contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Volans NGFW Next-Generation Firewall: new CVE

CVE-2026-135797 · record published 24 November 2026

Analysis Report

Anyone running Volans NGFW r5.1 with the SSLVPN Client feature active must act immediately: the exploit is publicly available and no fixed version is confirmed. Disable the SSLVPN Client or block …

PREPARED BY	NamiQ	DATE	25 November 2026
FACTS AS OF	25 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 4.0 10.0**	STATUS	Not on CISA's exploited list; exploitation not recorded

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/volans-ngfw-next-generation-firewall-cve-2026-135797

The bottom line

> *Anyone running Volans NGFW r5.1 with the SSLVPN Client feature active must act immediately: the exploit is publicly available and no fixed version is confirmed. Disable the SSLVPN Client or block untrusted access to it now.*

At a glance

Fact	Detail
Product	Volans NGFW Next-Generation Firewall (CVE-2026-135797)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by VulDB on 24 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 25 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	No source we read names a fixed version
Who looks first	Anyone operating Volans NGFW at version r5.1 with the SSLVPN Client feature enabled. The risk is highest where the SSLVPN interface is reachable from the internet or an untrusted network.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Volans NGFW in your estate?	Nothing to do for this CVE.	Check which version is installed.
Is the installed version r5.1?	The record lists only r5.1 as affected; monitor vendor communications.	Check whether the SSLVPN Client feature is enabled.
Is the SSLVPN Client feature currently enabled?	Risk is substantially reduced; monitor for a confirmed fix.	Determine whether untrusted users can reach the SSLVPN interface.
Can untrusted users reach the SSLVPN interface over the network?	Restrict access to trusted hosts and monitor for a vendor-confirmed fix.	Disable the SSLVPN Client or block access immediately.

What it is

The record describes an OS command injection flaw in the SSLVPN Client of Volans NGFW r5.1. A remote attacker who can reach the SSLVPN interface can supply a crafted value in the img argument to run arbitrary commands on the operating system of the device.

Things people will get wrong

- My NGFW is not internet-facing, so this does not apply. The record says the attack can be executed remotely; any network path to the SSLVPN interface on r5.1 is a risk. Not internet-facing is not the same as unreachable.
- The vendor will release a fix shortly. The record says the vendor did not respond to disclosure. No patch and no workaround have been published by any source read for this note.

How we would triage it

This is our judgement.

Step 1: Find the version you are running

- Check the management console or documentation for the installed version of Volans NGFW. The record names r5.1 as the affected version.
- If you cannot determine the version from the interface, consult your supplier or deployment records.

Step 2: Check whether the SSLVPN Client is active

- In the firewall's administration interface, review which features and services are currently enabled.
- If the SSLVPN Client is not needed, disable it until a confirmed fix is available.

Step 3: Reduce exposure for the SSLVPN interface

- If the SSLVPN Client must remain active, restrict network access to the interface to trusted IP ranges only.
- Review firewall rules to confirm that untrusted external users cannot reach the SSLVPN interface.

Step 4: Monitor for a vendor fix

- No fixed version is named in any source; monitor the Volans vendor's official channels for a security advisory or updated release.
- The record says the vendor did not respond to disclosure; allow extra time before assuming a patch will arrive promptly.

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.

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-2026-135797, a command injection flaw in the SSLVPN Client of Volans NGFW r5.1. The exploit is publicly available and no patch has been confirmed by the vendor. Please can you tell us: whether we run Volans NGFW and which version; whether the SSLVPN Client is enabled; what network access controls apply to the SSLVPN interface. The affected version is r5.1 and no fixed version is known. We would like written confirmation of the installed version and of any remediation steps taken by [your chosen date].*

The weakness behind it

The record classes this as CWE-78 and CWE-77.

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
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 record describes a remotely exploitable flaw in a network-facing SSLVPN component; exploiting a public-facing application would likely be the method of initial access.

Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	CWE-78 and CWE-77 describe command injection; this would typically result in commands executed via the host's command interpreter.

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

The CVE record:

> *A vulnerability was identified in Volans NGFW Next-Generation Firewall r5.1. Impacted is the function exec of the file sslvpn/sslvpn_client.php of the component SSLVPN Client. Such manipulation of the argument img leads to os command injection. The attack can be executed remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.*

Versions of Volans NGFW Next-Generation Firewall the record lists as affected:

- r5.1

The record gives no version ranges. Use the vendor's advisory for the affected versions.

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-2026-135797
```

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-2026-135797
```

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 a fixed version. It is not known whether the vendor intends to publish a patch or when.
- The record does not say whether authentication is required before the vulnerable parameter can be reached.
- No workaround has been published; the vendor did not respond to the researcher's disclosure.
- It is not known whether versions of Volans NGFW other than r5.1 are affected.
- Exploitation is not recorded. That is not the same as none.
- This is a new record: scores, versions and wording can change in the first days, and they are as at 25 November 2026. We have not read the vendor's advisory page and we have not tested it.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "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-2026-135797: score 10, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:P`
As the CVE record gives it.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Attack requirements	None	Works against a default deployment.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	High	Total loss of confidentiality.
Vulnerable system: integrity	High	Total loss of integrity.
Vulnerable system: availability	High	Total loss of availability.
Subsequent systems: confidentiality	High	Total loss of confidentiality.
Subsequent systems: integrity	High	Total loss of integrity.
Subsequent systems: availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
24 November 2026	CVE record published by VulDB.

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
Volans NGFW r5.1, SSLVPN Client enabled, interface reachable from the internet or an untrusted network	Medium	Immediately

Volans NGFW r5.1, SSLVPN Client enabled, access restricted to internal trusted hosts only	Medium	This week
Volans NGFW r5.1, SSLVPN Client confirmed disabled	Low	Next patch cycle
Volans NGFW running a version other than r5.1	Low	Monitor for vendor advisory
No Volans NGFW in the estate	None	None for this CVE

Appendix 4. Definition of done

- Every Volans NGFW Next-Generation Firewall you run is listed, with its version.
- Each is outside the affected list, or the vendor's fix or mitigation is in place.
- The version output or a screenshot is saved with the date.
- Anything not done has an owner and a date.

Sources

- CVE record for CVE-2026-135797: https://www.cve.org/CVERecord?id=CVE-2026-135797
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/442767
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/442767/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-135797