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

Anyone running SonicWall SonicOS SSLVPN on version 7.3.3-7015 or older, or 8.2.2-8015 or older, needs to act by 20 November 2026. Find out which SonicOS version each device runs and whether SAML is …

PREPARED BY	NamiQ	DATE	10 November 2026
FACTS AS OF	10 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

> *Anyone running SonicWall SonicOS SSLVPN on version 7.3.3-7015 or older, or 8.2.2-8015 or older, needs to act by 20 November 2026. Find out which SonicOS version each device runs and whether SAML is configured for SSLVPN.*

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)	0.01, the estimated chance in the next 30 days, as at 10 November 2026
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 SonicWall firewalls with SonicOS SSLVPN and SAML authentication configured. The record lists SonicOS 7.3.3-7015 and older, and 8.2.2-8015 and older, as affected.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run any SonicWall firewalls with the SSLVPN service enabled?	Nothing to do for this CVE.	Check the SonicOS version (next question).
Is your SonicOS version 7.3.3-7015 or older, or 8.2.2-8015 or older?	Not in the affected range the record names.	Check whether SAML is configured for SSLVPN (next question).
Is SAML configured as an authentication method for your SSLVPN?	This specific bypass does not apply to your setup.	Treat as exposed and apply vendor mitigations before 20 November 2026.

Is the SSLVPN reachable from the internet by untrusted users?	Risk is lower, but internal users with alternate credentials could still exploit it.	Act immediately; do not wait for the CISA deadline.

What it is

A person who already holds valid credentials for a non-SAML login method can use those to reach the SSLVPN while skipping the SAML authentication check. If that SAML configuration also enforces multi-factor authentication, the second factor is bypassed too.

Why it matters

SSLVPN is typically the main remote-access gateway, so a bypass there converts an alternate credential directly into network access with no second factor required. The record's weakness is CWE-308: the system accepts a credential from one pathway to satisfy an enforcement rule set by another. SAML-enforced MFA is often the sole strong control on remote entry; removing it leaves the VPN protected only by whatever the alternate method requires. Our reading is that the practical impact exceeds what the EPSS of 0.00532 suggests, because the value lies not in the exploit itself but in the unimpeded network access it delivers.

Things people will get wrong

- We have MFA enabled so we are protected. The record says SAML-enforced MFA is specifically what this flaw bypasses. If SAML enforces your MFA on SSLVPN, that protection is removed by this vulnerability.
- An attacker needs no credentials to exploit this. The record requires valid credentials for an alternate authentication method. This targets accounts with more than one login path configured, not anonymous access.

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 SonicOS version on each device

- Log in to the SonicOS management interface and note the firmware version shown on the dashboard or system status page.

- Compare against the affected ranges in the record: 7.3.3-7015 and older, and 8.2.2-8015 and older.

```
show version
```

Step 2: Check whether SSLVPN and SAML are both active

- In the SonicOS management interface, confirm whether the SSLVPN service is enabled.
- Check the authentication settings for SSLVPN and note whether SAML is listed as an active method.

```
show sslvpn status
```

Step 3: Apply vendor mitigations

- CISA's required action is to apply mitigations per vendor instructions. No vendor advisory was available at publication; seek current guidance directly from SonicWall.
- No source names a fixed version. Confirm the correct target version with SonicWall before scheduling an update.

Step 4: Review SSLVPN authentication logs

- Check SSLVPN session logs for successful logins by accounts that have alternate authentication methods and show no corresponding SAML authentication event.
- Look for non-SAML login events immediately followed by SSLVPN session establishment for the same account.

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 about CVE-2026-19868, an authentication bypass in SonicWall SonicOS SSLVPN. The flaw allows a user with valid alternate-method credentials to skip SAML authentication, including any SAML-enforced multi-factor authentication. Affected versions are SonicOS 7.3.3-7015 and older, and 8.2.2-8015 and older. CISA has set a remediation deadline of 20 November 2026. Please confirm whether we run SonicOS SSLVPN, the exact version on each device, and whether SAML authentication is configured. We would like written confirmation of the version in use and of any mitigations applied, by 18 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:

- SSLVPN session logs for successful logins by accounts with alternate authentication configured, where no SAML authentication event appears in the same session.
- Authentication logs showing a non-SAML login event immediately followed by an SSLVPN session establishment for the same account.
- SSLVPN activity from accounts that have both SAML and alternate methods configured, particularly at unusual times or from unexpected source addresses.

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 a network-reachable access gateway; a bypass here would likely be used as the entry point into the protected network, circumventing the required SAML step entirely.
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	The record requires valid alternate-method credentials; this points to an attacker using an existing account's secondary login path to satisfy the VPN check without completing MFA.
Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	The flaw is an authentication enforcement gap in a network-facing service; exploitation would typically target this weakness as the route past the authentication gate.

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

- No source names the version that first resolves this flaw; that should be confirmed directly with SonicWall before patching.
- The sources do not say whether a workaround exists short of patching, such as disabling alternate authentication methods for SSLVPN.
- It is not stated whether the bypass applies when the alternate method is a local account only, or also when it is a third-party identity provider.
- The record does not say whether SAML configurations for services other than SSLVPN within SonicOS are also affected.

- We have not tested this against any environment. Versions and scores are as the sources state them and as at 10 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
Affected SonicOS version, SSLVPN with SAML configured, reachable from the internet	High	Before 20 November 2026
Affected SonicOS version, SSLVPN with SAML configured, internal access only	Medium	This week
Affected SonicOS version, SSLVPN enabled but SAML not configured	Low	Next patch cycle

Affected SonicOS version, SSLVPN disabled	Low	Next patch cycle
SonicOS version newer than those the record names as affected	None	No action needed for this CVE

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