contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

24 November 2026 · 3 new critical CVEs worth reading

Analysis Report

207 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	24 November 2026
FACTS AS OF	24 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-2026-11-24

The bottom line

> *THE BOTTOM LINE: All three records score 10 out of 10 and require no authentication; each affects a different product. The question that matters is which of the three your environment runs.*

978 CVE records were published in the last 30 hours. 207 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
Microsoft Azure App Service for Linux (CVE-2026-109484)	10 (CVSS 3.1)	The record's affected range ends just before 110.0.7.78 and 111.0.7.3, suggesting those are the first unaffected builds; no unaffected releases are listed and no vendor advisory could be read.	Technical Analysis
Acer Connect M6E 5G Portable WiFi Router (CVE-2026-128791)	10 (CVSS 4.0)	M6E_GBL_1.00.000107, available via over-the-air update — stated in the CVE record.	Technical Analysis
hexpm (CVE-2026-129514)	10 (CVSS 4.0)	The source identifies the fix at commit 379b0a29bcc95164249f38ad7d772a37a8ff9533 in hexpm/hexpm. No release version number is named in any source.	Technical Analysis

Microsoft Azure App Service for Linux, CVE-2026-109484

Azure App Service for Linux customers should contact Microsoft support, ask for the current platform build, and request written confirmation the fix is applied. No self-service action is available.

Score 10 (CVSS 3.1), published by Microsoft on 24 November 2026. Weakness: CWE-75.

Special element injection in Azure App Service for Linux lets a network attacker with no credentials raise their privileges on the platform. This affects the Linux variant; the record names no limiting condition on network access or position.

Acer Connect M6E 5G Portable WiFi Router, CVE-2026-128791

Anyone running the Acer Connect M6E 5G on affected firmware should apply the over-the-air update to M6E_GBL_1.00.000107 from the router's settings now. The record names this as the fixed version.

Score 10 (CVSS 4.0), published by Acer on 24 November 2026. Weakness: CWE-306.

Any device on the router's WiFi can send one unauthenticated request to permanently delete files on an Acer Connect M6E 5G. No credentials are needed — only WiFi access. The record identifies the affected operation as deleting meeting recordings.

hexpm, CVE-2026-129514

Only self-hosted hexpm operators need act. The source identifies the fix at commit 379b0a29bcc95164249f38ad7d772a37a8ff9533 in hexpm/hexpm; no release version number is named in any source.

Score 10 (CVSS 4.0), published by EEF on 24 November 2026. Weakness: CWE-502.

An unauthenticated attacker can send a crafted request to any hexpm route and run operating system commands as the application process. The record states the parser runs before authentication. Active exploitation was recorded on 23 November 2026.

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-2026-109484,CVE-2026-128791,CVE-2026-129514
```

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-2026-109484 --cve CVE-2026-128791 --cve CVE-2026-129514
```

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 24 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-2026-109484: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C`

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-2026-128791: 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`

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-2026-129514: 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:A`

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.

Appendix 2. Timeline

Date	Event
24 November 2026	Microsoft Azure App Service for Linux, CVE-2026-109484: record published by Microsoft.
24 November 2026	Acer Connect M6E 5G Portable WiFi Router, CVE-2026-128791: record published by Acer.
24 November 2026	hexpm, CVE-2026-129514: record published by EEF.

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-2026-109484: https://www.cve.org/CVERecord?id=CVE-2026-109484
- CVE record for CVE-2026-128791: https://www.cve.org/CVERecord?id=CVE-2026-128791
- CVE record for CVE-2026-129514: https://www.cve.org/CVERecord?id=CVE-2026-129514