contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

# Daily threat watch

**17 November 2026 · 3 exploited CVEs added this week**

## Analysis Report

3 entries added to CISA's exploited list in the week to 17 November 2026. 2 with a deadline inside three days, in the order to work them.

| | | | |
|---|---|---|---|
| PREPARED BY | NamiQ | DATE | 17 November 2026 |
| FACTS AS OF | 17 November 2026 | VERSION | 1.0 |
| ACT ON NOW | 2 of 3 | STATUS | Facts as at 17 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-2026-11-17

## The bottom line

> *If you run Check Point firewalls or management servers, or UnrealIRCd with linked servers, check them first: CISA's date of 16 November 2026 has passed for both. Puppet Enterprise users have until 1 December 2026 but should confirm their version now.*

CISA added 3 vulnerabilities to its exploited list from 12 November 2026 to 17 November 2026. 2 have a deadline within three days or already past, 2 of them past.

Separately, 1380 new CVE records were published in the last 30 hours, 225 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: Perforce Puppet Enterprise, CVE-2026-115731.
- Deadline passed since: Check Point Multiple Products, CVE-2026-123039; UnrealIRCd, CVE-2026-114713.
- 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.

One entry is new since the watch of 16 November 2026: CVE-2026-115731 (Puppet Enterprise). 31 entries dropped out of the week. The CISA dates passed for CVE-2026-123039 and CVE-2026-114713.

## At a glance

| Entry | Act | CISA date | Fixed in | EPSS |
|---|---|---|---|---|
| Check Point Multiple Products (CVE-2026-123039) | Today | 1 day past CISA's deadline | Not stated; see the note | 0.02 |
| UnrealIRCd (CVE-2026-114713) | Today | 1 day 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 |

| | | | | |
|---|---|---|---|---|
| Perforce Puppet Enterprise (CVE-2026-115731) | Next patch cycle | Due in 14 days | Puppet Enterprise 2023.8.13, 2025.12.1 or 2026.0.1, bundling puppet-agent 8.22.2 or 9.1.3. The record says to restart puppet server afterwards. | 0.00 |

## How the week connects

These three have little in common: different products and different weakness types. Each needs the attacker to hold some access first: a CA-signed certificate, a local account on the device, or a chat account on a linked IRC network. Puppet and Check Point both give control of a central system.

## Do this today, in this order

- Check Point Multiple Products, CVE-2026-123039, 1 day past CISA's deadline. Check Point Gaia OS: a logged-in local user can send a command to a root-owned socket and run it as root. Matters to anyone running the listed Check Point firewall or management products.
- UnrealIRCd, CVE-2026-114713, 1 day past CISA's deadline. UnrealIRCd: any user on a network with two or more linked servers can inject server commands that run with server authority. Matters only to those who run linked IRC servers.

The first hour:

- Ask who runs Check Point firewalls or management servers, and note their Jumbo Hotfix levels for CVE-2026-123039. No fixed version is stated in what we read.
- Find any UnrealIRCd server. If two or more are linked, apply the hot-patch or move to 6.2.7.1.
- Find any Puppet Enterprise server and its version. Plan the move to a fixed release and restart puppet server afterwards.
- Review how the Puppet certificate authority signs requests. Automatic signing without strong checks lets an outsider obtain a certificate.

## In the next patch cycle

- Perforce Puppet Enterprise, CVE-2026-115731, due in 14 days. Puppet Enterprise: a client with any CA-signed certificate can run its own code on the Puppet Server. Whoever runs Puppet Server should check the version and how certificates get signed.

## Who can skip most of this

If you run no Check Point gear, no UnrealIRCd and no Puppet Enterprise, you can skip most of this week. That says nothing about other flaws in the products you do run.

## 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, please confirm in writing whether we run any of these: Check Point firewall or management products (CVE-2026-123039), UnrealIRCd (CVE-2026-114713) or Puppet Enterprise (CVE-2026-115731). CISA's dates for the first two, 16 November 2026, have passed. The Puppet date is 1 December 2026. For each one we run, please send the exact version, whether the fix is applied, and the date it was applied. Please reply by the end of this week. 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 >= "2026-11-12" and .dateAdded <= "2026-11-
17")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 17 November 2026 it printed 3 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-2026-115731
```

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-2026-115731
```

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 17 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). |
| 1 December 2026 | Perforce Puppet Enterprise, CVE-2026-115731: CISA's deadline (added 17 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/