مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

High-Severity vulnerability in SonicWall SonicOS

Tracking #:432315610

Date:13-02-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a High-Severity vulnerability in SonicWall SonicOS that could be exploited to gain unauthorised access to affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-22394**
- CVSS v3 Score 8.6 High
- An improper authentication vulnerability exists in the SonicWall SonicOS SSL-VPN feature. This vulnerability could potentially allow a remote attacker to bypass authentication and gain unauthorized access to network.
- A successful exploit could enable a remote attacker to bypass authentication restrictions on the targeted system

Affected Products:
Gen7 - 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, NSv 270, NSv 470, NSv 870.

Affected Versions:
This issue affects only firmware version SonicOS 7.1.1-7040

Fixed Versions:
SonicOS 7.1.1-7047 and higher versions

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:

1. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0003