contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Nitramix Revertix – Backup, Migration, Staging & Clone: new CVE

CVE-2026-134994 · record published 27 November 2026

Analysis Report

Any WordPress site running the Revertix plugin at version 1.0.3 or earlier should update to version 1.0.4 immediately. The flaw requires no login; update first, then

PREPARED BY	NamiQ	DATE	28 November 2026
FACTS AS OF	28 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.8**	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/nitramix-revertix-8211-backup-migration-cve-2026-134994

The bottom line

> *Any WordPress site running the Revertix plugin at version 1.0.3 or earlier should update to version 1.0.4 immediately. The flaw requires no login; update first, then confirm the installed version. If you do not run WordPress, nothing to do here.*

At a glance

Fact	Detail
Product	Nitramix Revertix – Backup, Migration, Staging & Clone (CVE-2026-134994)
Severity	Critical: 9.8 (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 28 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	Revertix 1.0.4 — the Patchstack advisory, published 25 November 2026, names this as the patched version.
Who looks first	Owners and administrators of WordPress sites where the Revertix – Backup, Migration, Staging & Clone plugin is installed at version 1.0.3 or earlier.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run any WordPress websites?	Nothing to do for this CVE.	Check whether the Revertix plugin is installed on any of them.
Is the Revertix – Backup, Migration, Staging & Clone plugin installed on any site?	Nothing to do for this CVE.	Check the installed version.
Is the installed version 1.0.3 or earlier?	You are on the patched version; nothing further needed.	Update to version 1.0.4 immediately.

What it is

An unauthenticated attacker can send crafted data that the plugin deserialises without checking; the record and advisory state this allows harmful actions on the server. No login or prior access is needed.

What the vendor's advisory says

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

- Patchstack advisory, 25 November 2026: priority High, CVSS 9.8, unauthenticated. Fix: version 1.0.4 or later. A Patchstack mitigation rule is stated as available to block attacks while an update is pending. No other CVEs are mentioned for this release.

Things people will get wrong

- 'We get little traffic so attackers won't target our site.' The Patchstack advisory states these flaws are used in mass-exploit campaigns targeting thousands of sites regardless of traffic size or popularity.
- 'The plugin is deactivated so we are safe.' Neither the record nor the advisory states that deactivation removes the risk. The fix is to update to version 1.0.4.

How we would triage it

This is our judgement.

Step 1: Find which WordPress sites run Revertix

- Check each WordPress installation's plugin list for 'Revertix – Backup, Migration, Staging & Clone' and note the version shown.
- Any site showing version 1.0.3 or earlier is in the affected range stated by the record.

Step 2: Reduce exposure while arranging the update

- If an immediate update is not possible, assess whether the plugin can be deactivated temporarily; the advisory does not confirm that deactivation alone removes the risk.
- The Patchstack advisory states a mitigation rule is available to block attacks, though this requires a Patchstack subscription.

Step 3: Update to version 1.0.4

- The Patchstack advisory and the CVE record both name 1.0.4 as the patched version; update each affected site to at least that version.
- After updating, confirm the version shown in the plugin list is 1.0.4 or later.

Step 4: Review if a site was exposed on an affected version

- If a site ran 1.0.3 or earlier while reachable from the internet, review WordPress and server logs for unexpected PHP errors or unfamiliar file changes.
- Also check for new administrator accounts that cannot be accounted for, as these may indicate follow-on activity after a successful injection.

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 a recently published vulnerability, CVE-2026-134994, affecting the WordPress plugin 'Revertix – Backup, Migration, Staging & Clone' at version 1.0.3 and earlier. The flaw allows an unauthenticated attacker to inject objects via deserialisation, with a CVSS score of 9.8. The patched version is 1.0.4. Could you please check whether this plugin is installed on any of our WordPress sites, confirm which version is running, and update to 1.0.4 where needed? We would like written confirmation of the installed version and that the update has been applied, ideally by 2 December 2026.*

The weakness behind it

The record classes this as CWE-502.

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; an attacker would exploit it directly over the web, making this the likely initial access route.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	PHP Object Injection via CWE-502 would typically enable an attacker to invoke server-side code execution by controlling the data the plugin deserialises.
Create Account (T1136): Creating a new account so the attacker can come back later.	Persistence: staying in	In a WordPress context, code execution following object injection would likely be used to create a new administrator account as a persistence mechanism.

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:

> *Deserialization of Untrusted Data vulnerability in Nitramix Revertix – Backup, Migration, Staging & Clone revertix allows Object Injection.This issue affects Revertix – Backup, Migration, Staging & Clone: from n/a through 1.0.3.*

Versions of Nitramix Revertix – Backup, Migration, Staging & Clone the record lists as affected:

- all versions up to and including 1.0.3

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 Revertix – Backup, Migration, Staging & Clone plugin to the latest available version (at least 1.0.4).*

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-2026-134994
```

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-2026-134994
```

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 record and advisory do not specify which PHP classes or gadget chains are present in the plugin, so the full range of server-side impact from a successful injection is not stated.
- It is not stated whether exploitation requires the plugin to be actively in use (for example, a migration or restore operation in progress) or whether idle installation is sufficient.
- No information is given on whether a successful exploitation attempt leaves observable entries in WordPress or server logs that would confirm it occurred.
- 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 28 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", "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-2026-134994: score 9.8, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/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	Unchanged	Damage stays inside 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
WordPress site running Revertix 1.0.3 or earlier, reachable from the internet	Medium	Update immediately
WordPress site running Revertix 1.0.3 or earlier, internal or access-controlled only	Medium	Update this week
WordPress site with Revertix 1.0.3 or earlier installed but currently deactivated	Medium	Update or remove before reactivating
WordPress site running Revertix 1.0.4 or later	None	No action needed
No WordPress sites in your estate	None	No action needed for this CVE

Appendix 4. Definition of done

- Every Nitramix Revertix – Backup, Migration, Staging & Clone 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-2026-134994: https://www.cve.org/CVERecord?id=CVE-2026-134994
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: patchstack.com/database/wordpress/plugin/revertix/vulnerabilit: https://patchstack.com/database/wordpress/plugin/revertix/vulnerability/wordpress-revertix-backup-migration-staging-clone-plugin-1-0-3-php-object-injection-vulnerability?_s_id=cve