2650, NSA 3600, NSA 3650, NSA 4600, NSA 4650, NSA 5600, NSA 5650, NSA 6600, NSA 6650, SM 9200, SM 9250, SM 9400, SM 9450, SM 9600, SM 9650, TZ 300P, TZ 600P, SOHO 250, SOHO 250W, TZ 350, TZ 350W	6.5.4.14-109n and older versions	6.5.2.8-2n (for SM9800, NSsp 12400, NSsp 12800)  6.5.4.15.116n (for other Gen6 Firewall appliances)
Gen7 Firewalls - TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700, NSa 3700, NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700	SonicOS build version 7.0.1-5035 and older versions.	This vulnerability is not reproducible in SonicOS firmware version higher than 7.0.1-5035. However, SonicWall recommends to install the latest firmware

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by SonicWall.

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-2024-0015>