contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Webdeclic WPMasterToolKit: new CVE

CVE-2026-134963 · record published 27 November 2026

Analysis Report

WordPress sites running WPMasterToolKit at 2.26.1 or below and granting Contributor access to users outside the owner's team need to act. Update the plugin to version 2.26.2 — the Patchstack advisory …

PREPARED BY	NamiQ	DATE	27 November 2026
FACTS AS OF	27 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.9**	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/webdeclic-wpmastertoolkit-cve-2026-134963

The bottom line

> *WordPress sites running WPMasterToolKit at 2.26.1 or below and granting Contributor access to users outside the owner's team need to act. Update the plugin to version 2.26.2 — the Patchstack advisory names this as the patched version.*

At a glance

Fact	Detail
Product	Webdeclic WPMasterToolKit (CVE-2026-134963)
Severity	Critical: 9.9 (CVSS 3.1)
Status	A new CVE record, published by Patchstack on 27 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 27 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	WPMasterToolKit 2.26.2, per the Patchstack advisory published 25 November 2026.
Who looks first	WordPress site owners running WPMasterToolKit at version 2.26.1 or below. The Patchstack advisory lists Contributor as the minimum privilege needed to exploit this, so sites with external contributors face the most direct exposure.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you have WPMasterToolKit installed on any WordPress site?	Nothing to do for this CVE.	Check the installed version next.
Is the installed version 2.26.1 or earlier?	Not in the affected range; nothing further to do.	Check who holds Contributor access on the site.
Does the site have Contributor accounts held by anyone outside your trusted team?	Lower risk; update at the next maintenance window.	Update to version 2.26.2 without delay.

What it is

The record describes an attacker with at least Contributor-level access in WordPress injecting code that runs on the server. The Patchstack advisory says this allows the attacker to run their own code on the server and take the site over. The weakness is CWE-94, Improper Control of Code Generation.

Why it matters

Our reading is that the score of 9.9 reflects the consequence of full code execution, not how easy it is to reach — an attacker needs a valid Contributor-level account before the flaw can be used. For a site where only the owner and trusted staff hold any accounts, the practical exposure is lower than the score implies. The Patchstack advisory says this class of flaw is used in mass-exploit campaigns against thousands of sites regardless of their size or traffic, so updating to 2.26.2 is the right step even where contributor accounts are few.

What the vendor's advisory says

We read one page on patchstack.com. In short:

- The Patchstack advisory (25 November 2026) says to update to version 2.26.2 or later. Patchstack has issued a mitigation rule to block attacks on unpatched sites. No other CVEs fixed in this release are named in the advisory.

Things people will get wrong

- The score of 9.9 means anyone on the internet can exploit this without an account. The Patchstack advisory lists Contributor as the minimum required privilege. An attacker needs that level of access in WordPress first; without it, the flaw cannot be reached.
- Sites with no external contributors are fully safe and do not need to update. Internal accounts can be compromised. Updating to 2.26.2 is the stated remediation; keeping an unpatched version installed remains unnecessary risk even with restricted contributors.

How we would triage it

This is our judgement.

Step 1: Find the installed version

- Log in to WordPress and go to Plugins; WPMasterToolKit's current version is shown in the plugin list.
- If the version shown is 2.26.1 or below, the site is in the affected range per the Patchstack record.

Step 2: Review who holds Contributor access

- In WordPress, go to Users and filter by the Contributor role to see which accounts are at that level or above.
- If any account belongs to someone outside your trusted team, treat the update as urgent.

Step 3: Update the plugin to 2.26.2

- Update WPMasterToolKit via the WordPress Plugins screen, or ask your hosting provider to do so.
- The Patchstack advisory names 2.26.2 as the patched version; confirm the displayed version after updating.

Step 4: Confirm the update took effect

- After updating, verify the installed version is 2.26.2 or later in the WordPress Plugins screen.
- If the version still shows 2.26.1 or below, the update did not complete — repeat the update or contact the hosting provider.

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 writing about CVE-2026-134963, a code injection vulnerability in the WPMasterToolKit WordPress plugin by Webdeclic. The Patchstack advisory published on 25 November 2026 gives it a CVSS score of 9.9 and states that all versions up to and including 2.26.1 are affected. Version 2.26.2 is the patched release. An attacker with at least Contributor-level WordPress access can exploit this to execute code on the server. We would like to know whether this plugin is installed on any of our WordPress sites, which version is running, and when it will be updated to 2.26.2 or later. Please confirm in writing the version installed and the date any update is applied.*

The weakness behind it

The record classes this as CWE-94.

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
Valid Accounts (T1078): Logging in with a real account the attacker should not have, so the activity looks like normal use.	Initial Access: getting in	Exploiting this flaw requires a valid Contributor-level WordPress account; an attacker would likely use a compromised or socially obtained account to reach the vulnerable code path.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	CWE-94 (Improper Control of Code Generation) in a server-side plugin would typically result in execution of server-side scripts or commands once the injection point is reached.
Exploitation for Privilege Escalation (T1068): Using a flaw to gain higher rights than the account had, such as administrator or root.	Privilege Escalation: gaining higher rights	Executing arbitrary code from a Contributor-level account would typically escalate privileges to server or site-admin level; the Patchstack advisory says the site can be taken over.

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:

> *Improper Control of Generation of Code ('Code Injection') vulnerability in Webdeclic WPMasterToolKit wpmastertoolkit allows Code Injection.This issue affects WPMasterToolKit: from n/a through 2.26.1.*

Versions of Webdeclic WPMasterToolKit the record lists as affected:

- all versions up to and including 2.26.1

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

What the record says to do about it, in the vendor's words:

> *Update the WordPress WPMasterToolKit plugin to the latest available version (at least 2.26.2).*

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-2026-134963
```

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-2026-134963
```

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

- The source does not name the specific feature or input within WPMasterToolKit where the injection point exists.

- The source does not confirm whether the developer's release notes for 2.26.2 name this CVE.
- The source does not say whether the flaw affects a core function or an optional module of the plugin.
- No indication is given of whether this specific flaw has been used in an active attack; the source says this class of flaw is typical in mass campaigns but does not confirm it for this CVE.
- 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 27 November 2026. We read the vendor pages listed under Sources; nothing here has been tested.
- 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-2026-134963: score 9.9, `CVSS:3.1/AV:N/AC:L/PR:L/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	Low	An ordinary account is enough.
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
27 November 2026	CVE record published by Patchstack.

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
Running ≤2.26.1 with Contributor accounts held by external users, site publicly reachable	Medium	Without delay
Running ≤2.26.1 and uncertain which users hold Contributor-level access	Medium	Identify accounts today, then update
Running ≤2.26.1 with Contributor access limited to the owner and trusted staff only	Medium	This week
Running version 2.26.2 or later	None	None for this CVE

Appendix 4. Definition of done

- Every Webdeclic WPMasterToolKit 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-2026-134963: https://www.cve.org/CVERecord?id=CVE-2026-134963
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: patchstack.com/database/wordpress/plugin/wpmastertoolkit/vulne: https://patchstack.com/database/wordpress/plugin/wpmastertoolkit/vulnerability/wordpress-wpmastertoolkit-plugin-2-26-1-arbitrary-code-execution-vulnerability-2?_s_id=cve