contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

27 November 2026 · 3 new critical CVEs worth reading

Analysis Report

71 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	27 November 2026
FACTS AS OF	27 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-2026-11-27

The bottom line

> *THE BOTTOM LINE: All three records describe remote code execution flaws with scores of 9.9 or above. Two — Mitel OpenScape 4000 and a TRENDnet router — need no login; the third, a WordPress plugin, needs a Contributor account. The sorting question is whether any of these products are in your estate.*

394 CVE records were published in the last 30 hours. 71 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
Mitel OpenScape 4000 (CVE-2026-137721)	10 (CVSS 3.1)	V11 R2.14 or later (both products). Hotfix PLT HF5 for V11 R1.26. A Mitel-supplied patch for V10 R0.28 through V11 R0.22 (OpenScape 4000) or V10 R1.34 through V11 R0.22 (Manager).	Technical Analysis
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

Mitel OpenScape 4000, CVE-2026-137721

Upgrade to V11 R2.14 or later. The vendor's advisory names Hotfix PLT HF5 for V11 R1.26 and a separate patch for older versions. The vendor says no login is needed to exploit this.

Score 10 (CVSS 3.1), published by Mitre on 27 November 2026. Weakness: CWE-78.

The vendor's advisory says an unauthenticated attacker can inject and run operating-system commands through the Platform component of OpenScape 4000 and its Manager. The weakness is CWE-78. The vendor says no credential is needed; network access alone is sufficient.

TRENDnet TEW-751DR, CVE-2026-138004

No patched firmware is recorded in any source. Anyone running a TEW-751DR or TEW-733GR on firmware 1.03B01 should isolate the device from untrusted networks or plan to replace it.

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

The record says an unauthenticated attacker can inject shell commands through the router's UPnP endpoint. A researcher's notes say commands run as root. The source states WAN-side exposure was not verified; risk is most immediate from the LAN.

Webdeclic WPMasterToolKit, CVE-2026-134963

Update WPMasterToolKit to 2.26.2 — named as the patched release in the Patchstack advisory. Sites where only the owner and trusted staff hold accounts face lower practical risk than the score suggests.

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

The Patchstack advisory says an attacker with Contributor-level WordPress access can inject code that runs on the server and take the site over. The weakness is CWE-94. The limiting condition is a valid Contributor account — the flaw is unreachable without one.

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-2026-137721,CVE-2026-138004,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 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-2026-137721 --cve CVE-2026-138004 --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

- These are new records. A record can change in the first days: scores, versions and wording are as at 27 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-2026-137721: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/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	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.

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.

Appendix 2. Timeline

Date	Event
27 November 2026	Mitel OpenScape 4000, CVE-2026-137721: record published by Mitre.
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.

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-2026-137721: https://www.cve.org/CVERecord?id=CVE-2026-137721
- 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