contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

12 November 2026 · 3 new critical CVEs worth reading

Analysis Report

130 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	12 November 2026
FACTS AS OF	12 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-2026-11-12

The bottom line

> *Three new high-scoring flaws, all fixed by the vendor. The one question that sorts them: does an attacker need to log in first? The STAGGS WordPress plugin flaw needs no account, so any site running it is exposed to anyone. The Quay and M365 Manager Plus flaws each need a valid login.*

694 CVE records were published in the last 30 hours. 130 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
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
Zohocorp M365 Manager Plus (CVE-2026-12591)	9.9 (CVSS 3.1)	M365 Manager Plus build 4818 (the vendor's advisory says it was fixed on 24 June 2026; builds 4817 and earlier are affected).	Technical Analysis

STAGGS, CVE-2026-78287

Anyone running the STAGGS WordPress plugin should update to 3.4.0 now; 3.3.0 and earlier are affected. No login is needed, so treat it as urgent and first find which sites have it installed.

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

A code-injection flaw lets an attacker run code on the web server without any account. It affects WordPress sites running the STAGGS plugin at version 3.3.0 or earlier. The record states no limiting condition.

Red Hat OpenShift Update Service, CVE-2026-110697

If you run no Quay or OpenShift registry, nothing to do. Anyone sharing one across teams should move to the patched build for their branch; the advisory lists fixes from 3.9.28 to 3.18.3.

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

An authenticated user crafts a namespace name whose wildcard character matches other tenants, then steals their robot-account tokens to read, push or overwrite their images. One limit: a basic account on a shared Quay or OpenShift registry is needed.

Zohocorp M365 Manager Plus, CVE-2026-12591

Running ManageEngine M365 Manager Plus? Upgrade to build 4818; 4817 and earlier are affected. The flaw needs a logged-in technician, so a server with no delegated technicians can wait.

Score 9.9 (CVSS 3.1), published by Zohocorp on 12 November 2026. Weakness: CWE-862.

A logged-in technician exploits weak permission checks in the delegated administration interface to gain rights beyond their role, leading to code execution on the server. It affects ManageEngine M365 Manager Plus, and needs a technician login.

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-2026-78287,CVE-2026-110697,CVE-2026-12591
```

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-2026-110697 --cve CVE-2026-12591
```

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 12 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-2026-110697: 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.

CVE-2026-12591: 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.
11 November 2026	Red Hat OpenShift Update Service, CVE-2026-110697: record published by Redhat.
12 November 2026	Zohocorp M365 Manager Plus, CVE-2026-12591: record published by Zohocorp.

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-2026-110697: https://www.cve.org/CVERecord?id=CVE-2026-110697
- CVE record for CVE-2026-12591: https://www.cve.org/CVERecord?id=CVE-2026-12591