contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

27 November 2026 · 18 exploited CVEs added this week

Analysis Report

18 entries added to CISA's exploited list in the week to 27 November 2026. 16 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	27 November 2026
FACTS AS OF	27 November 2026	VERSION	1.0
ACT ON NOW	16 of 18	STATUS	Facts as at 27 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-2026-11-27

The bottom line

> *CISA added 18 vulnerabilities to its exploited list from 21 November 2026 to 27 November 2026. 16 have a deadline within three days or already past, 2 of them past. Read the exploited list first. It is the work list. Everything else is a reading list.*

Separately, 663 new CVE records were published in the last 30 hours, 152 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: Drupal Core, CVE-2026-136716; OSGeo GeoServer, CVE-2026-129243; OSGeo GeoServer, CVE-2026-120705.
- Deadline passed since: N-able MailAssure, CVE-2026-134624; Project MONAI MONAI Label, CVE-2026-133968.
- Left the seven-day window (43): CVE-2026-129448, CVE-2026-123890, CVE-2026-76466, CVE-2025-42884, 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
Project MONAI MONAI Label (CVE-2026-133968)	Today	1 day past CISA's deadline	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	1 day past CISA's deadline	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

Drupal Core (CVE-2026-132165)	Today	Due today	Drupal 10.6.22, 11.3.22, 11.4.13 per vendor advisory SA-CORE-2026-017 (18 November 2026). Drupal 8, 9, 10.5.x and below, and 11.2.x and below are end-of-life; no patch is available for them.	0.08
Idunno AntiCsrf (CVE-2026-131914)	Today	Due today	Not stated; see the note	0.04
Optimizely Web Experimentation (CVE-2026-132224)	Today	Due today	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
Vates Xen Orchestra (CVE-2026-133469)	Today	Due tomorrow	xen-orchestra 6.9.2 (stable) and 6.10.1 (latest); xo-server 5.211.2 and 5.213.1. The record states these versions are fixed.	0.32
Mitel MiCollab (CVE-2026-133323)	Today	Due tomorrow	Vendor advisory MISA-2026-0012 states a patch is available for MiCollab 10.3 (10.3.0.18). The advisory does not name a later release number; contact Mitel for the exact patch identifier.	0.06
Danfoss AK-SM 800A Series (CVE-2023-25915)	Today	Due tomorrow	The record's affected range ends below version 3.3, making 3.3 the first version not listed as affected. No vendor advisory could be read to confirm an explicit fix release.	0.02
Danfoss AK-SM 800A Series (CVE-2023-25914)	Today	Due tomorrow	The record lists affected versions as those below 3.3. No vendor advisory was available; no source explicitly names the fixed release.	0.02
Hewlett Packard Enterprise (HPE) Juniper Session Smart Conductor and Session Smart Router (CVE-2026-103406)	Today	Due tomorrow	Session Smart Conductor 7.0.5, 7.1.7, and 7.2.3 and all subsequent releases, per the record published 28 October 2026. No vendor advisory page was available to confirm further detail.	0.02
Mitel MiCollab (CVE-2026-133303)	Today	Due tomorrow	The vendor's advisory says a patch is available for release 10.3. The exact patched build number is not in the available source text; contact Mitel or your reseller for the specific package.	0.01

Mitel MiCollab (CVE-2026-133324)	Today	Due tomorrow	The vendor's advisory says: apply the provided patch for version 10.3 (10.3.0.18), or upgrade to a later release. No specific later version number is named in the advisory.	0.01
Mitel MiCollab (CVE-2026-133275)	Today	Due tomorrow	The vendor's advisory (MISA-2026-0012) states a patch is available for release 10.3; the advisory text available does not give the exact patched build number.	0.01
Drupal Core (CVE-2026-136716)	Today	Due in 3 days	Drupal 10.6.23; Drupal 11.3.23; Drupal 11.4.14 (vendor advisory, 25 November 2026). The advisory also requires running update.php after upgrading.	0.01
OSGeo GeoServer (CVE-2026-120705)	Today	Due in 3 days	The vendor's November 2026 advisory announces GeoServer 3.0.2, 2.28.6, and 2.27.7 as current releases; it does not explicitly state which release first fixed this CVE.	n/a
OSGeo GeoServer (CVE-2026-129243)	Today	Due in 3 days	GeoServer 3.0.2, 2.28.6, and 2.27.7, as listed in the vendor's advisory release announcements.	n/a
Danfoss AK-SM 800A Series (CVE-2025-41450)	Next patch cycle	Due in 12 days	Version 4.2 of the AK-SM 8xxA Series. The record, published by Danfoss on 8 May 2025, states all versions before 4.2 are affected; 4.2 is the first version outside that range.	0.04
Mitel MiCollab (CVE-2026-133311)	Next patch cycle	Due in 12 days	The vendor's advisory says a patch is available for MiCollab release 10.3 (10.3.0.18); apply it, or upgrade to a later release. No specific later version number is named in the advisory.	0.01

Do this today, in this order

- Project MONAI MONAI Label, CVE-2026-133968, 1 day past CISA's deadline.
- N-able MailAssure, CVE-2026-134624, 1 day past CISA's deadline.
- Drupal Core, CVE-2026-132165, due today.
- Idunno AntiCsrf, CVE-2026-131914, due today.
- Optimizely Web Experimentation, CVE-2026-132224, due today.
- Vates Xen Orchestra, CVE-2026-133469, due tomorrow.

- Mitel MiCollab, CVE-2026-133323, due tomorrow.
- Danfoss AK-SM 800A Series, CVE-2023-25915, due tomorrow.
- Danfoss AK-SM 800A Series, CVE-2023-25914, due tomorrow.
- Hewlett Packard Enterprise (HPE) Juniper Session Smart Conductor and Session Smart Router, CVE-2026-103406, due tomorrow.
- Mitel MiCollab, CVE-2026-133303, due tomorrow.
- Mitel MiCollab, CVE-2026-133324, due tomorrow.
- Mitel MiCollab, CVE-2026-133275, due tomorrow.
- Drupal Core, CVE-2026-136716, due in 3 days.
- OSGeo GeoServer, CVE-2026-120705, due in 3 days.
- OSGeo GeoServer, CVE-2026-129243, due in 3 days.

In the next patch cycle

- Danfoss AK-SM 800A Series, CVE-2025-41450, due in 12 days.
- Mitel MiCollab, CVE-2026-133311, due in 12 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 >= "2026-11-21" and .dateAdded <= "2026-11-27")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 27 November 2026 it printed 18 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-2026-133968,CVE-2026-134624,CVE-2026-132165,CVE-2026-131914,CVE-2026-132224,CVE-2026-133469,CVE-2026-133323,CVE-2023-25915
```

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-2026-133968 --cve CVE-2026-134624 --cve CVE-2026-132165 --cve CVE-2026-131914 --cve CVE-2026-132224 --cve CVE-2026-133469 --cve CVE-2026-133323 --cve CVE-2023-25915
```

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 27 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
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	Drupal Core, CVE-2026-132165: CISA's deadline (added 24 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).
28 November 2026	Vates Xen Orchestra, CVE-2026-133469: CISA's deadline (added 25 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	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).
30 November 2026	Drupal Core, CVE-2026-136716: CISA's deadline (added 27 November 2026).
30 November 2026	OSGeo GeoServer, CVE-2026-120705: CISA's deadline (added 27 November 2026).
30 November 2026	OSGeo GeoServer, CVE-2026-129243: CISA's deadline (added 27 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/