CVE-2026-19868

SonicWall SonicOS SSLVPN Use of Single-factor Authentication Vulnerability

CISA KEV since Nov 6, 2026 | Actively exploited

An authentication enforcement vulnerability in SonicOS SSLVPN service may allow a user with valid credentials for an alternate authentication method to bypass SAML authentication controls. Successful exploitation may also bypass SAML-enforced multi-factor authentication (MFA).

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
75/100	7.5	—	Nov 20, 2026
Urgent priority	High · NVD	Not scored	CISA federal deadline in 14 days

Signals behind the score

☑ counted in the score ☐ not counted — evidence for 5 of 8 signals

☑ **CISA KEV**	Listed in the catalog	☐ **Vendor exploitation**	Confirmed exploitation in the wild
☐ **Ransomware**	No known ransomware campaign association	☑ **KEV recency**	Added to CISA KEV within the last 30 days
☐ **EPSS**	EPSS score not yet published - scored at FIRST's population median until known	☐ **Pre-patch disclosure**	Disclosure status unavailable
☑ **CVSS**	Base score 7.5	☐ **Microsoft Exploitability Index**	Not a Microsoft CVE

Remediation

Patch This Cycle — Untagged reference available; patch status is not confirmed

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
SonicWall / SonicOS SSLVPN	–	no fixed version listed	NVD

Sources

Vendor guidance	psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0014	**Additional guidance**	cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-19868
BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk	**Forensics Triage Requirements**	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk
NVD	nvd.nist.gov/vuln/detail/CVE-2026-19868	**CISA KEV**	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-118429	**Current data**	evulnable.com/vulnerability-management/cve/CVE-2026-19868

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.