contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

4 November 2026 · 5 exploited CVEs added this week

Analysis Report

5 entries added to CISA's exploited list in the week to 4 November 2026. 4 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	4 November 2026
FACTS AS OF	4 November 2026	VERSION	1.0
ACT ON NOW	4 of 5	STATUS	Facts as at 4 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-2026-11-04

The bottom line

> *Update every WordPress site to 7.1.4 today — the CISA deadline is 6 November 2026, two days away. Three other deadlines (Ivanti CVE-2026-111357, GitLab CVE-2026-97229, and Cisco CVE-2026-76418) have already passed; confirm whether you run those products now.*

CISA added 5 vulnerabilities to its exploited list from 29 October 2026 to 4 November 2026. 4 have a deadline within three days or already past, 3 of them past.

Separately, 910 new CVE records were published in the last 30 hours, 115 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: CVE-2026-46300, CVE-2026-41709, CVE-2026-111497, CVE-2026-48356, CVE-2026-109618, CVE-2026-109619, CVE-2026-104935, CVE-2026-104935, CVE-2026-104935, CVE-2026-104935, CVE-2026-109618, CVE-2026-109619, CVE-2026-109618, CVE-2026-109619, CVE-2026-59309, CVE-2026-59310, CVE-2026-47876, CVE-2026-59309, CVE-2026-59310, CVE-2026-47876, CVE-2026-41703, CVE-2026-109619, CVE-2026-109618, CVE-2026-104935, CVE-2026-104935, CVE-2026-104935, CVE-2026-104935, CVE-2026-109618, CVE-2026-109619, CVE-2026-109618, CVE-2026-109619, CVE-2026-59309, CVE-2026-59310, CVE-2026-47876, CVE-2026-59309, CVE-2026-59310, CVE-2026-47876, CVE-2026-41703, CVE-2026-48356, CVE-2026-48356, CVE-2026-111497, CVE-2026-111497, CVE-2026-104935, CVE-2026-104935, CVE-2026-104935, CVE-2026-104935, CVE-2026-46300, CVE-2026-109618, CVE-2026-109619, CVE-2026-46300, CVE-2026-109618, CVE-2026-109619, CVE-2026-41709, CVE-2026-41709, CVE-2026-59309, CVE-2026-59310, CVE-2026-47876, CVE-2026-59309, CVE-2026-59310, CVE-2026-47876, CVE-2026-41703, CVE-2026-41709, CVE-2026-104935, CVE-2026-104935, CVE-2026-104935, CVE-2026-104935, CVE-2026-104935.

No new entries were added since 3 November 2026. Several CVEs left the week's watch. No deadlines passed during that period.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
GitLab Community Edition and Enterprise Edition (CVE-2026-97229)	Today	3 days past CISA's deadline	GitLab CE/EE 19.2.8, 19.3.5, 19.4.2	0.28

Cisco Secure Firewall ASA Software and Cisco Secure FTD Software (CVE-2026-76418)	Today	3 days past CISA's deadline	Not stated; see the note	0.01
Ivanti Connect Secure (CVE-2026-111357)	Today	2 days past CISA's deadline	Not stated; see the note	0.01
WordPress Core (CVE-2026-119977)	Today	Due in 2 days	WordPress 7.1.4	0.01
Ivanti Connect Secure (CVE-2026-118527)	Next patch cycle	Due in 9 days	25.1.1.3 (25.x branch) and 22.8R2.6 (22.x branch), per the record published 3 November 2026; these are named as the first unaffected versions.	n/a

How the week connects

The two Ivanti Connect Secure items are explicitly linked: the record names CVE-2026-118527 and CVE-2026-111357 as chainable with each other and with CVE-2026-104935. The remaining three items — WordPress, GitLab, and Cisco ASA/FTD — affect unrelated products with different weakness classes and share no stated connection with each other or with the Ivanti items.

