contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

25 November 2026 · 19 exploited CVEs added this week

Analysis Report

19 entries added to CISA's exploited list in the week to 25 November 2026. 17 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	25 November 2026
FACTS AS OF	25 November 2026	VERSION	1.0
ACT ON NOW	17 of 19	STATUS	Facts as at 25 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-2026-11-25

The bottom line

> *CISA added 19 vulnerabilities to its exploited list from 20 November 2026 to 25 November 2026. 17 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, 899 new CVE records were published in the last 30 hours, 171 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: Vates Xen Orchestra, CVE-2026-133469; Mitel MiCollab, CVE-2026-133324; Mitel MiCollab, CVE-2026-133323; Mitel MiCollab, CVE-2026-133311; Mitel MiCollab, CVE-2026-133303; Mitel MiCollab, CVE-2026-133275; Hewlett Packard Enterprise (HPE) Juniper Session Smart Conductor and Session Smart Router, CVE-2026-103406; Danfoss AK-SM 800A Series, CVE-2025-41450; Danfoss AK-SM 800A Series, CVE-2023-25915; Danfoss AK-SM 800A Series, CVE-2023-25914.
- Left the seven-day window (39): 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, CVE-2026-82384.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
Apache Roller (CVE-2026-129448)	Today	2 days past CISA's deadline	Apache Roller 6.1.6 or later, as stated in the record.	0.24
Broadcom VMware vCenter (CVE-2026-123890)	Today	2 days past CISA's deadline	vCenter 9.1.1.0200, 9.0.2.0200, 8.0 U3m; Cloud Foundation 5.2.5. The vendor's advisory lists vCenter 7.0 as affected too (contact Broadcom Support); the CVE record does not include 7.0.	0.05

Cisco Expressway Series (CVE-2026-76466)	Today	2 days past CISA's deadline	X15.5.20 for releases X15.5.3 and earlier. X14 and earlier have no direct fix; the vendor's advisory says those customers must migrate to a fixed release.	0.01
SAP NetWeaver (CVE-2025-42884)	Today	2 days 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 tomorrow	0.8.6, released 22 November 2026. The release notes name both a pip package and a Docker image at that version.	0.27
N-able MailAssure (CVE-2026-134624)	Today	Due tomorrow	The record names all builds before 20261121.1943 as affected; 20261121.1943 is the first unaffected build. No vendor advisory page was available to confirm further detail.	0.02
Idunno AntiCsrf (CVE-2026-131914)	Today	Due in 2 days	Not stated; see the note	0.04
Optimizely Web Experimentation (CVE-2026-132224)	Today	Due in 2 days	Optimizely closed the vulnerability on 16 November 2026, the same day as the incident. The record states all versions before 17 November 2026 were affected; no customer installation is needed.	0.01
Drupal Core (CVE-2026-132165)	Today	Due in 2 days	Drupal 10.6.22, 11.3.22, 11.4.13 (advisory SA-CORE-2026-017, 18 November 2026)	n/a
Mitel MiCollab (CVE-2026-133323)	Today	Due in 3 days	Vendor patch for MiCollab 10.3 (10.3.0.18); the advisory instructs upgrading to that release and applying the patch. The source text is truncated before the full steps; no higher version number is named.	0.03
Danfoss AK-SM 800A Series (CVE-2023-25915)	Today	Due in 3 days	The CVE record lists AK-SM800A versions before 3.3 as affected; 3.3 is the implied boundary. No vendor advisory was readable to confirm it as the fixed release.	0.01

