contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

16 November 2026 · 2 exploited CVEs added this week

Analysis Report

2 entries added to CISA's exploited list in the week to 16 November 2026. 2 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	16 November 2026
FACTS AS OF	16 November 2026	VERSION	1.0
ACT ON NOW	2 of 2	STATUS	Facts as at 16 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-2026-11-16

The bottom line

> *Both items are due with CISA today, 16 November 2026. If you run UnrealIRCd, upgrade to 6.2.7.1 or apply the vendor's hot-patch. If you run Check Point firewall or management products, confirm your versions now: no fixed version is stated.*

CISA added 2 vulnerabilities to its exploited list from 11 November 2026 to 16 November 2026. 2 have a deadline within three days or already past.

Separately, 389 new CVE records were published in the last 30 hours, 66 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

- 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 15 November 2026. Earlier entries have left the week's list, and no deadline has passed since then. Both items shown now are due today.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
Check Point Multiple Products (CVE-2026-123039)	Today	Due today	Not stated; see the note	0.02
UnrealIRCd (CVE-2026-114713)	Today	Due today	UnrealIRCd 6.2.7.1 (released 7 November 2026); or the vendor's hot-patch bundle, which the vendor says fixes it without a restart.	0.01

How the week connects

The two items have little in common: different products and different weaknesses. Both let a user who already has access gain more authority than intended: root on the Check Point device, server

authority on UnrealIRCd. Nothing in the record links them.

Do this today, in this order

- Check Point Multiple Products, CVE-2026-123039, due today. The record says a logged-in local user on a Check Point Gaia OS device can send a command to a world-writable socket and have it run as root. Matters to anyone running the listed Check Point products.
- UnrealIRCd, CVE-2026-114713, due today. The record says any user on a network with two or more linked UnrealIRCd servers can inject server-to-server commands that run with server authority. Matters to IRC server operators.

The first hour:

- Find out whether you run UnrealIRCd and which version. If it is below 6.2.7.1, upgrade or apply the vendor's hot-patch.
- Find out whether you run Check Point Firewall, Security Gateway or Security Management products, and write down each version.
- For Check Point, ask the vendor or your provider for the fixed version. The sources we read do not state one.
- Until Check Point is confirmed fixed, limit who holds local accounts on those devices.

Who can skip most of this

If you run neither UnrealIRCd nor any Check Point product, you can skip this week's two items. That says nothing about other flaws in what 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, two flaws on CISA's exploited list are due today, 16 November 2026. Please confirm whether we run UnrealIRCd (CVE-2026-114713) or Check Point firewall, gateway or management products (CVE-2026-123039). For UnrealIRCd, please confirm our version is 6.2.7.1 or later, or that the vendor's hot-patch is applied. For Check Point, please tell us the installed versions and which fix applies. Please send written confirmation of each version and fix by the end of tomorrow. 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 >= "2026-11-11" and .dateAdded <= "2026-11-16")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 16 November 2026 it printed 2 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
```

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
```

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 16 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).

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/