contact@namiq.io · namiq.io

NamiQ

WEEKLY HIGHLIGHT AND GUIDELINE

Weekly highlight and guideline

Week to 22 November 2026 · 5 exploited, 20 new critical

Analysis Report

The week to 22 November 2026: 5 entries added to CISA's exploited list, 20 new critical records worth reading, the deadlines to watch, and a plan for Monday to Friday.

PREPARED BY	NamiQ	DATE	22 November 2026
FACTS AS OF	22 November 2026	VERSION	1.0
ACT ON FIRST	3 of 5	STATUS	Facts as at 22 November 2026

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/weekly-highlight-2026-11-22

The bottom line

> *From 16 November 2026 to 22 November 2026 CISA added 5 vulnerabilities to its exploited list, 3 with a deadline within three days of today or already past. The daily highlights named 20 new critical records that nothing says yet anyone is using. Start Monday with the exploited list. It is the work list; the new records are a reading list.*

At a glance

Entry	What it is	Act by	Fixed in	Read next
Vanderbilt University Research Electronic Data Capture (REDCap), CVE-2026-90817	On CISA's exploited list	1 day past CISA's deadline	REDCap 16.0.49 LTS, 17.3.10 LTS or 17.4.4 Standard Release, as applicable (CVE record; no fix date given)	Technical Analysis
Synology DiskStation Manager (DSM), CVE-2024-10441	On CISA's exploited list	1 day past CISA's deadline	DSM 7.2.2-72806-1, 7.2.1-69057-6, 7.2-64570-4, 7.1.1-42962-7; BSM 1.1-65374 (vendor advisory, first published 5 November 2024)	Technical Analysis
Apache Axis, CVE-2026-90436	On CISA's exploited list	1 day past CISA's deadline	Not stated; see the note	Technical Analysis
Perforce Puppet Enterprise, CVE-2026-115731	On CISA's exploited list	CISA's date 1 December 2026	Puppet Enterprise 2023.8.13, 2025.12.1 or 2026.0.1 (these bundle puppet-agent 8.22.2 or 9.1.3), then restart puppet server. The record says so; no vendor page was read.	Technical Analysis
BerriAI LiteLLM, CVE-2026-40217	On CISA's exploited list	CISA's date 2 December 2026	Not stated; see the note	Technical Analysis
rucio (CVE-2026-100397)	New record, scored 10	Check this week	35.9.1, 38.6.1, 40.4.2, 41.1.1 (as the CVE record states them)	Technical Analysis
ASUS Control Center Express (CVE-2026-114202)	New record, scored 10	Check this week	See the note	Technical Analysis

Oracle Corporation Oracle Business Intelligence Enterprise Edition (CVE-2026-114784)	New record, scored 10	Check this week	See the note	Technical Analysis
Oracle Corporation Oracle Platform Security for Java (CVE-2026-114824)	New record, scored 10	Check this week	See the note	Technical Analysis
lxc incus (CVE-2026-130778)	New record, scored 10	Check this week	Incus 7.6.0 (the vendor's advisory, 29 October 2026; the record lists 7.6.0 as unaffected).	Technical Analysis
Mitel MiCollab (CVE-2026-133323)	New record, scored 10	Check this week	The vendor's advisory says a patch is available for release 10.3 (10.3.0.18) that addresses this flaw; upgrade to that release and apply the patch. No higher fixed build is named.	Technical Analysis
D-Link DIR-600L (CVE-2026-133493)	New record, scored 10	Check this week	See the note	Technical Analysis
D-Link DIR-600L (CVE-2026-133993)	New record, scored 10	Check this week	See the note	Technical Analysis
Tegsoft Yönetim ve Bilişim Hizmetleri Tic. Ltd. Şti. Tegsoft Contact Center (CVE-2026-14914)	New record, scored 10	Check this week	The record states all versions before latest-202611161510 are affected, making that the first unaffected version. No vendor advisory was available to confirm this.	Technical Analysis
Arize-ai phoenix (CVE-2026-53998)	New record, scored 10	Check this week	15.7.0. The record says it is fixed there. The release notes dated 13 May 2026 list 'prevent format-string injection in f-string template formatter'.	Technical Analysis
hefy2027 cf-manager (CVE-2026-71499)	New record, scored 10	Check this week	cf-manager 1.1.2. Both the CVE record and the project's release notes name it as the fixed version.	Technical Analysis
mirendev runtime (CVE-2026-75521)	New record, scored 10	Check this week	0.11.1. The vendor's advisory says to upgrade and restart the server so the new listener setting takes effect.	Technical Analysis

