

DAILY CVE HIGHLIGHT

Daily CVE highlight

31 October 2026 · 3 new critical CVEs worth reading

Analysis Report

124 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: 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-2026-10-31

The bottom line

Three unrelated products, three different weaknesses, and each scores 10. One question sorts them: do you run LXD or MicroCloud, SOCFortress CoPilot, or Bazarr? If not, none of these concerns you.

605 CVE records were published in the last 30 hours. 124 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
Canonical LXD (CVE-2026-112816)	10 (CVSS 4.0)	lxd 6.10.1, 5.21.9, 5.0.11, 4.0.15; microcloud 2.1.5, 3.4.1 (snap, 29 October 2026)	Our note, below
socfortress CoPilot (CVE-2026-61738)	10 (CVSS 3.1)	0.1.77, taken from the record's affected range (before 0.1.77). The sources give no release notes or fix date.	Our note, below
morpheus65535 bazarr (CVE-2026-61826)	10 (CVSS 3.1)	1.5.7-beta.14 (the record says versions before it are affected; no other fixed version is named)	Our note, below

Canonical LXD, CVE-2026-112816

If you run LXD or MicroCloud, update this week: LXD 6.10.1, 5.21.9, 5.0.11 or 4.0.15, or MicroCloud 2.1.5 or 3.4.1. The vendor released these fixes on 29 October 2026.

Score 10 (CVSS 4.0), published by Canonical on 30 October 2026. Weakness: CWE-295.

A crafted certificate chain lets an unauthenticated attacker be treated as any trusted client, with full access to the cluster and its virtual machines. It matters where the attacker can reach the LXD HTTPS listener.

socfortress CoPilot, CVE-2026-61738

If you run CoPilot below 0.1.77, ask your IT provider this week to move to 0.1.77 or later. That version comes from the record's affected range; no fix date is given.

Score 10 (CVSS 3.1), published by GitHub on 30 October 2026. Weakness: CWE-22, CWE-73, CWE-434.

A crafted file name in the Google Cloud report upload makes the server write the uploaded JSON outside the report folder. It needs an admin or analyst login and content that passes as valid Google

Cloud report JSON.

morpheus65535 bazarr, CVE-2026-61826

If you run Bazarr, first check who can reach it, then update to 1.5.7-beta.14 or later now. The record names no other fixed version.

Score 10 (CVSS 3.1), published by GitHub on 30 October 2026. Weakness: CWE-352, CWE-862.

Bazarr's Plex endpoints ask for no API key, so an anonymous caller can switch off the Plex link, store their own key, or bind their own Plex account. It matters only if an untrusted person can reach Bazarr.

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-2026-112816: 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-2026-61738: 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-2026-61826: 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.

Appendix 2. Timeline

Date	Event
30 October 2026	Canonical LXD, CVE-2026-112816: record published by Canonical.
30 October 2026	socfortress CoPilot, CVE-2026-61738: record published by GitHub.
30 October 2026	morpheus65535 bazarr, CVE-2026-61826: record published by GitHub.

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-2026-112816: <https://www.cve.org/CVERecord?id=CVE-2026-112816>
- CVE record for CVE-2026-61738: <https://www.cve.org/CVERecord?id=CVE-2026-61738>
- CVE record for CVE-2026-61826: <https://www.cve.org/CVERecord?id=CVE-2026-61826>