contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

11 November 2026 · 3 new critical CVEs worth reading

Analysis Report

436 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	11 November 2026
FACTS AS OF	11 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-2026-11-11

The bottom line

> *THE BOTTOM LINE: The three records are unrelated — a WordPress plugin, a conferencing platform, and a container registry — but all score 9.9 or higher and can be reached over a network with no or minimal authentication. The question that sorts them: which of these products runs in your environment?*

2174 CVE records were published in the last 30 hours. 436 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
STAGGS (CVE-2026-78287)	10 (CVSS 3.1)	3.4.0, per the Patchstack advisory published 9 November 2026.	Technical Analysis
Adobe Connect (CVE-2026-121351)	10 (CVSS 3.1)	Per the vendor's advisory (APSB26-191, 10 November 2026): 12.12.a, 12.11.i, 12.10.f, 12.9.a, and 12.8.a on Windows. The CVE record names 12.8.a as the first unaffected release.	Technical Analysis
Red Hat OpenShift Update Service (CVE-2026-110697)	9.9 (CVSS 3.1)	Red Hat Quay 3.9.28, 3.10.28, 3.12.24, 3.14.10, 3.15.9, 3.16.7, 3.17.7, or 3.18.3, per the vendor's advisory. Quay.io has already been fixed by Red Hat.	Technical Analysis

STAGGS, CVE-2026-78287

Anyone running STAGGS at version 3.3.0 or earlier should update now. The Patchstack advisory names 3.4.0 as the fixed version. Check which version is installed across all WordPress sites first.

Score 10 (CVSS 3.1), published by Patchstack on 11 November 2026. Weakness: CWE-94.

The STAGGS WordPress plugin at version 3.3.0 or earlier has a code injection flaw (CWE-94). The Patchstack advisory says any internet-based attacker can inject and run code on the web server without holding an account. The record states no limiting condition.

Adobe Connect, CVE-2026-121351

Anyone on Adobe Connect 12.8 or earlier should act now. The vendor's advisory APSB26-191 names fixed releases per branch; the record names 12.8.a as the first unaffected release.

Score 10 (CVSS 3.1), published by Adobe on 10 November 2026. Weakness: CWE-22.

Adobe Connect at version 12.8 or earlier has a path traversal flaw (CWE-22). The record says an attacker can read files outside the application's scope with no account and no user interaction. The record states no limiting condition.

Conditions the score may not show: needs a user action.

Red Hat OpenShift Update Service, CVE-2026-110697

Anyone running Red Hat Quay shared across teams should update. The vendor's advisory names fixed releases across Quay versions 3.9 through 3.18. The vendor says Quay.io is already fixed.

Score 9.9 (CVSS 3.1), published by Redhat on 11 November 2026. Weakness: CWE-89.

In Red Hat Quay, an attacker with any account can create a namespace name that acts as a SQL wildcard, retrieving decrypted robot tokens from other tenants. The vendor's advisory scores this 9.9; a low-privilege account is the only prerequisite.

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-2026-78287,CVE-2026-121351,CVE-2026-110697
```

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-2026-78287 --cve CVE-2026-121351 --cve CVE-2026-110697
```

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 11 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-2026-78287: 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.

CVE-2026-121351: 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-2026-110697: 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
11 November 2026	STAGGS, CVE-2026-78287: record published by Patchstack.
10 November 2026	Adobe Connect, CVE-2026-121351: record published by Adobe.
11 November 2026	Red Hat OpenShift Update Service, CVE-2026-110697: record published by Redhat.

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-2026-78287: https://www.cve.org/CVERecord?id=CVE-2026-78287
- CVE record for CVE-2026-121351: https://www.cve.org/CVERecord?id=CVE-2026-121351
- CVE record for CVE-2026-110697: https://www.cve.org/CVERecord?id=CVE-2026-110697