contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

STAGGS: new CVE

CVE-2026-78287 · record published 11 November 2026

Analysis Report

If your site runs the STAGGS WordPress plugin at version 3.3.0 or earlier, update to 3.4.0 immediately — no login is needed to exploit it. The first step is to check which version of STAGGS is ...

PREPARED BY	NamiQ	DATE	11 November 2026
FACTS AS OF	11 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/staggs-cve-2026-78287

The bottom line

> *If your site runs the STAGGS WordPress plugin at version 3.3.0 or earlier, update to 3.4.0 immediately — no login is needed to exploit it. The first step is to check which version of STAGGS is installed across your WordPress sites.*

At a glance

Fact	Detail
Product	STAGGS (CVE-2026-78287)
Severity	Critical: 10 (CVSS 3.1)
Status	A new CVE record, published by Patchstack on 11 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 11 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	3.4.0, per the Patchstack advisory published 9 November 2026.
Who looks first	Anyone running a WordPress site with the STAGGS plugin installed at version 3.3.0 or earlier needs to act. The record states no authentication is required to trigger the flaw.

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 the STAGGS plugin is installed.
Is the STAGGS plugin installed on any WordPress site you run?	Nothing to do for this CVE.	Check the installed version.
Is the installed version of STAGGS 3.3.0 or earlier?	Nothing further to do for this CVE.	Update to version 3.4.0 or later now.

What it is

A flaw in how the STAGGS plugin handles input allows an attacker to inject and run their own code on the web server without holding any account on the site.

Why it matters

The score is 10 and no authentication is required, meaning any internet-facing site with this plugin is reachable by anyone without an account. The Patchstack advisory states this class of flaw is used in mass-exploit campaigns that target sites regardless of traffic size or popularity. The weakness is code injection (CWE-94), which gives an attacker full server-side code execution rather than read access alone. Our reading is that the zero-login barrier and the mass-campaign pattern described in the advisory make this worth treating as urgent even though it does not yet carry a CISA listing.

What the vendor's advisory says

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

- The Patchstack advisory (9 November 2026) names 3.4.0 as the patched version and states no other CVEs are fixed in the same release. Patchstack says it has issued a mitigation rule for subscribers who cannot update immediately; no other workaround is stated.

Things people will get wrong

- Only high-traffic or well-known sites are worth attacking. The Patchstack advisory states that mass-exploit campaigns target sites regardless of traffic size or popularity; site obscurity is not a defence.
- A login page on the site prevents exploitation. The record states the flaw is unauthenticated. A login requirement on the site's front page does not prevent this — no account on the site is needed.

How we would triage it

This is our judgement.

Step 1: Find the version of STAGGS installed

- In the WordPress admin panel, go to Plugins and check the version shown next to STAGGS.
- Any version at or below 3.3.0 is affected, per the Patchstack record published 9 November 2026.

Step 2: Update STAGGS to version 3.4.0 or later

- The Patchstack advisory states that updating to 3.4.0 resolves the vulnerability.
- Update through the WordPress admin panel, or ask your hosting provider to do it if you do not have direct access.

Step 3: Confirm the update is in place

- After updating, verify the installed version is 3.4.0 or later through the WordPress admin panel.
- If a hosting provider carried out the update, ask for written confirmation of the version now running.

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-2026-78287, a remote code execution flaw in the STAGGS WordPress plugin. The record states it affects all versions up to and including 3.3.0 (CVSS 10, no login required to exploit), and that version 3.4.0 resolves it. Could you please check whether the STAGGS plugin is installed on any WordPress sites you manage for us, confirm the version running on each, and update to 3.4.0 on any site that is on an affected version? We would like written confirmation of the version found and confirmation that the update has been applied. As no authentication is needed to exploit this, we would like to resolve it as quickly as possible.*

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
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 publicly accessible WordPress plugin requiring no authentication, making exploitation of a public-facing application the likely initial access 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 code injection granting RCE would typically result in command or script execution on the server once the flaw is triggered.
Create Account (T1136): Creating a new account so the attacker can come back later.	Persistence: staying in	Unauthenticated RCE on a WordPress site would likely be followed by creating a new administrator account to maintain persistent access.

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 Staggs STAGGS staggs allows Remote Code Inclusion.This issue affects STAGGS: from n/a through 3.3.0.*

Versions of STAGGS the record lists as affected:

- all versions up to and including 3.3.0

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 STAGGS plugin to the latest available version (at least 3.4.0).*

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-2026-78287
```

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-2026-78287
```

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 sources do not describe which specific request or feature within the plugin triggers the code injection.
- The sources do not say whether the flaw behaves differently on WordPress multisite installations.
- 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 11 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-2026-78287: 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
11 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
STAGGS <= 3.3.0 installed on an internet-facing WordPress site	Medium	Immediately
STAGGS <= 3.3.0 on a site reachable by any untrusted user, even on an intranet	Medium	Immediately
STAGGS <= 3.3.0 on a site not currently public but previously internet-facing	Medium	This week
STAGGS installed and version confirmed as 3.4.0 or later	None	No action needed for this CVE
WordPress sites in use but STAGGS plugin not installed	None	No action needed for this CVE

Appendix 4. Definition of done

- Every STAGGS 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-2026-78287: https://www.cve.org/CVERecord?id=CVE-2026-78287
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: patchstack.com/database/wordpress/plugin/staggs/vulnerability/: https://patchstack.com/database/wordpress/plugin/staggs/vulnerability/wordpress-staggs-plugin-3-3-0-remote-code-execution-rce-vulnerability?_s_id=cve