contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

8 November 2026 · 3 new critical CVEs worth reading

Analysis Report

84 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	8 November 2026
FACTS AS OF	8 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-2026-11-08

The bottom line

> *THE BOTTOM LINE: three records today, all scored 9.9 or above, covering different products with no shared flaw. Two — OpenAM and Kyverno — have vendor fixes; the D-Link DIR-878 is end-of-life with none available. The sorting question: does your environment run any of these three products?*

339 CVE records were published in the last 30 hours. 84 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
OpenIdentityPlatform OpenAM (CVE-2026-123551)	10 (CVSS 4.0)	OpenAM 16.1.4 — packages openam-federation-library, openam-notifications-websocket, and openam-server-only (advisory GHSA-5c3q-hp86-xjr8, published 22 October 2026).	Technical Analysis
D-Link DIR-878 (CVE-2026-124560)	10 (CVSS 2.0)	No fixed version. The record states this product is no longer supported by its maintainer, and no unaffected release is listed.	Technical Analysis
kyverno (CVE-2026-124440)	9.9 (CVSS 3.1)	1.19.2 (GitHub advisory GHSA-39w8-hv5g-f73w, published 23 October 2026)	Technical Analysis

OpenIdentityPlatform OpenAM, CVE-2026-123551

Anyone running OpenAM 14.0.0 to 16.1.3 should upgrade to 16.1.4. The analysis cites advisory GHSA-5c3q-hp86-xjr8, published 22 October 2026, as the fix. Confirm the installed version first.

Score 10 (CVSS 4.0), published by VulnCheck on 8 November 2026. Weakness: CWE-201.

The record describes a legacy endpoint bypass letting an unauthenticated attacker passively collect live session tokens from the notification WebSocket, hijacking sessions. The one limit: network access to the OpenAM port. Affects versions 14.0.0 to 16.1.3.

D-Link DIR-878, CVE-2026-124560

No fix exists. The record states the DIR-878 is no longer supported and lists no unaffected release. Any organisation still running this device should plan to replace it.

Score 10 (CVSS 2.0), published by VulDB on 9 November 2026. Weakness: CWE-122, CWE-119.

The record says the DIR-878 HNAP handler at firmware version 1.20B05 has a heap-based buffer overflow triggered by a crafted uid argument, potentially allowing remote code execution. The record notes the exploit is public. The record states no limiting condition.

kyverno, CVE-2026-124440

Teams running Kyverno 1.19.1 on a shared cluster where namespace tenants can create policies should update to 1.19.2. Only 1.19.1 is listed as affected. Confirm the installed version first.

Score 9.9 (CVSS 3.1), published by VulnCheck on 8 November 2026. Weakness: CWE-441.

A user who can create namespaced Policies can append a malformed percent-escape to an API call path, bypass the namespace guard, and run calls as the admission-controller service account at cluster scope, escalating to cluster admin. Affects Kyverno 1.19.1 only.

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-2026-123551,CVE-2026-124560,CVE-2026-124440
```

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-2026-123551 --cve CVE-2026-124560 --cve CVE-2026-124440
```

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 8 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-2026-123551: 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-2026-124440: 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
8 November 2026	OpenIdentityPlatform OpenAM, CVE-2026-123551: record published by VulnCheck.
9 November 2026	D-Link DIR-878, CVE-2026-124560: record published by VulDB.
8 November 2026	kyverno, CVE-2026-124440: 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-2026-123551: https://www.cve.org/CVERecord?id=CVE-2026-123551
- CVE record for CVE-2026-124560: https://www.cve.org/CVERecord?id=CVE-2026-124560
- CVE record for CVE-2026-124440: https://www.cve.org/CVERecord?id=CVE-2026-124440