contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

2 November 2026 · 3 new critical CVEs worth reading

Analysis Report

75 new records scored 8.5 or higher in the last 30 hours. 3 to read first, and the conditions each score leaves out.

PREPARED BY	NamiQ	DATE	2 November 2026
FACTS AS OF	2 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-2026-11-02

The bottom line

> *All three are remotely exploitable router flaws scored at the maximum, none with a known fix. Two share the same command-injection weakness in WAVLINK devices; one is a separate stack overflow in a Linksys router. The question that sorts them: can the management interface be reached from outside the local network?*

506 CVE records were published in the last 30 hours. 75 scored 8.5 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
WAVLINK WN536AX6-A (CVE-2026-120276)	10 (CVSS 4.0)	See the note	Our note, below
Linksys E8450 (CVE-2026-120283)	10 (CVSS 4.0)	See the note	Our note, below
WAVLINK WN551X3-A (CVE-2026-120344)	10 (CVSS 4.0)	See the note	Our note, below

WAVLINK WN536AX6-A, CVE-2026-120276

No fixed version is known. Take the web management interface off any untrusted network now; the exploit is public. Same weakness type and file as CVE-2026-120344 on a different WAVLINK model.

Score 10 (CVSS 4.0), published by VulDB on 1 November 2026. Weakness: CWE-78, CWE-77.

On firmware V260507_2.0.0, an attacker who can reach the WAVLINK WN536AX6-A web management interface can inject OS commands by manipulating the group_name argument in /bin/ioos. The record states the exploit is publicly available. The limiting condition is network access to the management interface.

Linksys E8450, CVE-2026-120283

No fixed version is known and the vendor did not respond to disclosure. Check whether the router's management interface is reachable from outside the local network and restrict it if it is.

Score 10 (CVSS 4.0), published by VulDB on 2 November 2026. Weakness: CWE-121, CWE-119.

On firmware 1.2.00.360516, an attacker who can reach the Linksys E8450's portal.cgi endpoint can trigger a stack buffer overflow by supplying a crafted hidden_timezone argument. The vendor did not respond to the disclosure. The limiting condition is network access to the management endpoint.

WAVLINK WN551X3-A, CVE-2026-120344

No fixed version is stated. The same weakness, argument name, and file appear in CVE-2026-120276 on a different WAVLINK model. Restrict management interface access to trusted networks only.

Score 10 (CVSS 4.0), published by VulDB on 2 November 2026. Weakness: CWE-78, CWE-77.

On firmware M51X3_V251020-WO-182e965, the WAVLINK WN551X3-A WireGuard CLI Group Handler passes the group_name argument to a system call without sanitising it. The attack is fully remote and the exploit has been disclosed publicly. The limiting condition is network access to the affected interface.

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-2026-120276,CVE-2026-120283,CVE-2026-120344
```

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 names of running container images 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-2026-120276 --cve CVE-2026-120283 --cve CVE-2026-120344
```

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. It reads the names of the running images, not what is 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 2 November 2026. Nothing here has been tested.
- Exploitation is not recorded for any of them. That is not the same as none.
- The bottom line and the sentence under each product are our interpretation of the records and the vendors' pages, not a statement by the vendors.

Appendix 1. Severity decoded

CVE-2026-120276: 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-2026-120283: 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-2026-120344: 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
1 November 2026	WAVLINK WN536AX6-A, CVE-2026-120276: record published by VulDB.
2 November 2026	Linksys E8450, CVE-2026-120283: record published by VulDB.
2 November 2026	WAVLINK WN551X3-A, CVE-2026-120344: 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-2026-120276: https://www.cve.org/CVERecord?id=CVE-2026-120276
- CVE record for CVE-2026-120283: https://www.cve.org/CVERecord?id=CVE-2026-120283
- CVE record for CVE-2026-120344: https://www.cve.org/CVERecord?id=CVE-2026-120344