contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

18 November 2026 · 7 exploited CVEs added this week

Analysis Report

7 entries added to CISA's exploited list in the week to 18 November 2026. 5 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	18 November 2026
FACTS AS OF	18 November 2026	VERSION	1.0
ACT ON NOW	5 of 7	STATUS	Facts as at 18 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-2026-11-18

The bottom line

> *Start with REDCap, Apache Axis 1.x and Synology DSM or BeeStation: CISA's date for all three is 21 November 2026. Check Point Gaia and UnrealIRCd with linked servers are already past their 16 November 2026 date, so confirm those too. Puppet Enterprise and LiteLLM can follow.*

CISA added 7 vulnerabilities to its exploited list from 12 November 2026 to 18 November 2026. 5 have a deadline within three days or already past, 2 of them past.

Separately, 1685 new CVE records were published in the last 30 hours, 340 of them scored 8.5 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

- New: Vanderbilt University Research Electronic Data Capture (REDCap), CVE-2026-90817; Apache Axis, CVE-2026-90436; BerriAI LiteLLM, CVE-2026-40217; Synology DiskStation Manager (DSM), CVE-2024-10441.
- Left the seven-day window (31): 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.

Four entries are new since the watch of 17 November 2026: REDCap, Apache Axis, LiteLLM and Synology DSM (CVE-2026-90817, CVE-2026-90436, CVE-2026-40217, CVE-2024-10441). 31 entries left the week. No deadline has passed since that watch.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
Check Point Multiple Products (CVE-2026-123039)	Today	2 days past CISA's deadline	Not stated; see the note	0.02
UnrealIRCd (CVE-2026-114713)	Today	2 days past CISA's deadline	UnrealIRCd 6.2.7.1 (vendor release, 7 November 2026), or the vendor's hot-patch bundle-20261107 that needs no restart.	0.00

Vanderbilt University Research Electronic Data Capture (REDCap) (CVE-2026-90817)	Today	Due in 3 days	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 in 3 days	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 in 3 days	Not stated; see the note	0.01
Perforce Puppet Enterprise (CVE-2026-115731)	Next patch cycle	Due in 13 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 14 days	Not stated; see the note	0.17

How the week connects

REDCap and Puppet Enterprise share CWE-94, code generation. Axis, LiteLLM, Synology and Puppet also end with code running on the server, by different routes. Check Point needs a local login and UnrealIRCd needs linked servers. Otherwise the products are unrelated.

Do this today, in this order

- Check Point Multiple Products, CVE-2026-123039, 2 days past CISA's deadline. A logged-in local user can get root on Check Point Gaia through a world-writable socket. It matters most where a low-privilege or contractor login could be stolen. No fixed version is recorded.
- UnrealIRCd, CVE-2026-114713, 2 days past CISA's deadline. Any user on a network with two or more linked UnrealIRCd servers can inject server commands. It matters only if you run linked servers. The vendor calls it the critical one of nine issues fixed in 6.2.7.1.
- Vanderbilt University Research Electronic Data Capture (REDCap), CVE-2026-90817, due in 3 days. Code execution on a REDCap server with no login, through a route not meant for public surveys. The attacker needs a valid public survey hash. Anyone running REDCap 13.3.0 or later should look.
- Synology DiskStation Manager (DSM), CVE-2024-10441, due in 3 days. Remote code execution on Synology DSM and BeeStation OS with no login. How it is reached is not published. The vendor's advisory says there is no mitigation, so updating is the only listed fix.
- Apache Axis, CVE-2026-90436, due in 3 days. Code execution in Apache Axis 1.x with no login, through a crafted SOAP fault, if a suitable class is on the classpath. The record says it may be

end-of-life. No fixed version is recorded.

The first hour:

- List where REDCap, Apache Axis 1.x, Synology DSM or BeeStation and Check Point Gaia run, with their versions. Do this before anything else.
- Synology: update to the fixed DSM or BSM version. REDCap: upgrade to 16.0.49, 17.3.10 or 17.4.4. Both are due 21 November 2026.
- Axis 1.x: no fix is recorded, so cut off its network exposure. Check Point: apply the vendor's mitigations. UnrealIRCd with linked servers: upgrade to 6.2.7.1.
- Then Puppet Enterprise (upgrade, restart puppet server) and LiteLLM (find who holds a key and whether it is reachable from outside).

In the next patch cycle

- Perforce Puppet Enterprise, CVE-2026-115731, due in 13 days. Any holder of a certificate from the Puppet certificate authority can run code on the Puppet Server. Automatic signing can hand one to an outsider, so check how requests are signed as well as the version.
- BerriAI LiteLLM, CVE-2026-40217, due in 14 days. A logged-in LiteLLM proxy user can run code on the server through a guardrail test endpoint. The researchers' advisory says it runs as the LiteLLM process user, root in the default Docker image.

Who can skip most of this

You can skip most of this week if you run none of REDCap, Apache Axis, LiteLLM, Synology DSM or BeeStation, Puppet Enterprise, Check Point Gaia or UnrealIRCd. That says nothing about 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, could you confirm whether we run any of these: REDCap (CVE-2026-90817), Apache Axis (CVE-2026-90436), Synology DSM or BeeStation (CVE-2024-10441), Check Point Gaia (CVE-2026-123039), UnrealIRCd (CVE-2026-114713), Puppet Enterprise (CVE-2026-115731) or LiteLLM (CVE-2026-40217)? CISA's date is 21 November 2026 for the first three and 16 November 2026, already past, for the Check Point and UnrealIRCd entries. Please send us, in writing by Friday, each version in use and the fix or mitigation applied, or the date it will be.*

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 >= "2026-11-12" and .dateAdded <= "2026-11-
18")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 18 November 2026 it printed 7 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-2026-123039,CVE-2026-114713,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-2026-123039 --cve CVE-2026-114713 --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 18 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
16 November 2026	Check Point Multiple Products, CVE-2026-123039: CISA's deadline (added 13 November 2026).
16 November 2026	UnrealIRCd, CVE-2026-114713: CISA's deadline (added 13 November 2026).
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/