contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

13 November 2026 · 3 new critical CVEs worth reading

Analysis Report

218 new records scored 8.5 or higher in the last 30 hours. 3 to read first, and the conditions each score leaves out.

PREPARED BY	NamiQ	DATE	13 November 2026
FACTS AS OF	13 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-2026-11-13

The bottom line

> *All three records describe remotely exploitable flaws where no named patched version exists and the attacker needs no prior access — or only a free or subscriber account. The question that sorts them: which of these three products is running in your environment right now?*

879 CVE records were published in the last 30 hours. 218 scored 8.5 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
Linksys EA8100 (CVE-2026-127275)	10 (CVSS 4.0)	See the note	Technical Analysis
Jet Admin Cloud Platform (CVE-2026-123965)	9.9 (CVSS 3.1)	No fixed version is named in the record; remediation status is 'none available'. A source states mitigation via a sandbox component around 29 October 2026, but no release number is given.	Technical Analysis
themagnifico52 Hotel Booking Lite (CVE-2026-125851)	9.9 (CVSS 3.1)	No official patch is available. The CVE record lists no unaffected version. Patchstack reported this on 11 November 2026 and states no patch exists.	Technical Analysis

Linksys EA8100, CVE-2026-127275

No patched firmware is named. Block the router's management interface from the internet immediately. The exploit is public.

Score 10 (CVSS 4.0), published by VulDB on 12 November 2026. Weakness: CWE-306, CWE-287.

Two functions in the Linksys EA8100's JNAP API do not check who is calling. The record says a remote attacker can change remote-management and WiFi-warning settings without logging in. The exploit is public and the vendor did not respond.

Jet Admin Cloud Platform, CVE-2026-123965

No fixed version is named. Contact Jet Admin to confirm the October 2026 sandbox mitigation covers your deployment, then rotate all credentials held in .env files.

Score 9.9 (CVSS 3.1), published by Cisa-cg on 13 November 2026. Weakness: CWE-200.

Scored 9.9. A free Jet Admin account is enough for a remote attacker to expose the platform's .env files and extract the credentials in them. A source states a sandbox mitigation was applied around 29 October 2026; no release number is given.

themagnifico52 Hotel Booking Lite, CVE-2026-125851

No patch exists. If Hotel Booking Lite at 2.5.1 or earlier is installed, disable user registration immediately. The analysis notes this flaw type is used in mass-exploit campaigns targeting many sites.

Score 9.9 (CVSS 3.1), published by Patchstack on 13 November 2026. Weakness: CWE-434.

A subscriber-level WordPress account is enough to upload a PHP web shell to a site running Hotel Booking Lite at version 2.5.1 or earlier. This gives the attacker command execution using the web server's own permissions. No patch is named in the record.

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-2026-127275,CVE-2026-123965,CVE-2026-125851
```

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-2026-127275 --cve CVE-2026-123965 --cve CVE-2026-125851
```

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 13 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-2026-127275: 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-2026-123965: score 9.9, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:L`

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	Low	Some data or behaviour can be altered.
Availability	Low	Reduced performance or interruptions.

CVE-2026-125851: 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
12 November 2026	Linksys EA8100, CVE-2026-127275: record published by VulDB.
13 November 2026	Jet Admin Cloud Platform, CVE-2026-123965: record published by Cisa-cg.
13 November 2026	themagnifico52 Hotel Booking Lite, CVE-2026-125851: 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-2026-127275: https://www.cve.org/CVERecord?id=CVE-2026-127275
- CVE record for CVE-2026-123965: https://www.cve.org/CVERecord?id=CVE-2026-123965
- CVE record for CVE-2026-125851: https://www.cve.org/CVERecord?id=CVE-2026-125851