contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

22 November 2026 · 3 new critical CVEs worth reading

Analysis Report

81 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	22 November 2026
FACTS AS OF	22 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-2026-11-22

The bottom line

> *THE BOTTOM LINE: three remotely exploitable, high-scoring flaws across a consumer router, a WordPress plugin, and a database engine — two with no recorded fix. The question that sorts them: does your network include a D-Link DIR-600L, a site running Nexter Blocks Pro, or a SurrealDB instance?*

383 CVE records were published in the last 30 hours. 81 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
D-Link DIR-600L (CVE-2026-133993)	10 (CVSS 4.0)	See the note	Technical Analysis
POSIMYTH Nexter Blocks Pro (CVE-2026-125294)	9.8 (CVSS 3.1)	See the note	Technical Analysis
surrealdb (CVE-2026-134292)	9.8 (CVSS 3.1)	SurrealDB 4.0.0, per the GitHub security advisory GHSA-5w6j-qm42-4rc2 published 3 November 2026 and the VulnCheck record published 21 November 2026.	Technical Analysis

D-Link DIR-600L, CVE-2026-133993

Any D-Link DIR-600L on firmware 2.17b02 is exposed; the exploit is public and no fix is recorded. Disable UPnP on the device now and check D-Link for a firmware update.

Score 10 (CVSS 4.0), published by VulDB on 21 November 2026. Weakness: CWE-121, CWE-119.

A remote attacker can send a crafted request to the GENA subscription handler, triggering a stack-based buffer overflow and potentially running their own code on the device. The record names firmware version 2.17b02. The record states no limiting condition.

POSIMYTH Nexter Blocks Pro, CVE-2026-125294

Any site running Nexter Blocks Pro at 5.0.10 or below is exposed; no fix is recorded. Deactivate the plugin now and audit for unexpected administrator accounts.

Score 9.8 (CVSS 3.1), published by Wordfence on 21 November 2026. Weakness: CWE-269.

An unauthenticated attacker can bypass the plugin's filter using Unicode look-alike characters and register a WordPress account with full Administrator access. Versions up to and including 5.0.10 are affected. The record states no limiting condition.

surrealdb, CVE-2026-134292

Update SurrealDB to 4.0.0; the GitHub security advisory GHSA-5w6j-qm42-4rc2 names this as the fix. If only fully trusted administrators connect, risk is lower. Confirm the version in use first.

Score 9.8 (CVSS 3.1), published by VulnCheck on 21 November 2026. Weakness: CWE-862.

An authenticated user blocked from certain built-in functions can call them through the embedded JavaScript engine, bypassing access controls. The record lists SurrealDB versions 1.0.0 to below 4.0.0 as affected. A database account is required.

Conditions the score may not show: authenticated.

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-2026-133993,CVE-2026-125294,CVE-2026-134292
```

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-2026-133993 --cve CVE-2026-125294 --cve CVE-2026-134292
```

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 22 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-2026-133993: 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-2026-125294: 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.

CVE-2026-134292: 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
21 November 2026	D-Link DIR-600L, CVE-2026-133993: record published by VulDB.
21 November 2026	POSIMYTH Nexter Blocks Pro, CVE-2026-125294: record published by Wordfence.
21 November 2026	surrealdb, CVE-2026-134292: record published by VulnCheck.

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-2026-133993: https://www.cve.org/CVERecord?id=CVE-2026-133993
- CVE record for CVE-2026-125294: https://www.cve.org/CVERecord?id=CVE-2026-125294
- CVE record for CVE-2026-134292: https://www.cve.org/CVERecord?id=CVE-2026-134292