contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

6 November 2026 · 3 new critical CVEs worth reading

Analysis Report

99 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

> *THE BOTTOM LINE: All three records score 10 and require no prior login; each is reachable over a network. The weaknesses are unrelated. The question that sorts them is whether your environment includes Microsoft Entra Device Registration, the WP Libre Form WordPress plugin, or a self-hosted Wanderer instance below 0.20.0.*

626 CVE records were published in the last 30 hours. 99 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
Microsoft Entra Device Registration (CVE-2026-109469)	10 (CVSS 3.1)	See the note	Our note, below
Unknown WP Libre Form (CVE-2026-118423)	10 (CVSS 3.1)	See the note	Our note, below
open-wanderer wanderer (CVE-2026-71495)	10 (CVSS 3.1)	0.20.0, released 7 July (per the v0.20.0 release notes on GitHub)	Our note, below

Microsoft Entra Device Registration, CVE-2026-109469

Anyone running Microsoft Entra Device Registration must act now. No fixed version is recorded; confirm whether the service is reachable from untrusted networks and watch for Microsoft guidance.

Score 10 (CVSS 3.1), published by Microsoft on 6 November 2026. Weakness: CWE-639.

An attacker with network access can substitute a key they control for one Entra Device Registration expects, bypassing authorisation and elevating privileges. No login is needed. The record uses CWE-639 and names no specific version range.

Unknown WP Libre Form, CVE-2026-118423

Anyone running WP Libre Form 1.5.0.1 on WordPress must act without delay. No fixed version is recorded; disable the plugin immediately and watch the vendor's channel for a patched release.

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

An unauthenticated attacker can submit a form to WP Libre Form 1.5.0.1, upload a PHP file to a web-accessible path, and have the server execute it on request, giving full remote code execution. The record names no fixed version. The weakness is CWE-434.

open-wanderer wanderer, CVE-2026-71495

Update any self-hosted Wanderer instance below 0.20.0 to 0.20.0 now. The analysis notes the fix has been available since 7 July. Confirm the PUBLIC_PRIVATE_INSTANCE setting at the same time.

Score 10 (CVSS 3.1), published by GitHub on 6 November 2026. Weakness: CWE-918.

An unauthenticated attacker sends a request to Wanderer's download endpoint with any URL; the server fetches and returns it, reaching internal services. Affects versions below 0.20.0. Limiting condition: PUBLIC_PRIVATE_INSTANCE is not set to true.

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-2026-109469,CVE-2026-118423,CVE-2026-71495
```

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-2026-109469 --cve CVE-2026-118423 --cve CVE-2026-71495
```

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 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-2026-109469: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C`

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-2026-118423: 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-2026-71495: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/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	None	Nothing can be altered.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
6 November 2026	Microsoft Entra Device Registration, CVE-2026-109469: record published by Microsoft.
6 November 2026	Unknown WP Libre Form, CVE-2026-118423: record published by WPScan.
6 November 2026	open-wanderer wanderer, CVE-2026-71495: record published by GitHub.

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-2026-109469: https://www.cve.org/CVERecord?id=CVE-2026-109469
- CVE record for CVE-2026-118423: https://www.cve.org/CVERecord?id=CVE-2026-118423
- CVE record for CVE-2026-71495: https://www.cve.org/CVERecord?id=CVE-2026-71495