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 without delay; the record scores this 10 and no fixed version is named. Disable the plugin now and watch the vendor's channel for a …

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 without delay; the record scores this 10 and no fixed version is named. Disable the plugin now and watch the vendor's channel for a patched release.*

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	Anyone who runs a WordPress site with WP Libre Form version 1.5.0.1 installed, particularly where the form is publicly reachable. The attack requires no login.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run any WordPress sites?	Nothing to do for this CVE.	Check whether WP Libre Form is installed.
Is WP Libre Form installed on any of those sites?	Nothing to do for this CVE.	Check the installed version.
Is the installed version 1.5.0.1?	The record covers only 1.5.0.1; monitor the vendor for guidance on other versions.	Disable the plugin immediately; no fixed version is named in the record.

What it is

An unauthenticated attacker can submit a form handled by this plugin and upload a PHP file to a location the web server can reach. The server then executes that file on request, giving the attacker full remote code execution with no prior login.

Why it matters

A score of 10 reflects that no authentication is needed and the result is full code execution on the server. The weakness — CWE-434 — means the plugin accepts any file type, including server-side scripts. An attacker submits the form, plants a PHP file in a web-accessible path, then fetches that file to run commands as the web server user. Our reading is that any publicly reachable form powered by this plugin is an open door: there is no login requirement, and the record names no patch. Disabling the plugin removes the exposure until a fix is available.

Things people will get wrong

- Only 1.5.0.1 is listed, so other versions must be safe. The record covers only 1.5.0.1 and names no fixed version. It does not state that other versions are unaffected; the record is simply silent on them.
- A score of 10 means it is already being actively exploited. The record is new and does not appear on CISA's list of exploited vulnerabilities. The score reflects the ease and impact of the flaw, not confirmed active use.

How we would triage it

This is our judgement.

Step 1: Find which WordPress sites have this plugin installed

- List all WordPress installations you operate and check the Plugins section of each site's dashboard for WP Libre Form.
- Confirm the exact version shown; the record covers version 1.5.0.1.

Step 2: Disable the plugin on any site running 1.5.0.1

- Deactivate WP Libre Form on every site where it is confirmed as version 1.5.0.1; this removes the exposed upload path.
- No fixed version is named in the record, so disabling is the safest step until a patched release is available.

Step 3: Check for unexpected PHP files in upload directories

- Review the WordPress uploads directory for PHP files; the flaw allows an attacker to place one there to run commands.
- Any PHP file found in the uploads directory warrants immediate investigation.

Step 4: Watch for a patched release

- Monitor the plugin's listing for a new release that names this flaw as fixed.
- No source names a fixed version at this time; apply any confirmed patch without delay.

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 critical security flaw in a WordPress plugin: CVE-2026-118423 in WP Libre Form version 1.5.0.1. The flaw allows an unauthenticated attacker to upload a PHP file and execute it on the server, with no login required. The CVSS score is 10. No fixed version has been published at this time. Please check whether WP Libre Form is installed on any WordPress site we operate, confirm which version is running, and disable the plugin immediately on any site running version 1.5.0.1. We ask for written confirmation of the installed version and the action taken by 13 November 2026. We will monitor for a patched release and ask you to apply it promptly once one is available.*

The weakness behind it

The record classes this as CWE-434.

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so
Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	The description names a public-facing WordPress form as the entry point; an unauthenticated attacker would likely exploit it directly over the network, with no credentials needed.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	Once a PHP file is uploaded and fetched, it would typically run as server-side code and issue arbitrary commands as the web server user.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

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 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-2026-118423
```

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. 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

- No fixed version has been named in the record or any source; it is not known when a patch will be available.
- It is not known whether versions other than 1.5.0.1 are affected.
- No workaround other than disabling the plugin is recorded in any source.
- 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", "Likely ATT&CK mapping", "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
WordPress site running WP Libre Form 1.5.0.1 with the form publicly reachable	High	immediately
Same version installed, form accessible only to authenticated users	Medium	this week
Plugin installed but version not yet confirmed	Medium	confirm the version this week
Plugin installed, version is not 1.5.0.1	Low	monitor the vendor for guidance

WP Libre Form is not installed on any site you operate	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/