flytohub flyto-core (CVE-2026-77312)	New record, scored 10	Check this week	flyto-core 2.26.8 (PyPI); the vendor's release notes call it a security release fixing this arbitrary file write and four other advisories.	Technical Analysis
Dassault Systèmes Station Launcher App in 3DEXPERIENCE platform (CVE-2026-93664)	New record, scored 10	Check this week	See the note	Technical Analysis
Danfoss AK-SC 355 (CVE-2026-127057)	New record, scored 9.9	Check this week	No fixed release. The record lists all versions as affected and names no unaffected release. The vendor says to migrate to the AK-SM800A series for ongoing security updates.	Technical Analysis
D-Link DCS-935L (CVE-2026-133680)	New record, scored 9.9	Check this week	See the note	Technical Analysis
POSIMYTH Nexter Blocks Pro (CVE-2026-125294)	New record, scored 9.8	Check this week	See the note	Technical Analysis
tenseijs @tensei/auth (CVE-2026-129552)	New record, scored 9.8	Check this week	See the note	Technical Analysis
surrealdb (CVE-2026-134292)	New record, scored 9.8	Check this week	SurrealDB 4.0.0, per the GitHub security advisory GHSA-5w6j-qm42-4rc2 published 3 November 2026 and the VulnCheck record published 21 November 2026.	Technical Analysis
CVE-2026-67429 (CVE-2026-67429)	New record	Check this week	See the note	The vendor's page

What was added, day by day

- 17 November 2026: Perforce Puppet Enterprise, CVE-2026-115731.
- 18 November 2026: Vanderbilt University Research Electronic Data Capture (REDCap), CVE-2026-90817; Synology DiskStation Manager (DSM), CVE-2024-10441; Apache Axis, CVE-2026-90436; BerriAI LiteLLM, CVE-2026-40217.

The exploited list: what to do with each

- Vanderbilt University Research Electronic Data Capture (REDCap), CVE-2026-90817, 1 day past CISA's deadline.
- Synology DiskStation Manager (DSM), CVE-2024-10441, 1 day past CISA's deadline.
- Apache Axis, CVE-2026-90436, 1 day past CISA's deadline.
- Perforce Puppet Enterprise, CVE-2026-115731, due in 9 days.
- BerriAI LiteLLM, CVE-2026-40217, due in 10 days.

New critical records worth reading

None of these is on CISA's exploited list when we read it, so a score here is the record's author describing the worst case. Read the condition before you act on the number.

