contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

31 October 2026 · 3 new critical CVEs worth reading

Analysis Report

68 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	31 October 2026
FACTS AS OF	31 October 2026	VERSION	1.0
TOP SCORE	Critical: 9.9	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-2026-10-31

The bottom line

> *Three unrelated products, each with a flaw that lets an attacker run commands or code on a server. The question that sorts them: do you run any of them? Only the invoice plugin needs no login; the other two need an account.*

339 CVE records were published in the last 30 hours. 68 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
pgadmin.org pgAdmin 4 (CVE-2026-116241)	9.9 (CVSS 3.1)	pgAdmin 4 9.19. The record lists versions before 9.19 as affected. The tracking issue says the fix is pending for 9.19, and no source confirms a release.	Our note, below
mqttsnet thinglinks (CVE-2026-62853)	9.9 (CVSS 3.1)	ThingLinks 1.4.0 (released 22 July 2026, per the project's release notes)	Our note, below
addonsorg PDF Invoice for WooCommerce + Drag and Drop Template Builder (CVE-2026-109220)	9.8 (CVSS 3.1)	See the note	Our note, below

pgadmin.org pgAdmin 4, CVE-2026-116241

If you run pgAdmin 4, limit who can sign in now. Ask your IT provider to move to 9.19 once it is released. The tracking issue says the fix is pending; no release is confirmed.

Score 9.9 (CVSS 3.1), published by PostgreSQL on 30 October 2026. Weakness: CWE-78, CWE-115.

An ordinary database role can make pgAdmin's Import/Export tool run an operating-system command on the pgAdmin host, as the account running pgAdmin. The description ties it to standard_conforming_strings being off.

mqttsnet thinglinks, CVE-2026-62853

If you run ThingLinks, update to 1.4.0 this week. Before that, find out who can log in to it.

Score 9.9 (CVSS 3.1), published by GitHub on 30 October 2026. Weakness: CWE-78, CWE-94.

A logged-in user can send their own Groovy code to the rule engine's script endpoint, and the server runs it with no sandbox. The attacker needs a login, which the vendor's advisory says can be low-privilege.

Conditions the score may not show: authenticated.

addonsorg PDF Invoice for WooCommerce + Drag and Drop Template Builder, CVE-2026-109220

If you run this plugin, act today: check whether it is installed and which version. No fixed version is named in the sources, so do not assume one.

Score 9.8 (CVSS 3.1), published by Wordfence on 31 October 2026. Weakness: CWE-502.

The record says text in the checkout note field reaches code that rebuilds PHP objects without checks, so someone with no account can run code on the server. The record states no limiting condition.

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.

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 31 October 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-2026-116241: 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-2026-62853: 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-2026-109220: 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
30 October 2026	pgadmin.org pgAdmin 4, CVE-2026-116241: record published by PostgreSQL.
30 October 2026	mqttsnet thinglinks, CVE-2026-62853: record published by GitHub.
31 October 2026	addonsorg PDF Invoice for WooCommerce + Drag and Drop Template Builder, CVE-2026-109220: record published by Wordfence.

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-2026-116241: https://www.cve.org/CVERecord?id=CVE-2026-116241
- CVE record for CVE-2026-62853: https://www.cve.org/CVERecord?id=CVE-2026-62853
- CVE record for CVE-2026-109220: https://www.cve.org/CVERecord?id=CVE-2026-109220