contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

21 November 2026 · 5 exploited CVEs added this week

Analysis Report

5 entries added to CISA's exploited list in the week to 21 November 2026. 3 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	21 November 2026
FACTS AS OF	21 November 2026	VERSION	1.0
ACT ON NOW	3 of 5	STATUS	Facts as at 21 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/daily-threat-watch-2026-11-21

The bottom line

> *Three items have a CISA deadline of today, 21 November 2026 — REDCap (CVE-2026-90817), Apache Axis (CVE-2026-90436), and Synology DSM or BeeStation (CVE-2024-10441) — and must be acted on now. The two remaining items, LiteLLM and Puppet Enterprise, fall due in December.*

CISA added 5 vulnerabilities to its exploited list from 15 November 2026 to 21 November 2026. 3 have a deadline within three days or already past.

Separately, 615 new CVE records were published in the last 30 hours, 99 of them scored 8 or higher. They are in the day's CVE highlight, not on this list, because nothing says yet that anyone is using them.

What changed since the last watch

- Left the seven-day window (33): CVE-2026-123039, CVE-2026-114713, CVE-2026-116606, CVE-2026-111560, CVE-2026-124194, CVE-2026-20320, CVE-2026-125350, CVE-2026-111793, CVE-2026-123158, CVE-2026-116779, CVE-2026-123218, CVE-2026-102895, CVE-2026-19868, CVE-2026-119977, CVE-2024-27834, CVE-2026-111357, CVE-2026-118527, CVE-2026-97229, CVE-2026-76418, CVE-2026-46300, CVE-2026-41709, CVE-2026-111497, CVE-2026-48356, CVE-2026-109618, CVE-2026-109619, CVE-2026-104935, CVE-2026-59309, CVE-2026-59310, CVE-2026-47876, CVE-2026-41703, CVE-2024-27833, CVE-2024-27851, CVE-2024-27808.

No new entries were added since the previous watch of 20 November 2026. Thirty-three items left the tracked set; no deadlines passed since then.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
Vanderbilt University Research Electronic Data Capture (REDCap) (CVE-2026-90817)	Today	Due today	REDCap 16.0.49 LTS, 17.3.10 LTS or 17.4.4 Standard Release, as applicable (CVE record; no fix date given)	0.04
Synology DiskStation Manager (DSM) (CVE-2024-10441)	Today	Due today	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)	0.01
Apache Axis (CVE-2026-90436)	Today	Due today	Not stated; see the note	0.01

Perforce Puppet Enterprise (CVE-2026-115731)	Next patch cycle	Due in 10 days	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.	0.01
BerriAI LiteLLM (CVE-2026-40217)	Next patch cycle	Due in 11 days	Not stated; see the note	0.17

How the week connects

REDCap, Apache Axis, and Synology DSM all allow an unauthenticated remote attacker to run code on the server, though they are unrelated products with different weaknesses. REDCap and Puppet Enterprise share CWE-94 (improper control of code generation) but are different products with different attack paths. Puppet needs a CA-signed certificate to exploit; LiteLLM needs a logged-in user.

Do this today, in this order

- Vanderbilt University Research Electronic Data Capture (REDCap), CVE-2026-90817, due today. REDCap research data platform. An unauthenticated attacker with a valid public survey hash can pass a crafted file path during data import to run code on the server. Anyone who hosts REDCap must act.
- Synology DiskStation Manager (DSM), CVE-2024-10441, due today. Synology DiskStation (DSM) and BeeStation (BSM). A flaw in the system plugin daemon lets a remote attacker run code with no login. The vendor's advisory names fixed versions for both product lines.
- Apache Axis, CVE-2026-90436, due today. Apache Axis (record: end-of-life). A crafted SOAP fault makes Axis load an attacker-named class and run it with no login. No fix is recorded; the record advises moving away from Axis 1.x.

The first hour:

- Check whether REDCap, Apache Axis, or any Synology device runs in your environment — these three have a CISA deadline of today, 21 November 2026.
- For any Synology device found, check the firmware version against the fixed releases: DSM 7.2.2-72806-1, 7.2.1-69057-6, 7.2-64570-4, 7.1.1-42962-7, or BSM 1.1-65374.
- For REDCap, upgrade to 16.0.49, 17.3.10 or 17.4.4. For Apache Axis 1.x, the record states no patch exists; isolate it from the network.
- Note where LiteLLM and Puppet Enterprise run; act on Puppet Enterprise before 1 December 2026 and LiteLLM before 2 December 2026.

In the next patch cycle

- Perforce Puppet Enterprise, CVE-2026-115731, due in 10 days. Perforce Puppet Enterprise. A machine with a CA-signed certificate can run code on the Puppet Server via a crafted report; the record notes automatic signing may let an outsider obtain a certificate.
- BerriAI LiteLLM, CVE-2026-40217, due in 11 days. LiteLLM AI proxy. The record says a logged-in user can send code to a guardrail test endpoint and use bytecode rewriting to run it on the server. Check who can reach LiteLLM.

Who can skip most of this

Anyone who runs none of REDCap, Apache Axis, BerriAI LiteLLM, Synology DSM or BeeStation, and Perforce Puppet Enterprise has nothing to act on from this week's list; that does not mean their environment is free of other flaws.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *Hello, We have five CISA-listed vulnerabilities to review this week. Three have a deadline of today, 21 November 2026: REDCap (CVE-2026-90817), Apache Axis (CVE-2026-90436), and Synology DSM or BeeStation (CVE-2024-10441). Two more fall due shortly: Puppet Enterprise (CVE-2026-115731) by 1 December 2026, and BerriAI LiteLLM (CVE-2026-40217) by 2 December 2026. Please confirm in writing, for each product: whether we run it, the current version installed, and whether the fix is in place. For Apache Axis, as no patch is recorded, please confirm whether it has been isolated from the network or removed. We need written confirmation for the three with today's deadline by end of day. Thank you.*

Check it yourself in two minutes

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

```
curl -s https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json \
  | jq -r '.vulnerabilities[] | select(.dateAdded >= "2026-11-15" and .dateAdded <= "2026-11-
21")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 21 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.
- EPSS is recalculated daily; the figures are as at 21 November 2026 and will have moved. The order is a rule on CISA's dates and EPSS, not a verdict on your estate: check what you run first.
- The bottom line, how the week connects, the first hour, who can skip it and the message are our interpretation of the records, not a statement by CISA or the vendors.

Appendix 1. Timeline

Date	Event
21 November 2026	Vanderbilt University Research Electronic Data Capture (REDCap), CVE-2026-90817: CISA's deadline (added 18 November 2026).
21 November 2026	Synology DiskStation Manager (DSM), CVE-2024-10441: CISA's deadline (added 18 November 2026).
21 November 2026	Apache Axis, CVE-2026-90436: CISA's deadline (added 18 November 2026).
1 December 2026	Perforce Puppet Enterprise, CVE-2026-115731: CISA's deadline (added 17 November 2026).
2 December 2026	BerriAI LiteLLM, CVE-2026-40217: CISA's deadline (added 18 November 2026).

Appendix 2. Definition of done

- Every product on the list was checked against what you run.
- 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 compensating limit.
- Logs for the weeks before the update were searched for what you patched late.

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/