



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Multiple Vulnerabilities in SonicWall SonicOS

Tracking #:432318864

Date:30-04-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in SonicWall SonicOS. These vulnerabilities could allow unauthorized access to management functions, path traversal to restricted services, and denial-of-service attacks through firewall crashes.

TECHNICAL DETAILS:

Vulnerability Details

- CVE-2026-0204**
Severity: High | **CVSS:** 8.0
 An improper access control vulnerability in SonicOS may allow certain management interface functions to be accessible under specific conditions, potentially enabling unauthorized access to sensitive administrative capabilities.
- CVE-2026-0205**
Severity: Medium | **CVSS:** 6.8
 A post-authentication path traversal vulnerability may allow an authenticated attacker to interact with normally restricted services, potentially expanding access within the device.
- CVE-2026-0206**
Severity: Medium | **CVSS:** 4.9
 A post-authentication stack-based buffer overflow vulnerability may allow a remote attacker with privileges to crash the firewall, resulting in denial-of-service.

Fixed Platforms	Fixed Versions
Gen6 Hardware 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	6.5.5.2-28n
Gen7 NSv - NSv 270, NSv 470, NSv 870 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, NSsp 15700 Gen7 NSv - NSV270, NSv470, NSv870 (ESX, KVM, HYPER-V, AWS, Azure)	7.3.2-7010
Gen8 Firewalls - TZ80, TZ280, TZ380, TZ480, TZ580, TZ680, NSa 2800, NSa 3800, NSa 4800, NSa 5800	8.2.0-8009

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.

ADVISORY

مجلس الأمن السيبراني

CYBER SECURITY COUNCIL



The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- <https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0004>