مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Denial of Service (DoS) Vulnerability in SonicOS

Tracking #:432318069

Date:26-11-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed SonicWall has disclosed a stack-based buffer overflow vulnerability in the SonicOS SSLVPN service, tracked as CVE-2025-40601.

TECHNICAL DETAILS:

SonicWall has disclosed a stack-based buffer overflow vulnerability in the SonicOS SSLVPN service, tracked as CVE-2025-40601. The flaw allows a remote, unauthenticated attacker to trigger a Denial-of-Service (DoS) condition, potentially causing vulnerable firewalls to crash before authentication occurs.

Although no active exploitation or publicly released proof-of-concepts have been observed, SonicWall strongly urges immediate action. The vulnerability affects multiple Gen7 and Gen8 SonicWall firewalls when the SSLVPN interface/service is enabled.

Vulnerability Details:

- CVE-2025-40601
- Severity**:** High (CVSS v3.0: 7.5)
- Type: Stack-Based Buffer Overflow
- CWE: 121 – Improper Restriction of Operations within the Bounds of a Memory Buffer:

Affected Products:

Affected Platform(s)	Affected Version(s)
Gen7 hardware 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, NSsp 15700 Gen7 virtual Firewalls (NSv) - NSV270, NSv470, NSv870 (ESX, KVM, HYPER-V, AWS, Azure)	7.3.0-7012 and older versions (7.0.1 branch is not affected)
Gen8 Firewalls - TZ80, TZ280, TZ380, TZ480, TZ580, TZ680, NSa 2800, NSa 3800, NSa 4800, NSa 5800	8.0.2-8011 and older versions

Fixed Versions:

Fixed Platform(s)	Fixed Version(s)
Gen7 hardware 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, NSsp 15700 Gen7 virtual Firewalls (NSv) - NSV270, NSv470, NSv870 (ESX, KVM, HYPER-V, AWS, Azure)	7.3.1-7013 and higher versions

Gen8 Firewalls - TZ80, TZ280, TZ380, TZ480, TZ580, TZ680, NSa 2800, NSa 3800, NSa 4800, NSa 5800	8.0.3-8011 and higher versions

RECOMMENDATIONS:

- Organizations relying on SonicWall devices for remote access or perimeter defense should apply the recommended patches or enforce access restrictions to mitigate risk.

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-2025-0016