contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

24 November 2026 · 9 exploited CVEs added this week

Analysis Report

9 entries added to CISA's exploited list in the week to 24 November 2026. 9 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	24 November 2026
FACTS AS OF	24 November 2026	VERSION	1.0
ACT ON NOW	9 of 9	STATUS	Facts as at 24 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-2026-11-24

The bottom line

> *CISA added 9 vulnerabilities to its exploited list from 19 November 2026 to 24 November 2026. 9 have a deadline within three days or already past, 4 of them past. Read the exploited list first. It is the work list. Everything else is a reading list.*

Separately, 978 new CVE records were published in the last 30 hours, 207 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

- New: Optimizely Web Experimentation, CVE-2026-132224; Drupal Core, CVE-2026-132165; Idunno AntiCsrf, CVE-2026-131914; N-able MailAssure, CVE-2026-134624; Project MONAI MONAI Label, CVE-2026-133968; Cisco Expressway Series, CVE-2026-76466; Apache Roller, CVE-2026-129448; Broadcom VMware vCenter, CVE-2026-123890; SAP NetWeaver, CVE-2025-42884.
- Deadline passed since: Cisco Expressway Series, CVE-2026-76466; Apache Roller, CVE-2026-129448; Broadcom VMware vCenter, CVE-2026-123890; SAP NetWeaver, CVE-2025-42884.
- Left the seven-day window (38): CVE-2026-90817, CVE-2024-10441, CVE-2026-90436, CVE-2026-115731, CVE-2026-40217, 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.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
Apache Roller (CVE-2026-129448)	Today	1 day past CISA's deadline	Apache Roller 6.1.6, which the record says disables extension types and rejects XML-RPC requests when the XML-RPC feature is off.	0.40
Broadcom VMware vCenter (CVE-2026-123890)	Today	1 day past CISA's deadline	Not stated; see the note	0.04

Cisco Expressway Series (CVE-2026-76466)	Today	1 day past CISA's deadline	X15.5.20 for devices on X15.5.3 or earlier. The advisory states that devices on X14 or earlier must migrate to a fixed release and does not name the migration target.	0.02
SAP NetWeaver (CVE-2025-42884)	Today	1 day past CISA's deadline	No specific patched version number is named in the sources. The vendor's advisory lists SAP Security Note 3660969 as the correction for EP-BASIS 7.50 and EP-RUNTIME 7.50.	0.01
Project MONAI MONAI Label (CVE-2026-133968)	Today	Due in 2 days	Not stated; see the note	0.50
N-able MailAssure (CVE-2026-134624)	Today	Due in 2 days	Build 20261121.1943, as named in the CVE record. No vendor advisory page was available; this figure comes from the record alone.	0.01
Idunno AntiCsrf (CVE-2026-131914)	Today	Due in 3 days	Not stated; see the note	0.01
Optimizely Web Experimentation (CVE-2026-132224)	Today	Due in 3 days	Optimizely closed the vulnerability server-side on 16 November 2026. The CVE record lists all versions before 17 November 2026 as affected. No customer-side patch is needed.	0.00
Drupal Core (CVE-2026-132165)	Today	Due in 3 days	Not stated; see the note	n/a

Do this today, in this order

- Apache Roller, CVE-2026-129448, 1 day past CISA's deadline.
- Broadcom VMware vCenter, CVE-2026-123890, 1 day past CISA's deadline.
- Cisco Expressway Series, CVE-2026-76466, 1 day past CISA's deadline.
- SAP NetWeaver, CVE-2025-42884, 1 day past CISA's deadline.
- Project MONAI MONAI Label, CVE-2026-133968, due in 2 days.
- N-able MailAssure, CVE-2026-134624, due in 2 days.
- Idunno AntiCsrf, CVE-2026-131914, due in 3 days.
- Optimizely Web Experimentation, CVE-2026-132224, due in 3 days.
- Drupal Core, CVE-2026-132165, due in 3 days.

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 >= "2026-11-19" and .dateAdded <= "2026-11-
24")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 24 November 2026 it printed 9 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-2026-129448,CVE-2026-123890,CVE-2026-76466,CVE-2025-
42884,CVE-2026-133968,CVE-2026-134624,CVE-2026-131914,CVE-2026-132224
```

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-2026-129448 --cve CVE-2026-123890 --cve CVE-2026-76466 --cve CVE-2025-
42884 --cve CVE-2026-133968 --cve CVE-2026-134624 --cve CVE-2026-131914 --cve CVE-2026-132224
```

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 24 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.

Appendix 1. Timeline

Date	Event
23 November 2026	Apache Roller, CVE-2026-129448: CISA's deadline (added 20 November 2026).
23 November 2026	Broadcom VMware vCenter, CVE-2026-123890: CISA's deadline (added 20 November 2026).
23 November 2026	Cisco Expressway Series, CVE-2026-76466: CISA's deadline (added 20 November 2026).
23 November 2026	SAP NetWeaver, CVE-2025-42884: CISA's deadline (added 20 November 2026).
26 November 2026	Project MONAI MONAI Label, CVE-2026-133968: CISA's deadline (added 23 November 2026).
26 November 2026	N-able MailAssure, CVE-2026-134624: CISA's deadline (added 23 November 2026).
27 November 2026	Idunno AntiCsrf, CVE-2026-131914: CISA's deadline (added 24 November 2026).
27 November 2026	Optimizely Web Experimentation, CVE-2026-132224: CISA's deadline (added 24 November 2026).
27 November 2026	Drupal Core, CVE-2026-132165: CISA's deadline (added 24 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/