- rucio, CVE-2026-100397, scored 10. If you run Rucio on a version below the fixed releases, upgrade to 35.9.1, 38.6.1, 40.4.2 or 41.1.1 this week, starting with any server that untrusted networks can reach. If you do not run Rucio, stop reading.
- ASUS Control Center Express, CVE-2026-114202, scored 10. If you run ASUS Control Center Express, your IT contact should find the installed version this week and ask ASUS for the fixed release. If you do not run it, you can stop reading.
- Oracle Corporation Oracle Business Intelligence Enterprise Edition, CVE-2026-114784, scored 10. Anyone running Oracle Business Intelligence Enterprise Edition 8.2.0.0.0 or 26.01.0.0.0 should treat this as urgent, starting today, 17 November 2026. First find out whether it is run and whether it can be reached over HTTP. If you do not run it, stop reading.
- Oracle Corporation Oracle Platform Security for Java, CVE-2026-114824, scored 10. If you run Oracle Fusion Middleware, find out this week whether Oracle Platform Security for Java is installed and which version it is. The record lists 12.2.1.4.0 and 14.1.2.0.0. If you do not run it, you can stop reading.
- lxc incus, CVE-2026-130778, scored 10. If you run Incus before 7.6.0 and its HTTPS listener can be reached by anyone you do not trust, act now: restrict that access to trusted hosts, then upgrade to 7.6.0. If you do not run Incus, or the listener is not enabled, you can stop reading.
- Mitel MiCollab, CVE-2026-133323, scored 10. Anyone running Mitel MiCollab should act now; if you do not run it, you can stop reading. First find out whether the Audio, Web and Video Conferencing component is in use and on which version, so you can plan the vendor's patch.
- D-Link DIR-600L, CVE-2026-133493, scored 10. If you run no D-Link DIR-600L router, you can stop here. If you run version 2.17b02, treat it as exposed: no fixed version is named, so restrict who can reach the device and plan a replacement now.
- D-Link DIR-600L, CVE-2026-133993, scored 10. Anyone running a D-Link DIR-600L on firmware 2.17b02 should act without delay: the exploit is already public and no patched firmware is recorded. Disable UPnP on the device now and check for a firmware update from D-Link.

- Tegsoft Yönetim ve Bilişim Hizmetleri Tic. Ltd. Şti. Tegsoft Contact Center, CVE-2026-14914, scored 10. Anyone running Tegsoft Contact Center must act immediately — the record assigns a CVSS score of 10, the maximum. First, confirm whether this product is deployed in your estate; if it is, update to latest-202611161510 without delay.
- Arize-ai phoenix, CVE-2026-53998, scored 10. If you run Phoenix from 13.0.0 up to but not including 15.7.0, update to 15.7.0 this week. If you do not run Phoenix, stop reading. First find the version and whether anyone untrusted can reach the service.
- hefy2027 cf-manager, CVE-2026-71499, scored 10. If you run cf-manager, move to 1.1.2 this week and check that API_SECRET is set before you do anything else. If you do not run cf-manager, you can stop reading: nothing here concerns you.
- mirendev runtime, CVE-2026-75521, scored 10. If you run Miren Runtime below 0.11.1, upgrade to 0.11.1 and restart the server now, and check whether port 8443 is reachable from outside your management network. If you do not run Miren Runtime, you can stop reading.
- flytohub flyto-core, CVE-2026-77312, scored 10. If you do not run Flyto2 Core (the flyto-core package), you can stop here. If you do, plan an update to version 2.26.8 without delay, and first list where it runs and which version each host has.
- Dassault Systèmes Station Launcher App in 3DEXPERIENCE platform, CVE-2026-93664, scored 10. If you run the 3DEXPERIENCE platform with the Station Launcher App, ask your IT provider or Dassault Systèmes this week which release you are on and whether a fix exists. If you do not use 3DEXPERIENCE, you can stop reading.
- Danfoss AK-SC 355, CVE-2026-127057, scored 9.9. All versions of the Danfoss AK-SC 355 and AK-SM 800 Series are affected and the vendor's record names no fixed release. Operators of these devices should remove any public IP exposure immediately and change credentials before planning migration to the AK-SM800A series.
- D-Link DCS-935L, CVE-2026-133680, scored 9.9. Anyone running a D-Link DCS-935L on firmware 1.10.01 should act now: the exploit has been made public as of 20 November 2026 and no fixed firmware is listed. Restrict the camera's web interface to trusted network paths immediately, or take it offline until a patch is available.
- POSIMYTH Nexter Blocks Pro, CVE-2026-125294, scored 9.8. Any WordPress site running Nexter Blocks Pro version 5.0.10 or below is exposed to unauthenticated administrator account creation; the record scores this 9.8. The vendor's materials name no fixed version; deactivate the plugin now and check for unexpected administrator accounts.
- tenseijs @tensei/auth, CVE-2026-129552, scored 9.8. If you run a Tensei site that uses the auth package, check now whether its JWT secret is set. If it is not, set one and treat any past administrator activity as suspect. No fixed version is named, so do not wait for one. Everyone else can stop reading.
- surrealdb, CVE-2026-134292, scored 9.8. Anyone running SurrealDB between version 1.0.0 and 3.x with restricted user accounts should update to 4.0.0; there is no CISA deadline but the score is 9.8. If only fully trusted administrators connect to your SurrealDB instance, risk is lower — confirm the version first.
- CVE-2026-67429, CVE-2026-67429.