Vates Xen Orchestra (CVE-2026-133469)	Today	Due in 3 days	xen-orchestra 6.9.2 (stable channel) and 6.10.1 (latest channel); xo-server 5.211.2 and 5.213.1. The vendor's advisory confirms fixes are released to both channels.	0.01
Danfoss AK-SM 800A Series (CVE-2023-25914)	Today	Due in 3 days	The record lists affected versions as below 3.3 for AK-SM800A, placing 3.3 as the boundary. No vendor advisory was readable to confirm which release carries the fix.	0.01
Hewlett Packard Enterprise (HPE) Juniper Session Smart Conductor and Session Smart Router (CVE-2026-103406)	Today	Due in 3 days	Session Smart Conductor 7.0.5, 7.1.7, and 7.2.3, per the record published 28 October 2026.	0.01
Mitel MiCollab (CVE-2026-133303)	Today	Due in 3 days	The vendor's advisory (MISA-2026-0012) states a patch is available for release 10.3. The advisory text does not name a specific patched sub-version number.	0.01
Mitel MiCollab (CVE-2026-133324)	Today	Due in 3 days	The vendor's advisory says: apply Mitel's patch to release 10.3 (10.3.0.18) following KB000129195, or upgrade to a later release. No specific later version number is named in the advisory.	0.00
Mitel MiCollab (CVE-2026-133275)	Today	Due in 3 days	The vendor's advisory states a patch is available for MiCollab release 10.3; the specific patch version number is not given in the advisory text available.	0.00
Danfoss AK-SM 800A Series (CVE-2025-41450)	Next patch cycle	Due in 14 days	Firmware version 4.2. The CVE record states all versions prior to 4.2 are affected; 4.2 is the first version the record identifies as outside the affected range.	0.01
Mitel MiCollab (CVE-2026-133311)	Next patch cycle	Due in 14 days	The vendor's advisory says: apply the patch provided for release 10.3 (10.3.0.18), or upgrade to a later release.	0.00

Do this today, in this order

- Apache Roller, CVE-2026-129448, 2 days past CISA's deadline.
- Broadcom VMware vCenter, CVE-2026-123890, 2 days past CISA's deadline.
- Cisco Expressway Series, CVE-2026-76466, 2 days past CISA's deadline.

- SAP NetWeaver, CVE-2025-42884, 2 days past CISA's deadline.
- Project MONAI MONAI Label, CVE-2026-133968, due tomorrow.
- N-able MailAssure, CVE-2026-134624, due tomorrow.
- Idunno AntiCsrf, CVE-2026-131914, due in 2 days.
- Optimizely Web Experimentation, CVE-2026-132224, due in 2 days.
- Drupal Core, CVE-2026-132165, due in 2 days.
- Mitel MiCollab, CVE-2026-133323, due in 3 days.
- Danfoss AK-SM 800A Series, CVE-2023-25915, due in 3 days.
- Vates Xen Orchestra, CVE-2026-133469, due in 3 days.
- Danfoss AK-SM 800A Series, CVE-2023-25914, due in 3 days.
- Hewlett Packard Enterprise (HPE) Juniper Session Smart Conductor and Session Smart Router, CVE-2026-103406, due in 3 days.
- Mitel MiCollab, CVE-2026-133303, due in 3 days.
- Mitel MiCollab, CVE-2026-133324, due in 3 days.
- Mitel MiCollab, CVE-2026-133275, due in 3 days.

In the next patch cycle

- Danfoss AK-SM 800A Series, CVE-2025-41450, due in 14 days.
- Mitel MiCollab, CVE-2026-133311, due in 14 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 >= "2026-11-20" and .dateAdded <= "2026-11-25")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 25 November 2026 it printed 19 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 25 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).
28 November 2026	Mitel MiCollab, CVE-2026-133323: CISA's deadline (added 25 November 2026).
28 November 2026	Danfoss AK-SM 800A Series, CVE-2023-25915: CISA's deadline (added 25 November 2026).
28 November 2026	Vates Xen Orchestra, CVE-2026-133469: CISA's deadline (added 25 November 2026).
28 November 2026	Danfoss AK-SM 800A Series, CVE-2023-25914: CISA's deadline (added 25 November 2026).
28 November 2026	Hewlett Packard Enterprise (HPE) Juniper Session Smart Conductor and Session Smart Router, CVE-2026-103406: CISA's deadline (added 25 November 2026).
28 November 2026	Mitel MiCollab, CVE-2026-133303: CISA's deadline (added 25 November 2026).
28 November 2026	Mitel MiCollab, CVE-2026-133324: CISA's deadline (added 25 November 2026).
28 November 2026	Mitel MiCollab, CVE-2026-133275: CISA's deadline (added 25 November 2026).
9 December 2026	Danfoss AK-SM 800A Series, CVE-2025-41450: CISA's deadline (added 25 November 2026).
9 December 2026	Mitel MiCollab, CVE-2026-133311: CISA's deadline (added 25 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/