contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

2 November 2026 · 3 new critical CVEs worth reading

Analysis Report

36 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 entries score 10 and are exploitable from the network with no recorded authentication barrier. Two are network routers for which no vendor patch exists; one is a Python sandbox library with a fix. The question is whether any of these products run in your environment.*

206 CVE records were published in the last 30 hours. 36 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
PrefectHQ prefab-ui (CVE-2026-120338)	10 (CVSS 3.1)	prefab-ui 0.21.0 is the first unaffected version per the record (affected range: 0.14.0 before 0.21.0). PyPI shows 0.21.1 as the latest available release.	Our note, below

WAVLINK WN536AX6-A, CVE-2026-120276

No patch is recorded. Any WAVLINK WN536AX6-A on firmware V260507_2.0.0 should have the web management interface removed from untrusted networks immediately as the first step.

Score 10 (CVSS 4.0), published by VulDB on 1 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.

Linksys E8450, CVE-2026-120283

No patch is recorded and the vendor did not respond to disclosure. Any Linksys E8450 on firmware 1.2.00.360516 should have the management interface blocked from external access immediately.

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

A stack-based buffer overflow in the Linksys E8450 portal.cgi handler lets a remote attacker potentially run code by sending a crafted hidden_timezone value. The vendor did not respond to disclosure. The limiting condition is network access to the endpoint.

PrefectHQ prefab-ui, CVE-2026-120338

Upgrade to prefab-ui 0.21.0 or later; the record names this as the first unaffected version. Relevant only if this library is in use with the GenerativeUI sandbox reachable.

Score 10 (CVSS 3.1), published by JFROG on 1 November 2026. Weakness: CWE-693, CWE-94, CWE-269.

Caller-supplied Python in the prefab-ui GenerativeUI sandbox can read and write files as the server OS user and persist via the virtualenv. The record gives FastMCP's GenerativeUI as the usual path. The limiting condition is that endpoint being reachable.

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.

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-2026-120338: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H`

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.
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	High	Total loss of integrity.
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.
1 November 2026	PrefectHQ prefab-ui, CVE-2026-120338: record published by JFROG.

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-2026-120338: https://www.cve.org/CVERecord?id=CVE-2026-120338