contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

19 November 2026 · 7 exploited CVEs added this week

Analysis Report

7 entries added to CISA's exploited list in the week to 19 November 2026. 5 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	19 November 2026
FACTS AS OF	19 November 2026	VERSION	1.0
ACT ON NOW	5 of 7	STATUS	Facts as at 19 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-2026-11-19

The bottom line

> *Check Point (CVE-2026-123039) and UnrealIRCd (CVE-2026-114713) are past CISA's date of 16 November 2026, so confirm those first. REDCap, Apache Axis and Synology DSM are due 21 November 2026. Puppet Enterprise (1 December 2026) and LiteLLM (2 December 2026) come after.*

CISA added 7 vulnerabilities to its exploited list from 13 November 2026 to 19 November 2026. 5 have a deadline within three days or already past, 2 of them past.

Separately, 918 new CVE records were published in the last 30 hours, 273 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 (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.

No new entries since the watch of 18 November 2026. Many items left the week's list, and no CISA deadline has passed since that watch.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
Check Point Multiple Products (CVE-2026-123039)	Today	3 days past CISA's deadline	Not stated; see the note	0.02
UnrealIRCd (CVE-2026-114713)	Today	3 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 2 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 2 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 2 days	Not stated; see the note	0.01
Perforce Puppet Enterprise (CVE-2026-115731)	Next patch cycle	Due in 12 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 13 days	Not stated; see the note	0.17

How the week connects

The products are unrelated, so there is no single story. Several records describe code running on the server, and REDCap and Puppet share the weakness CWE-94. Some need a foothold first: a login (LiteLLM), a certificate (Puppet) or a local account (Check Point).

Do this today, in this order

- Check Point Multiple Products, CVE-2026-123039, 3 days past CISA's deadline. The record says a root service on Gaia OS accepts commands from any local user without checking who they are. An attacker needs a login first. Matters to owners of the listed Check Point products.
- UnrealIRCd, CVE-2026-114713, 3 days past CISA's deadline. The record says any user on a network with two or more linked servers can inject server-to-server commands that run with server authority. Matters to UnrealIRCd networks with linked servers.
- Vanderbilt University Research Electronic Data Capture (REDCap), CVE-2026-90817, due in 2 days. The record says an unauthenticated attacker can run code on a REDCap server using crafted requests from a public survey. They need a valid survey hash. Matters to anyone hosting REDCap.
- Synology DiskStation Manager (DSM), CVE-2024-10441, due in 2 days. The record says a flaw in the system plugin daemon lets a remote attacker run code on a Synology DSM or BeeStation device. How it is reached is not published. Updating is the only fix the vendor lists.
- Apache Axis, CVE-2026-90436, due in 2 days. The record says a crafted SOAP fault makes Axis load a class the attacker names, giving code execution with no login. It also says the product may be end-of-life, so no patch may come.

The first hour:

- List where you run Check Point gateways or management servers, and UnrealIRCd with linked servers. CISA's date of 16 November 2026 has passed for both.
- Check Point: read the Jumbo Hotfix Take on each system and apply the vendor's mitigations. We found no fixed version recorded.
- UnrealIRCd: upgrade to 6.2.7.1, or apply the vendor's hot-patch bundle-20261107, which needs no restart.
- REDCap, Synology and Axis: read each version and update to the fixed ones above. Axis has no recorded fix, so cut off its network exposure.

In the next patch cycle

- Perforce Puppet Enterprise, CVE-2026-115731, due in 12 days. Any holder of a certificate signed by the Puppet certificate authority can run code on the Puppet Server. The record says automatic signing can hand one to an outsider.
- BerriAI LiteLLM, CVE-2026-40217, due in 13 days. A user who is already logged in to the LiteLLM proxy can send code to a guardrail test endpoint and run it on the server. The researchers' advisory says that is root in the default Docker image.

Who can skip most of this

If you run none of REDCap, Apache Axis, LiteLLM, Synology DSM or BeeStation, Puppet Enterprise, the listed Check Point products or linked UnrealIRCd servers, you can skip most of this week. Other flaws still apply to you.

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, CISA has listed several flaws as exploited. Please tell us which of these we run: Check Point (CVE-2026-123039), UnrealIRCd (CVE-2026-114713), REDCap (CVE-2026-90817), Apache Axis (CVE-2026-90436), Synology DSM or BeeStation (CVE-2024-10441), Puppet Enterprise (CVE-2026-115731) and LiteLLM (CVE-2026-40217). The first two are past CISA's date of 16 November 2026, and three more are due 21 November 2026. Please confirm in writing, for each one, the installed version and whether the fix or mitigation is applied, by the end of tomorrow. Where no fix exists, please tell us how it is shielded from the network. 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 >= "2026-11-13" and .dateAdded <= "2026-11-19")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 19 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 19 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/