contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

6 November 2026 · 3 new critical CVEs worth reading

Analysis Report

90 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	6 November 2026
FACTS AS OF	6 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-2026-11-06

The bottom line

> *All three records describe flaws that require no attacker login. Two score at the maximum of 10; the third scores 9.9. The one question that sorts them: do you run WP Libre Form on WordPress, Apache Juneau, or TPC Software Matchpoint?*

757 CVE records were published in the last 30 hours. 90 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
Unknown WP Libre Form (CVE-2026-118423)	10 (CVSS 3.1)	See the note	Our note, below
Apache Software Foundation Apache Juneau (CVE-2026-121489)	10 (CVSS 4.0)	Apache Juneau 9.2.1, as stated in the CVE record.	Our note, below
TPC Software Matchpoint (CVE-2026-111489)	9.9 (CVSS 4.0)	The vendor statement in the record recommends installing 'the latest available version' but does not name a version number.	Our note, below

Unknown WP Libre Form, CVE-2026-118423

Anyone running WP Libre Form 1.5.0.1 should disable or remove the plugin immediately. The record names no fixed version; contact the author and wait for a patch before reinstalling.

Score 10 (CVSS 3.1), published by WPScan on 6 November 2026. Weakness: CWE-434 Unrestricted Upload of File with Dangerous Type.

An unauthenticated visitor can upload a PHP file through WP Libre Form's submission feature and run it on the server, gaining remote code execution. The record covers version 1.5.0.1. The record states no limiting condition.

Apache Software Foundation Apache Juneau, CVE-2026-121489

Check whether DirectoryResource's view, upload, or delete settings are enabled. If any are on, upgrade to 9.2.1 immediately — the record names it as the fix. If all are off, upgrading is still

prudent; confirm which settings are active.

Score 10 (CVSS 4.0), published by Apache on 5 November 2026. Weakness: CWE-22.

An attacker who can reach Apache Juneau's DirectoryResource endpoint can escape its root directory and read, write, or delete any file the server process can access. The three enabling settings — view, upload, delete — are off by default.

TPC Software Matchpoint, CVE-2026-111489

Anyone running Matchpoint should contact TPC Software for the current release and install it. The record scores this 9.9. The vendor recommends updating but does not name a fixed version number.

Score 9.9 (CVSS 4.0), published by INCIBE on 5 November 2026.

A credential embedded in the Matchpoint mobile app can obtain the platform's authentication token without a password. The record says this grants unauthenticated access to API services. Exposure is highest where the API faces an untrusted network.

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-2026-118423,CVE-2026-121489,CVE-2026-111489
```

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-2026-118423 --cve CVE-2026-121489 --cve CVE-2026-111489
```

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 6 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-2026-118423: 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.

CVE-2026-121489: 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`

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-2026-111489: score 9.9, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:H/SI:H/SA:N`

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	None	No effect on availability.
Subsequent systems: confidentiality	High	Total loss of confidentiality.
Subsequent systems: integrity	High	Total loss of integrity.
Subsequent systems: availability	None	No effect on availability.

Appendix 2. Timeline

Date	Event
6 November 2026	Unknown WP Libre Form, CVE-2026-118423: record published by WPScan.
5 November 2026	Apache Software Foundation Apache Juneau, CVE-2026-121489: record published by Apache.
5 November 2026	TPC Software Matchpoint, CVE-2026-111489: record published by INCIBE.

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-2026-118423: https://www.cve.org/CVERecord?id=CVE-2026-118423
- CVE record for CVE-2026-121489: https://www.cve.org/CVERecord?id=CVE-2026-121489
- CVE record for CVE-2026-111489: https://www.cve.org/CVERecord?id=CVE-2026-111489