contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

SonicWall SonicOS SSLVPN exploited

CVE-2026-19868 · on CISA's exploited list since 6 November 2026

Analysis Report

Organisations running SonicWall SonicOS SSLVPN on the affected versions with SAML authentication enabled must act by 20 November 2026. First, confirm which firmware version is installed and whether …

PREPARED BY	NamiQ	DATE	6 November 2026
FACTS AS OF	6 November 2026	VERSION	1.0
SEVERITY	**High: CVSS 3.1 7.5**	STATUS	On CISA's exploited list; due 20 November 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/sonicwall-sonicos-sslvpn-cve-2026-19868

The bottom line

> *Organisations running SonicWall SonicOS SSLVPN on the affected versions with SAML authentication enabled must act by 20 November 2026. First, confirm which firmware version is installed and whether SAML is configured on the SSLVPN service.*

At a glance

Fact	Detail
Product	SonicWall SonicOS SSLVPN (CVE-2026-19868)
Severity	High: 7.5 (CVSS 3.1)
CISA	On its exploited list since 6 November 2026. Deadline for US federal agencies: 20 November 2026.
Chance of exploitation (EPSS)	Not available yet
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	No source we read names a fixed version
Who looks first	Organisations running SonicOS SSLVPN on version 7.3.3-7015 or older, or 8.2.2-8015 or older, with SAML authentication configured for the SSLVPN service.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run SonicWall SonicOS SSLVPN?	Nothing to do for this CVE.	Check the firmware version you run (next question).
Is your SonicOS version 7.3.3-7015 or older, or 8.2.2-8015 or older?	The record does not list your version as affected; monitor for further vendor guidance.	Check whether SAML authentication is enabled on the SSLVPN service (next question).
Is SAML authentication configured on the SSLVPN service?	The bypass described in the record requires SAML; apply any available patch this cycle.	Act now — the SAML and MFA enforcement may be bypassable.

What it is

An attacker who holds valid credentials for any non-SAML login method can bypass SAML authentication controls on the SSLVPN service, including any multi-factor authentication enforced through SAML.

Why it matters

SAML is typically deployed to enforce MFA for remote access. This flaw undermines that entire control: an attacker who already holds any alternate-method credentials can complete a VPN session as though MFA had been satisfied. The record's score is 7.5 (CVSS 3.1). Our reading is that the practical impact is higher for organisations that treat SAML as their sole MFA backstop for SSLVPN access, because successful exploitation removes that layer entirely without any visible failure. The root cause, CWE-308, is that a single-factor code path is not barred from completing a session that the SAML-enforced path was meant to gate.

Things people will get wrong

- "We have MFA on SSLVPN, so we are not affected." The record says this flaw bypasses SAML-enforced MFA specifically. An alternate-method login can complete the SSLVPN session without passing through the SAML flow.
- "An attacker needs to know our SAML configuration to exploit this." The record says exploitation requires valid credentials for an alternate authentication method, not knowledge of the SAML setup.

How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page before you run them. Words in capitals are for you to fill in.

Step 1: Find the firmware version on each SonicWall device

- Log into the SonicWall management interface and record the firmware version. The record lists 7.3.3-7015 and older, and 8.2.2-8015 and older, as affected.

```
show version
```

Step 2: Check whether SAML authentication is configured on SSLVPN

- In the management interface, review the SSLVPN authentication settings. If SAML is not in use, document that finding; the described bypass path requires it.

Step 3: Apply vendor mitigations

- Until a patch is confirmed, assess whether alternate-method logins to the SSLVPN can be restricted, or whether SSLVPN exposure can be reduced at the network boundary.

Step 4: Verify and record the outcome

- After applying any mitigation, confirm the firmware version installed, re-check the SSLVPN authentication configuration, and record the version and the date of change.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then. CISA's wording adds that you should stop using the product if no mitigation is available.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *We are writing regarding CVE-2026-19868, a vulnerability in SonicWall SonicOS SSLVPN. CISA has set a remediation deadline of 20 November 2026. The flaw allows a user with valid credentials for an alternate authentication method to bypass SAML authentication controls, including any SAML-enforced multi-factor authentication. Affected versions are SonicOS 7.3.3-7015 and older, and 8.2.2-8015 and older. No fixed version has been confirmed in the public record at the time of our review. Please confirm whether we run SonicOS SSLVPN, on which devices, which firmware version is installed, and whether SAML authentication is configured on the SSLVPN service. Please apply any available vendor patch or workaround and provide written confirmation of the firmware version in place and the fix applied by 19 November 2026.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Authentication log entries showing successful SSLVPN sessions completed via a non-SAML method (local, LDAP, or RADIUS) for accounts where SAML was the configured and expected path.
- SSLVPN session records for accounts that hold both a SAML identity and an alternate-method credential, particularly where the session did not follow the SAML flow.

The weakness behind it

The record classes this as CWE-308 (Use of Single-factor Authentication).

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so
External Remote Services (T1133): Using a remote-access service such as a VPN or remote desktop to get into the network.	Initial Access: getting in	SSLVPN is an external remote access service; exploiting this auth bypass would likely be used to gain initial access through that service without satisfying MFA.
Valid Accounts (T1078): Logging in with a real account the attacker should not have, so the activity looks like normal use.	Initial Access: getting in	Exploitation requires valid credentials for an alternate authentication method; an attacker would use those valid accounts to bypass the SAML-enforced control.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

CISA's catalogue entry:

> *SonicWall SonicOS SSLVPN contains a use of single-factor authentication vulnerability that 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).*

The CVE record, published by Sonicwall on 6 November 2026:

> *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).*

Versions of SonicWall SonicOS the record lists as affected:

- 7.3.3-7015 and older versions
- 8.2.2-8015 and older versions

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-19868
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the hardware (maker, model, firmware), the running container images with their operating system and packages, and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on

it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-19868
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- It is not stated whether a workaround — such as disabling alternate authentication methods for SSLVPN — is available or supported.
- The record does not state what level of network access an attacker requires, nor whether the SSLVPN service must be internet-facing for exploitation.
- It is not stated whether devices running SonicOS in configurations other than SSLVPN are affected.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 6 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-19868: score 7.5, `CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:L/A:N` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	High	Needs conditions outside the attacker's control.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Changed	Damage reaches beyond the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	Low	Some data or behaviour can be altered.
Availability	None	No effect on availability.

Appendix 2. Timeline

Date	Event
6 November 2026	CVE record published by Sonicwall.
6 November 2026	CISA added it to its list of exploited vulnerabilities.
20 November 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
SSLVPN on an affected version with SAML/MFA enabled, reachable from the internet	High	By 20 November 2026
SSLVPN on an affected version with SAML enabled, internal access only	Medium	This patch cycle
SSLVPN on an affected version without SAML configured	Medium	This patch cycle
SonicOS device with SSLVPN disabled entirely	Low	Next patch cycle

Appendix 4. Definition of done

- Every SonicWall SonicOS SSLVPN you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-19868: https://www.cve.org/CVERecord?id=CVE-2026-19868
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Reference in the CVE record: psirt.global.sonicwall.com: https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0014