Security Advisory

Vulnerability List

SONICOS AFFECTED BY MULTIPLE VULNERABILITIES
8

OVERVIEW

Advisory ID	SNWLID-2026-0004
First Published	2026-04-29
Last Updated	2026-04-29
Workaround	true
Status	Applicable
CVE	CVE-2026-0204, CVE-2026-0205, CVE-2026-0206
CWE	CWE-1390, CWE-35, CWE-121
CVSS v3	8.0
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Direct Link	

SUMMARY

1) CVE-2026-0204 - SonicOS Improper Access Control Vulnerability

A vulnerability in the access control mechanism of SonicOS may allow certain management interface functions to be accessible under specific conditions.

CVSS Score: 8.0
CVSS Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CWE-1390: Weak Authentication

2) CVE-2026-0205 - SonicOS post-authentication Path Traversal vulnerability

A post-authentication Path Traversal vulnerability in SonicOS allows an attacker to interact with usually restricted services.

CVSS Score: 6.8
CVSS Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:H
CWE-35: Path Traversal

3) CVE-2026-0206 - SonicOS post-authentication Stack-based Buffer Overflow vulnerability

A post-authentication Stack-based Buffer Overflow vulnerabilities in SonicOS allows a remote attacker to crash a firewall.

CVSS Score: 4.9
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H
CWE-121: Stack-based Buffer Overflow

AFFECTED PRODUCT(S)

Affected Platforms
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
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 Gen7 NSv - NSV270, NSv470, NSv870 (ESX, KVM, HYPER-V, AWS, Azure)
Gen8 Firewalls - TZ80, TZ280, TZ380, TZ480, TZ580, TZ680, NSa 2800, NSa 3800, NSa 4800, NSa 5800

CPE(S)

WORKAROUND

Until the below patches can be applied and all affected versions are fixed, SonicWall PSIRT strongly recommends that administrators fully disable HTTP/HTTPS-based firewall management and SSLVPN on all interfaces, and restrict management access to SSH only.

Disable SonicWall firewall management access

Disable SonicWall firewall SSL-VPN access

FIXED SOFTWARE

Fixed Platforms
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
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 Gen7 NSv - NSV270, NSv470, NSv870 (ESX, KVM, HYPER-V, AWS, Azure)
Gen8 Firewalls - TZ80, TZ280, TZ380, TZ480, TZ580, TZ680, NSa 2800, NSa 3800, NSa 4800, NSa 5800

COMMENTS

GEN6 Downgrade Warning

Downgrading from 6.5.5.2-28n to any prior firmware version is not supported.

Downgrading could result in the deletion of all LDAP users and a complete reset of all MFA settings.

If a downgrade is required, all LDAP users and MFA configurations must be manually reconfigured afterward. A full configuration backup is strongly recommended before upgrading.

CREDIT(S)

Advanced Research Team at CrowdStrike

REVISION HISTORY

Version	Date	Description
1.0	29-Apr-2026	Initial Release.

REFERENCE(S)

https://www.sonicwall.com/support/notices/security-advisory-firmware-update-required-gen-6-gen-7-and-gen-8-firewalls/kA1VN000001F03x0AC