contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

# Unknown WP Libre Form: new CVE

**CVE-2026-118423 · record published 6 November 2026**

## Analysis Report

Anyone running WP Libre Form 1.5.0.1 on a WordPress site must act now — the record names no fixed version. Disable or remove the plugin immediately while you wait for a patch from the author.

| | | | |
|---|---|---|---|
| PREPARED BY | NamiQ | DATE | 6 November 2026 |
| FACTS AS OF | 6 November 2026 | VERSION | 1.0 |
| SEVERITY | **Critical: CVSS 3.1 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/unknown-wp-libre-form-cve-2026-118423

## The bottom line

> *Anyone running WP Libre Form 1.5.0.1 on a WordPress site must act now — the record names no fixed version. Disable or remove the plugin immediately while you wait for a patch from the author.*

## At a glance

| Fact | Detail |
|---|---|
| Product | Unknown WP Libre Form (CVE-2026-118423) |
| Severity | Critical: 10 (CVSS 3.1) |
| Status | A new CVE record, published by WPScan on 6 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 6 November 2026, which means nothing public says yet that anyone is using it. |
| Fixed in | No source we read names a fixed version |
| Who looks first | WordPress site owners and their IT providers who have the WP Libre Form plugin at version 1.5.0.1 installed, particularly where the site and its forms are publicly reachable without a login. |

## Does this apply to you?

**Answer in order. Stop at the first no.**

| Question | If no | If yes |
|---|---|---|
| Do you run a WordPress site with the WP Libre Form plugin installed? | Nothing to do for this CVE. | Check the installed version (next question). |
| Is the installed version 1.5.0.1? | Nothing to do for this CVE. | Act now — disable the plugin; see steps below. |
| Can untrusted users reach the plugin's form without a WordPress login? | Lower priority, but no fix is recorded — disable the plugin at next maintenance window. | Treat this as urgent; disable the plugin immediately. |

## What it is

An unauthenticated attacker — no account required — can upload a PHP file through the plugin's form submission feature and then run it on the server, giving them full remote code execution.

## Why it matters

The CVE score is 10 — the maximum on CVSS 3.1. The description says no login is needed: any visitor can attempt to upload a PHP file and run it. The weakness is CWE-434 (unrestricted upload of a dangerous file type). Our reading is that this combination — maximum score, no authentication barrier, and direct code execution — makes this worth acting on immediately even though the record is new and no vendor advisory could be read. No workaround beyond disabling the plugin is currently known.

## Things people will get wrong

- There must be a patched version — I just need to update. The record lists no unaffected releases and no vendor advisory could be read. No fixed version is currently known; do not assume a version bump addresses this flaw without a changelog entry that names it.
- Because it is not on CISA's exploited list, this can wait. The CVE score is 10 and the description says no authentication is needed. A new record's absence from CISA's list reflects when it was read, not the severity of the flaw.

## How we would triage it

This is our judgement.

## Step 1: Find whether WP Libre Form is installed and note the version

- In WordPress admin, go to Plugins and look for 'WP Libre Form'; note the version shown beside it.
- If WP-CLI is available, the command below prints the installed version and status.

## Step 2: Disable or remove the plugin if version 1.5.0.1 is found

- The record names no fixed version; disabling the plugin removes the file upload route while you wait for a patch.
- Deleting the plugin entirely is the safer option if no site function depends on it.

## Step 3: Check whether a fixed release has appeared

- No unaffected release is listed in the record; check the plugin's changelog for any entry that names CVE-2026-118423 or a file upload security fix.
- Do not reinstall based on a version bump alone unless the changelog confirms it covers this CVE.

## Step 4: Confirm the site operates correctly without the plugin and record what was done

- Identify any forms relying on WP Libre Form and arrange alternatives if needed.
- Keep a written record of when the plugin was disabled, the version found, and who took the action.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

## Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *We have been made aware of a security flaw in the WP Libre Form WordPress plugin (CVE-2026-118423, CVSS score 10). The record states that an unauthenticated attacker can upload a PHP file through the plugin's form and execute it on the server. The only version named in the record is 1.5.0.1. No fixed version is currently recorded and no vendor advisory could be read. Please check whether this plugin is installed on any WordPress site we operate, confirm the installed version, and advise what action to take. If version 1.5.0.1 is present, we would like written confirmation that the plugin has been disabled or removed, together with the version confirmed, by 13 November 2026.*

## The weakness behind it

The record classes this as CWE-434.

## The sources, in their words

The CVE record:

> *The WP Libre Form WordPress plugin 1.5.0.1 does not validate the type of files uploaded through its form submissions, allowing unauthenticated attackers to upload PHP files to a web-accessible location and execute them, leading to remote code execution.*

Versions of Unknown WP Libre Form the record lists as affected:

- 1.5.0.1 through 1.5.0.1

The record gives no version ranges. Use the vendor's advisory for the affected versions.

## Check your own project

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

```
lattice-scan project . --cve CVE-2026-118423
```

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 id 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
```

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

- Whether a fixed version exists or is planned; no vendor advisory could be read and the record lists no unaffected releases.
- Whether versions other than 1.5.0.1 are affected; the record names only that exact version.
- Whether any workaround short of disabling the plugin is available.
- Whether the plugin is still actively maintained by its author.
- Exploitation is not recorded. That is not the same as none.
- This is a new record: scores, versions and wording can change in the first days, and they are as at 6 November 2026. We have not read the vendor's advisory page and we have not tested it.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

## 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` As the CVE record gives it.

| 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 |
|---|---|
| 6 November 2026 | CVE record published by WPScan. |

## Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

| Your situation | Priority | Timeframe |
|---|---|---|
| WP Libre Form 1.5.0.1 installed and form publicly accessible without a login | High | Immediately |
| WP Libre Form 1.5.0.1 installed and form exposure is unconfirmed | High | Today — verify exposure and disable |
| WP Libre Form is installed but the version has not been confirmed | Medium | This week — confirm version first |
| WP Libre Form is not installed on any site | None | None for this CVE |

## Appendix 4. Definition of done

- Every Unknown WP Libre Form you run is listed, with its version.
- Each is outside the affected list, or the vendor's fix or mitigation is in place.
- The version output or a screenshot is saved with the date.
- Anything not done has an owner and a date.

## Sources

- CVE record for CVE-2026-118423: https://www.cve.org/CVERecord?id=CVE-2026-118423
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: wpscan.com: https://wpscan.com/vulnerability/35149a79-aee1-4f13-ba29-583c2224c5da/