contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

27 November 2026 · 3 new critical CVEs worth reading

Analysis Report

152 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

> *All three records score 10; none requires a login to exploit. They affect three unrelated products — a Python package repository, a low-code database platform, and a telephony system — so the first question is which of them is in your environment.*

663 CVE records were published in the last 30 hours. 152 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
pulp_python (CVE-2026-126984)	10 (CVSS 3.1)	3.11.10, 3.12.11, 3.13.9, 3.19.8, 3.27.10, 3.36.7, 3.38.2	Technical Analysis
budibase server (CVE-2026-137498)	10 (CVSS 3.1)	@budibase/server 4.0.0, as named in the vendor's advisory (GHSA-x4w8-596q-fmh7) and the VulnCheck record.	Technical Analysis
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

pulp_python, CVE-2026-126984

If pull-through caching is enabled, act now. Fixed versions are 3.11.10, 3.12.11, 3.13.9, 3.19.8, 3.27.10, 3.36.7, and 3.38.2 — upgrade to the branch that matches the installed minor version.

Score 10 (CVSS 3.1), published by Redhat on 26 November 2026. Weakness: CWE-918.

An attacker reaching the content app can direct it to fetch any URL. The record says if the remote has stored credentials, those are sent to the attacker's chosen host. Under the default remote policy, the downloaded file is stored and served to later clients.

budibase server, CVE-2026-137498

Upgrade to Budibase server 4.0.0 without delay. Check first whether any published app exposes a MongoDB query with PUBLIC execution permission, as the advisory identifies that as the specific attack path.

Score 10 (CVSS 3.1), published by VulnCheck on 26 November 2026. Weakness: CWE-943.

An unauthenticated attacker can send one request to erase the MongoDB filter on a PUBLIC query, exposing every document to read, update, or deletion. The advisory says the app ID and query ID needed are visible in the app's normal traffic.

Mitel OpenScape 4000, CVE-2026-137721

Both products must be upgraded. The affected ranges put V11 R2.14 as the first unaffected version. The vendor's advisory also names patches for older V10 branches.

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

The Platform component of OpenScape 4000 and its Manager does not sanitise input, allowing arbitrary operating-system commands to run on the telephony platform. The vendor's advisory says no login is needed to trigger this.

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-2026-126984,CVE-2026-137498,CVE-2026-137721
```

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-2026-126984 --cve CVE-2026-137498 --cve CVE-2026-137721
```

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-2026-126984: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N`

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	None	No effect on availability.

CVE-2026-137498: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N`

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	None	No effect on availability.

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.

Appendix 2. Timeline

Date	Event
26 November 2026	pulp_python, CVE-2026-126984: record published by Redhat.
26 November 2026	budibase server, CVE-2026-137498: record published by VulnCheck.
27 November 2026	Mitel OpenScape 4000, CVE-2026-137721: record published by Mitre.

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-2026-126984: https://www.cve.org/CVERecord?id=CVE-2026-126984
- CVE record for CVE-2026-137498: https://www.cve.org/CVERecord?id=CVE-2026-137498
- CVE record for CVE-2026-137721: https://www.cve.org/CVERecord?id=CVE-2026-137721