CVE-2026-0206

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-0206
State	PUBLISHED
Assigner	sonicwall
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-29 17:16:40 UTC
Updated	2026-05-05 16:12:30 UTC
Description	A post-authentication Stack-based Buffer Overflow vulnerabilities in SonicOS allows a remote attacker to crash a firewall.

Risk And Classification

Primary CVSS: v3.1 4.9 MEDIUM from ADP

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

EPSS: 0.001720000 probability, percentile 0.380520000 (date 2026-05-05)

Problem Types: CWE-121 | CWE-121 CWE-121 Stack-based buffer overflow

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	4.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	4.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Sonicwall	Nsa 2650	-	All	All	All
Hardware	Sonicwall	Nsa 3600	-	All	All	All
Hardware	Sonicwall	Nsa 3650	-	All	All	All
Hardware	Sonicwall	Nsa 4600	-	All	All	All
Hardware	Sonicwall	Nsa 4650	-	All	All	All
Hardware	Sonicwall	Nsa 5600	-	All	All	All
Hardware	Sonicwall	Nsa 5650	-	All	All	All
Hardware	Sonicwall	Nsa 6600	-	All	All	All
Hardware	Sonicwall	Nsa 6650	-	All	All	All
Hardware	Sonicwall	Sm 9200	-	All	All	All
Hardware	Sonicwall	Sm 9250	-	All	All	All
Hardware	Sonicwall	Sm 9400	-	All	All	All
Hardware	Sonicwall	Sm 9450	-	All	All	All
Hardware	Sonicwall	Sm 9600	-	All	All	All
Hardware	Sonicwall	Sm 9650	-	All	All	All
Hardware	Sonicwall	Sohow	-	All	All	All
Hardware	Sonicwall	Soho 250	-	All	All	All
Hardware	Sonicwall	Soho 250w	-	All	All	All
Operating System	Sonicwall	Sonicos	All	All	All	All
Operating System	Sonicwall	Sonicos	All	All	All	All
Hardware	Sonicwall	Tz 300	-	All	All	All
Hardware	Sonicwall	Tz 300p	-	All	All	All
Hardware	Sonicwall	Tz 300w	-	All	All	All
Hardware	Sonicwall	Tz 350	-	All	All	All
Hardware	Sonicwall	Tz 350w	-	All	All	All
Hardware	Sonicwall	Tz 400	-	All	All	All
Hardware	Sonicwall	Tz 400w	-	All	All	All
Hardware	Sonicwall	Tz 500	-	All	All	All
Hardware	Sonicwall	Tz 500w	-	All	All	All

Hardware	Sonicwall	Tz 600	-	All	All	All
Hardware	Sonicwall	Tz 600p	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	SonicWall	SonicOS	affected 6.5.5.1-6n and older versions	Linux, Gen6, Gen7, Gen8
CNA	SonicWall	SonicOS	affected 7.0.1-5169 and older versions	Linux, Gen6, Gen7, Gen8
CNA	SonicWall	SonicOS	affected 7.3.1-7013 and older versions	Linux, Gen6, Gen7, Gen8
CNA	SonicWall	SonicOS	affected 8.1.0-8017 and older versions	Linux, Gen6, Gen7, Gen8

References

Reference	Source	Link	Tags
psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0004	PSIRT@sonicwall.com	psirt.global.sonicwall.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.