contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

30 October 2026 · 3 new critical CVEs worth reading

Analysis Report

121 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	30 October 2026
FACTS AS OF	30 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-2026-10-30

The short version

769 CVE records were published in the last 30 hours. 121 scored 8.5 or higher. 3 are below.

None of these is on CISA's exploited list, which means nothing public says yet that anyone is using them. A high score is the record's author describing the worst case. Read the conditions before you act on the number.

The three records are unrelated: different products, different weaknesses. One question sorts them. Do you run Canonical LXD, SOCFortress CoPilot or Bazarr? If not, none of these applies to you.

How we chose: highest score first, then fewest conditions in the wording, one product each. It is a fixed rule, not a judgement about your estate.

Canonical LXD, CVE-2026-112816

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

An unauthenticated attacker can present a crafted certificate chain and be accepted as any trusted client, with full access to the cluster and its virtual machines. The flaw is in the HTTPS listener, so check that exposure first.

> *Improper certificate validation in the HTTPS listener in Canonical LXD 4.0.14, 5.0.10, 5.21.8, 6.9 before 4.0.15, 5.0.11, 5.21.9, 6.10.1 allows an unauthenticated attacker to authenticate as any trusted client and gain full access to the cluster and managed virtual machines via a crafted certificate chain.*

Versions the record lists as affected:

- 4.0.14 up to, but not including, 4.0.15
- 5.0.10 up to, but not including, 5.0.11
- 5.21.8 up to, but not including, 5.21.9
- 6.9.0 up to, but not including, 6.10.1

If you run it: check the version, then read the vendor's page before you change anything.

socfortress CoPilot, CVE-2026-61738

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

A logged-in admin or analyst can upload a GCP report file whose raw filename is passed to the file writer, a path-handling flaw. The record is cut off, so the full effect is not shown. It needs an admin or analyst account.

> *SOCFortress CoPilot focuses on providing a single pane of glass for all your security operations needs. Prior to 0.1.77, `POST /api/scoutsuite/generate-gcp-report` in `backend/app/integrations/scoutsuite/routes/scoutsuite.py` admits admin and analyst users and validates the uploaded content as `GCPScoutSuiteJSON`, but passes raw `file.filename` from the multipart header to `save_file_to_directory` in `backend/app/integrations/scoutsuite/services/scoutsuite.py`. The writer combines this filename with …*

Versions the record lists as affected:

- < 0.1.77

If you run it: check the version, then read the vendor's page before you change anything.

morpheus65535 bazarr, CVE-2026-61826

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

Without logging in, anyone can clear Bazarr's stored Plex credentials and disable the integration, or save a key of their choosing. No PIN, account or prior state is needed. The record states no limiting condition.

> *Bazarr is a companion application to Sonarr and Radarr. Prior to 1.5.7-beta.14, the `api_ns_plex` namespace in `bazarr/api/plex/oauth.py` omits `@authenticate` on its Resource handlers, while normal APIs require an API key and no global authentication hook compensates. Anonymous callers can invoke `POST /api/plex/oauth/logout` to clear credentials and disable the integration, or `POST /api/plex/apikey` to persist an attacker-selected key, without a PIN, account or state precondition. `POST /api/plex/oauth/pin` and …*

Versions the record lists as affected:

- < 1.5.7-beta.14

If you run it: check the version, then read the vendor's page before you change anything.

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 list.
- If it is in range, open the vendor's page and note the fixed version and any mitigation.
- Book the update, and write down who owns it and by when.

What we could not confirm

- These are new records. We have not read each vendor's advisory page, and we have not tested any of them.
- A record can change in the first days: scores, versions and wording are as at 30 October 2026.
- Exploitation is not recorded for any of them. That is not the same as none.
- The sentences that open the page and each pick are our interpretation of the records, 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