contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

28 November 2026 · 3 new critical CVEs worth reading

Analysis Report

55 new records scored 8 or higher in the last 30 hours. 3 to read first, and the conditions each score leaves out.

PREPARED BY	NamiQ	DATE	28 November 2026
FACTS AS OF	28 November 2026	VERSION	1.0
TOP SCORE	Critical: 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/daily-cve-highlight-2026-11-28

The bottom line

> *Two of today's three records affect WordPress plugins and are fixable by updating; the third is a router with no patch available. All three describe a remotely exploitable path to compromise the affected system. The question that sorts them: do you run WPMasterToolKit, Revertix, or a TRENDnet TEW-751DR or TEW-733GR?*

289 CVE records were published in the last 30 hours. 55 scored 8 or higher. 3 are below, chosen by a fixed rule: highest score first, then fewest conditions in the wording, one product each. None is on CISA's exploited list, so a score here is the record's author describing the worst case. Read the condition before you act on the number.

At a glance

Product	Score	Fixed in	Read next
TRENDnet TEW-751DR (CVE-2026-138004)	10 (CVSS 4.0)	No source records a patched firmware version. The CVE record lists no unaffected releases.	Technical Analysis
Webdeclic WPMasterToolKit (CVE-2026-134963)	9.9 (CVSS 3.1)	WPMasterToolKit 2.26.2, per the Patchstack advisory published 25 November 2026.	Technical Analysis
Nitramix Revertix – Backup, Migration, Staging & Clone (CVE-2026-134994)	9.8 (CVSS 3.1)	Revertix 1.0.4 — the Patchstack advisory, published 25 November 2026, names this as the patched version.	Technical Analysis

TRENDnet TEW-751DR, CVE-2026-138004

No patched firmware is recorded in any source. Owners of a TRENDnet TEW-751DR or TEW-733GR at firmware 1.03B01 should isolate the device now — disable UPnP if possible — and plan to replace it.

Score 10 (CVSS 4.0), published by VulDB on 27 November 2026. Weakness: CWE-78, CWE-77.

An unauthenticated attacker reaching the UPnP service on a TRENDnet TEW-751DR or TEW-733GR at firmware 1.03B01 can inject shell commands. A researcher's notes say WAN-side exposure was not verified; immediate risk is from an attacker already on the LAN.

Webdeclic WPMasterToolKit, CVE-2026-134963

Update WPMasterToolKit to 2.26.2 — named as fixed by the Patchstack advisory. The score reflects full code execution; a site where only the owner holds accounts has lower practical exposure.

Score 9.9 (CVSS 3.1), published by Patchstack on 27 November 2026. Weakness: CWE-94.

An attacker with at least Contributor-level access to a WordPress site running WPMasterToolKit at 2.26.1 or below can inject code that runs on the server. The Patchstack advisory says this allows the attacker to take the site over.

Nitramix Revertix – Backup, Migration, Staging & Clone, CVE-2026-134994

Update Revertix to 1.0.4 immediately. The Patchstack advisory, published 25 November 2026, names this as the patched version. The flaw needs no login, so act before reviewing other priorities.

Score 9.8 (CVSS 3.1), published by Patchstack on 27 November 2026. Weakness: CWE-502.

An unauthenticated attacker can send crafted data that the Revertix WordPress plugin deserialises without checking. The record and the Patchstack advisory say this allows harmful actions on the server. Affects version 1.0.3 and below; no login is needed.

Fifteen minutes this morning

- List the products above you run. If none, you are done.
- For each one you run, read the version from the product and compare it to the fixed version in the table.
- If it is in range, follow the note: reduce exposure first, then update.
- Book the update, and write down who owns it and by when.

Check your own project

If you build software, you can compare what a project declares with these CVEs from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE ids leave your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-138004,CVE-2026-134963,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 ids 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-2026-138004 --cve CVE-2026-134963 --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

- These are new records. A record can change in the first days: scores, versions and wording are as at 28 November 2026. Nothing here has been tested.
- Exploitation is not recorded for any of them. That is not the same as none.
- The bottom line and the sentence under each product are our interpretation of the records and the vendors' pages, not a statement by the vendors.

Appendix 1. Severity decoded

CVE-2026-138004: score 10, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:P`

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.
Attack requirements	None	Works against a default deployment.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	High	Total loss of confidentiality.
Vulnerable system: integrity	High	Total loss of integrity.
Vulnerable system: availability	High	Total loss of availability.
Subsequent systems: confidentiality	High	Total loss of confidentiality.
Subsequent systems: integrity	High	Total loss of integrity.
Subsequent systems: availability	High	Total loss of availability.

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`

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.

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`

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	TRENDnet TEW-751DR, CVE-2026-138004: record published by VulDB.
27 November 2026	Webdeclic WPMasterToolKit, CVE-2026-134963: record published by Patchstack.
27 November 2026	Nitramix Revertix – Backup, Migration, Staging & Clone, CVE-2026-134994: record published by Patchstack.

Appendix 3. Definition of done

- The products above you run are listed, with versions.
- Each in range has the vendor's fixed version and mitigation noted.
- The update is booked, with an owner and a date.
- Anything not in range is recorded as checked.

Sources

- CVE record service: https://www.cve.org/
- CVE record for CVE-2026-138004: https://www.cve.org/CVERecord?id=CVE-2026-138004
- CVE record for CVE-2026-134963: https://www.cve.org/CVERecord?id=CVE-2026-134963
- CVE record for CVE-2026-134994: https://www.cve.org/CVERecord?id=CVE-2026-134994