Deadlines to watch

CISA's own deadlines for entries on its list, including ones added before this week. A date in the past means the deadline has already gone.

CISA's date	Entry	Where it stands
21 November 2026	Synology DiskStation Manager (DSM), CVE-2024-10441	1 day past CISA's deadline
21 November 2026	Apache Axis, CVE-2026-90436	1 day past CISA's deadline
21 November 2026	Vanderbilt University Research Electronic Data Capture (REDCap), CVE-2026-90817	1 day past CISA's deadline

The guideline: your week, in order

Thirty minutes on Monday does most of the work. The rest of the week is waiting, and then proving it is done.

The routine, every week

- List what you run: servers, firewalls, VPNs, hypervisors, apps, and who looks after each. One line each is enough, and it is the step most firms skip.
- Compare that list with the table above, product by product. Read each version from the product itself, not from an old inventory.
- For each product that matches, read the fixed version in our technical analysis or the vendor's page, and reduce exposure first if you cannot update today.
- Book the update. Write down who owns it and the date. A change with no name and no date does not happen.
- Save the proof: the version output or a screenshot, with the date. That is what an auditor, an insurer or a customer will ask for.

Keep a weekly record

One row per product you run that appears above. Fill it in as you go and keep it: it is the evidence that the week was handled.

Product	Version found	Fixed version	Owner	Done on

Check it yourself in two minutes

Everything above comes from public sources. This command prints CISA's additions in the same seven days with their due dates:

```
curl -s https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json \
  | jq -r '.vulnerabilities[] | select(.dateAdded >= "2026-11-16" and .dateAdded <= "2026-11-
22")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 22 November 2026 it printed 5 rows, the ones above. A later run may show more.

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-2026-90817,CVE-2024-10441,CVE-2026-90436,CVE-2026-
115731,CVE-2026-40217
```

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-2026-90817 --cve CVE-2024-10441 --cve CVE-2026-90436 --cve CVE-2026-
115731 --cve CVE-2026-40217
```

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

- Who is using these flaws, and how often. CISA names no attacker and we do not guess one. Ransomware use is as CISA records it; "unknown" means not recorded.
- Figures are as at 22 November 2026: EPSS and scores move, and a new record can change in its first days. Nothing here has been tested, and the order is a rule on CISA's dates, not a verdict on your estate. Check what you run first.

Appendix 1. Timeline

Date	Event
21 November 2026	Vanderbilt University Research Electronic Data Capture (REDCap), CVE-2026-90817: CISA's deadline.
21 November 2026	Apache Axis, CVE-2026-90436: CISA's deadline.
21 November 2026	Synology DiskStation Manager (DSM), CVE-2024-10441: CISA's deadline.

Appendix 2. Definition of done

- Every product above was checked against what you run, and the list is dated.
- Each one you run has a version, an owner and a date.
- Anything past CISA's deadline is patched, or has a written reason and a limit on exposure.
- The weekly record is filled in and kept.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- CVE record service: https://www.cve.org/