Do this today, in this order

- GitLab Community Edition and Enterprise Edition, CVE-2026-97229, 3 days past CISA's deadline. GitLab CE/EE allows an unauthenticated attacker to run code on the server by sending a crafted regular expression via the CI/CD configuration. The CVSS score is 10.
- Cisco Secure Firewall ASA Software and Cisco Secure FTD Software, CVE-2026-76418, 3 days past CISA's deadline. Cisco Secure Firewall ASA and FTD software can be forced to reload by an unauthenticated attacker when secondary authentication is configured on a tunnel group, cutting all traffic.
- Ivanti Connect Secure, CVE-2026-111357, 2 days past CISA's deadline. A local authenticated attacker on Ivanti Connect Secure can escalate privileges. The record says this was used as the final step in a chain with CVE-2026-104935 and CVE-2026-118527.
- WordPress Core, CVE-2026-119977, due in 2 days. WordPress Core (versions 4.7 through 7.1.3) is affected. An unauthenticated attacker can execute code on the server during a core upgrade by targeting predictable, web-accessible staging paths.

The first hour:

- Update every WordPress site to 7.1.4 now — the CISA deadline is 6 November 2026 and the flaw is exploitable during the upgrade window itself.

- Check whether you run Ivanti Connect Secure and identify the installed version; the CISA deadline for CVE-2026-111357 passed 2 November 2026.
- Check whether you run self-managed GitLab CE/EE and confirm it is on 19.2.8, 19.3.5, or 19.4.2; the CISA deadline passed 1 November 2026.
- Check Cisco ASA and FTD for tunnel groups with secondary authentication configured; the CISA deadline passed 1 November 2026.

In the next patch cycle

- Ivanti Connect Secure, CVE-2026-118527, due in 9 days. A logged-in attacker on Ivanti Connect Secure can write files to a predictable location on disk. The record names this as chainable with CVE-2026-111357 and CVE-2026-104935.

Who can skip most of this

Firms that run none of WordPress, Ivanti Connect Secure, self-managed GitLab CE/EE, or Cisco Secure Firewall ASA or FTD can set this week's list aside; other vulnerabilities may still apply to their estate.

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.

> *We need written confirmation on five CISA-listed vulnerabilities. Please check each product and confirm the version and patch status: - WordPress Core (CVE-2026-119977): our deadline is 6 November 2026 — update to 7.1.4. - Ivanti Connect Secure (CVE-2026-111357): deadline passed 2 November 2026 — confirm patch status. - Ivanti Connect Secure (CVE-2026-118527): deadline 13 November 2026 — confirm version 25.1.1.3 or 22.8R2.6. - GitLab CE/EE (CVE-2026-97229): deadline passed 1 November 2026 — confirm version 19.2.8, 19.3.5, or 19.4.2. - Cisco ASA or FTD (CVE-2026-76418): deadline passed 1 November 2026 — confirm patch status. Please reply in writing by 6 November 2026.*

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 >= "2026-10-29" and .dateAdded <= "2026-11-04")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 4 November 2026 it printed 5 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-2026-97229,CVE-2026-76418,CVE-2026-111357,CVE-2026-119977,CVE-2026-118527
```

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 names of running container images 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-2026-97229 --cve CVE-2026-76418 --cve CVE-2026-111357 --cve CVE-2026-119977 --cve CVE-2026-118527
```

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. It reads the names of the running images, not what is 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 4 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
1 November 2026	GitLab Community Edition and Enterprise Edition, CVE-2026-97229: CISA's deadline (added 29 October 2026).
1 November 2026	Cisco Secure Firewall ASA Software and Cisco Secure FTD Software, CVE-2026-76418: CISA's deadline (added 29 October 2026).
2 November 2026	Ivanti Connect Secure, CVE-2026-111357: CISA's deadline (added 30 October 2026).
6 November 2026	WordPress Core, CVE-2026-119977: CISA's deadline (added 3 November 2026).
13 November 2026	Ivanti Connect Secure, CVE-2026-118527: CISA's deadline (added 30 October 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/