contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

25 November 2026 · 3 new critical CVEs worth reading

Analysis Report

171 new records scored 8 or higher in the last 30 hours. 3 to read first, and the conditions each score leaves out.

PREPARED BY	NamiQ	DATE	25 November 2026
FACTS AS OF	25 November 2026	VERSION	1.0
TOP SCORE	Critical: 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/daily-cve-highlight-2026-11-25

The bottom line

> *3 new records scored 8 or higher and nothing says yet that anyone is using them. If you run any of these products, check the version today.*

899 CVE records were published in the last 30 hours. 171 scored 8 or higher. 3 are below, chosen by a fixed rule: highest score first, then fewest conditions in the wording, one product each. None is on CISA's exploited list, so a score here is the record's author describing the worst case. Read the condition before you act on the number.

At a glance

Product	Score	Fixed in	Read next
Volans NGFW Next-Generation Firewall (CVE-2026-135797)	10 (CVSS 4.0)	See the note	Technical Analysis
Netis WF2409E (CVE-2026-136136)	10 (CVSS 4.0)	See the note	Technical Analysis
Tenda RX3 (CVE-2026-136547)	10 (CVSS 4.0)	See the note	Technical Analysis

Volans NGFW Next-Generation Firewall, CVE-2026-135797

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.

Score 10 (CVSS 4.0), published by VulDB on 24 November 2026. Weakness: CWE-78, CWE-77.

A word search of the record found none of the usual conditions (privileges, a logged-in user, a non-default setting, local network, physical access, a click). That is a search, not a reading, so read the record yourself before you rule it out.

Netis WF2409E, CVE-2026-136136

Any owner of a Netis WF2409E running firmware 20261026 or earlier should act now — no patch is recorded and an exploit is publicly available. As a first step, block access to the router's web management interface from untrusted networks.

Score 10 (CVSS 4.0), published by VulDB on 24 November 2026. Weakness: CWE-287.

A word search of the record found none of the usual conditions (privileges, a logged-in user, a non-default setting, local network, physical access, a click). That is a search, not a reading, so read the

record yourself before you rule it out.

Tenda RX3, CVE-2026-136547

Anyone running a Tenda RX3 on firmware 16.03.13.11_multi should act immediately — the exploit is publicly disclosed, the score is 10, and no fixed firmware is recorded. Disable remote management access from the internet as a first step.

Score 10 (CVSS 4.0), published by VulDB on 25 November 2026. Weakness: CWE-287.

A word search of the record found none of the usual conditions (privileges, a logged-in user, a non-default setting, local network, physical access, a click). That is a search, not a reading, so read the record yourself before you rule it out.

Fifteen minutes this morning

- List the products above you run. If none, you are done.
- For each one you run, read the version from the product and compare it to the fixed version in the table.
- If it is in range, follow the note: reduce exposure first, then update.
- Book the update, and write down who owns it and by when.

Check your own project

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

```
lattice-scan project . --cve CVE-2026-135797,CVE-2026-136136,CVE-2026-136547
```

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 ids 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 --cve CVE-2026-136136 --cve CVE-2026-136547
```

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

- These are new records. A record can change in the first days: scores, versions and wording are as at 25 November 2026. Nothing here has been tested.
- Exploitation is not recorded for any of them. That is not the same as none.

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`

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.

CVE-2026-136136: 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`

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.

CVE-2026-136547: 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`

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	Volans NGFW Next-Generation Firewall, CVE-2026-135797: record published by VulDB.
24 November 2026	Netis WF2409E, CVE-2026-136136: record published by VulDB.
25 November 2026	Tenda RX3, CVE-2026-136547: record published by VulDB.

Appendix 3. Definition of done

- The products above you run are listed, with versions.
- Each in range has the vendor's fixed version and mitigation noted.

- The update is booked, with an owner and a date.
- Anything not in range is recorded as checked.

Sources

- CVE record service: https://www.cve.org/
- CVE record for CVE-2026-135797: https://www.cve.org/CVERecord?id=CVE-2026-135797
- CVE record for CVE-2026-136136: https://www.cve.org/CVERecord?id=CVE-2026-136136
- CVE record for CVE-2026-136547: https://www.cve.org/CVERecord?id=CVE-2026-136547