contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Unknown Confection WordPress Cable: new CVE

CVE-2026-115252 · record published 9 November 2026

Analysis Report

Any WordPress site running the Confection WordPress Cable plugin at versions 0.4.0 to 0.4.7 must act now; no fixed version is recorded in the CVE record or any source we could read. Disable and …

PREPARED BY	NamiQ	DATE	9 November 2026
FACTS AS OF	9 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-confection-wordpress-cable-cve-2026-115252

The bottom line

> *Any WordPress site running the Confection WordPress Cable plugin at versions 0.4.0 to 0.4.7 must act now; no fixed version is recorded in the CVE record or any source we could read. Disable and remove the plugin as the first step.*

At a glance

Fact	Detail
Product	Unknown Confection WordPress Cable (CVE-2026-115252)
Severity	Critical: 10 (CVSS 3.1)
Status	A new CVE record, published by WPScan on 9 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 9 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	No unaffected release is listed in the record. The vendor's page was unreadable, so no fixed version is known from any source we could read.
Who looks first	Any operator of a WordPress site with the Confection WordPress Cable plugin at versions 0.4.0 through 0.4.7 installed. No login is needed to trigger the flaw, so any site reachable from the internet is exposed to every visitor.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run the Confection WordPress Cable plugin on any WordPress site?	Nothing to do for this CVE.	Check the installed version.
Is the installed version between 0.4.0 and 0.4.7 inclusive?	Not in the affected range per the record.	Treat as affected; no patch is recorded.
Is that WordPress site reachable from the internet or from untrusted users on your network?	Risk is reduced but the plugin should still be disabled and removed.	Act now; the flaw needs no login.

What it is

An unauthenticated visitor can submit settings to the plugin with no login or token check. The plugin writes one of those settings directly into a PHP file and serves it, so the visitor's input runs as server-

side code. The record describes this as allowing arbitrary PHP execution by any unauthenticated user.

Why it matters

The score is 10 — the maximum. The flaw needs no login and no prior foothold: any HTTP request suffices. The plugin writes attacker-controlled input directly into a PHP file the server then executes, giving full server-side code execution. Our reading is that a score-10 unauthenticated write-to-execute path is about as severe as a web flaw gets; with server-side code execution an attacker can access files, credentials, and other data on the host, and a site does not need to be large or high-profile to be a worthwhile target once the plugin version is identifiable by automated scanning.

Things people will get wrong

- Our WordPress admin login protects us from this flaw The record says no login, capability check, or nonce is required. An attacker does not need to reach the admin panel; any HTTP request to the plugin's endpoint is sufficient.
- We can wait for the vendor to release a patch before acting The record lists no unaffected release, and the vendor's page was unreadable. There is no patch recorded from any source; there is nothing yet to wait for.

How we would triage it

This is our judgement.

Step 1: Find which sites run the plugin and confirm the version

- In each WordPress admin dashboard go to Plugins and search for 'Confection WordPress Cable'; note the installed version and status.
- If WP-CLI is available, list all plugins and their versions across each site to confirm what is installed.

Step 2: Disable and delete the plugin on every affected site

- Deactivate the plugin via the WordPress admin Plugins page, then delete it; deactivation alone stops the endpoint but leaves the plugin files on disk.
- No fixed version is recorded; reinstalling the same version is not a remedy.

Step 3: Locate and remove the standalone PHP file the plugin created

- The record says the plugin writes one of its settings into a standalone PHP file it then serves. After deleting the plugin, search the site's directory for any such file and remove it.
- The exact filename is not recorded in the CVE record; look for recently modified PHP files in or near the plugin's former directory.

Step 4: Watch for a patched release from the vendor

- Check the plugin's listing on wordpress.org for a release newer than 0.4.7 that names this CVE.
- Do not reinstall the plugin until a version is confirmed as unaffected by the vendor's own advisory.

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 are reviewing CVE-2026-115252, a score-10 flaw in the Confection WordPress Cable WordPress plugin (versions 0.4.0 to 0.4.7) that allows any unauthenticated visitor to execute code on the server. No patched version is recorded as of 9 November 2026. Please confirm: (1) whether this plugin is installed on any WordPress site we host or manage; (2) the installed version if so; (3) whether it has been deactivated and deleted; and (4) whether the standalone PHP file the plugin creates has been located and removed. We would like written confirmation of each point by [date].*

The weakness behind it

The record classes this as CWE-94 and CWE-862.

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 flaw is in a WordPress plugin reachable over HTTP with no authentication; exploitation would likely serve as the initial entry point into the server, matching a network-exposed public-facing application.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	The weakness is CWE-94 code injection: the plugin writes attacker input into a PHP file the server executes, which would typically result in arbitrary script execution on the host.

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 Confection WordPress Cable WordPress plugin from 0.4.0 to 0.4.7 does not perform any capability or nonce checks before saving its settings and writing one of them, unmodified, into a standalone PHP file that it then serves, allowing unauthenticated users to execute arbitrary PHP code on the server.*

Versions of Unknown Confection WordPress Cable the record lists as affected:

- 0.4.0 through 0.4.7

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-2026-115252
```

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-2026-115252
```

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

- Whether a patched version exists or is planned; the record lists no unaffected release and the vendor's page was unreadable.
- The exact filename and location of the standalone PHP file the plugin writes; the record does not name it.
- Whether exploit code for this flaw is publicly available; the record does not say.
- Whether versions below 0.4.0 are affected; the record names the range from 0.4.0 to 0.4.7 only.
- 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 9 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-2026-115252: 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
9 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
Plugin at 0.4.0–0.4.7 on a WordPress site reachable from the internet, no patch recorded	High	Now
Plugin at 0.4.0–0.4.7 on an internal site reachable by any untrusted user on the network	High	This week
Plugin is installed but the version has not yet been confirmed	Medium	Today — confirm version first
Plugin was installed in the past but its current status is unconfirmed	Medium	This week
The plugin is not installed on any site you operate	None	None for this CVE

Appendix 4. Definition of done

- Every Unknown Confection WordPress Cable 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-2026-115252: https://www.cve.org/CVERecord?id=CVE-2026-115252
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: wpscan.com: https://wpscan.com/vulnerability/aebe20c3-bc02-4082-bda8-bbaa01550925/