contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

3 November 2026 · 5 exploited CVEs added this week

Analysis Report

5 entries added to CISA's exploited list in the week to 3 November 2026. 4 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	3 November 2026
FACTS AS OF	3 November 2026	VERSION	1.0
ACT ON NOW	4 of 5	STATUS	Facts as at 3 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-2026-11-03

The bottom line

> *The CISA deadline for WordPress Core (CVE-2026-119977) is 6 November 2026 — update every WordPress site to 7.1.4 now. The deadlines for Ivanti Connect Secure (CVE-2026-111357), GitLab CE/EE (CVE-2026-97229), and Cisco ASA/FTD (CVE-2026-76418) passed on 1–2 November 2026; act on those today if you have not.*

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

Separately, 995 new CVE records were published in the last 30 hours, 101 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

- New: WordPress Core, CVE-2026-119977.
- Deadline passed since: Ivanti Connect Secure, CVE-2026-111357.
- 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-2026-119977 (WordPress Core) was added since the 2 November 2026 watch. A number of entries left the week, including CVE-2026-46300, CVE-2026-41709, and CVE-2026-111497 among others. The deadline for CVE-2026-111357 (Ivanti Connect Secure) passed since the last watch.

At a glance

Entry	Act	CISA date	Fixed in	EPSS

GitLab Community Edition and Enterprise Edition (CVE-2026-97229)	Today	2 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	2 days past CISA's deadline	Not stated; see the note	0.01
Ivanti Connect Secure (CVE-2026-111357)	Today	1 day past CISA's deadline	Not stated; see the note	0.01
WordPress Core (CVE-2026-119977)	Today	Due in 3 days	WordPress 7.1.4	0.01
Ivanti Connect Secure (CVE-2026-118527)	Next patch cycle	Due in 10 days	25.1.1.3 (25.x branch) and 22.8R2.6 (22.x branch), listed as unaffected in the record published 3 November 2026.	n/a

How the week connects

The two Ivanti Connect Secure items are directly linked: the record states that CVE-2026-118527 and CVE-2026-111357 chain with each other and with CVE-2026-104935, which has left this week's list. The remaining three items — WordPress Core, GitLab CE/EE, and Cisco ASA/FTD — affect different products with unrelated weakness classes and have little in common with the Ivanti pair or with each other.

Do this today, in this order

- GitLab Community Edition and Enterprise Edition, CVE-2026-97229, 2 days past CISA's deadline. GitLab CE/EE has an integer overflow that lets an unauthenticated attacker run code on the server via a crafted CI/CD regular expression. The record gives a CVSS score of 10.0.
- Cisco Secure Firewall ASA Software and Cisco Secure FTD Software, CVE-2026-76418, 2 days past CISA's deadline. Cisco ASA and FTD with SSL VPN and secondary authentication configured can be forced to reload by an unauthenticated attacker, causing a denial of service. No account is needed.
- Ivanti Connect Secure, CVE-2026-111357, 1 day past CISA's deadline. Ivanti Connect Secure has a missing-authentication flaw that lets a local authenticated attacker escalate privileges. The record says it chains with CVE-2026-104935 and CVE-2026-118527.
- WordPress Core, CVE-2026-119977, due in 3 days. WordPress Core has a race condition during core upgrades that lets an unauthenticated attacker run code on the server. Any site running below 7.1.4 must be updated.

The first hour:

- Update WordPress Core to 7.1.4 on every site via Dashboard → Updates; the CISA deadline is 6 November 2026.
- Patch Ivanti Connect Secure to 25.1.1.3 (25.x branch) or 22.8R2.6 (22.x branch) and confirm CVE-2026-111357 is also resolved; that deadline passed 2 November 2026.
- Upgrade GitLab CE/EE to 19.2.8, 19.3.5, or 19.4.2 — the deadline passed 1 November 2026 and the flaw allows unauthenticated code execution.
- Check Cisco ASA and FTD for SSL VPN with secondary authentication configured; apply any available patch — the deadline passed 1 November 2026.

In the next patch cycle

- Ivanti Connect Secure, CVE-2026-118527, due in 10 days. Ivanti Connect Secure allows a remote authenticated attacker to upload attacker-controlled files to a known disk location. The record says this chains with CVE-2026-111357 and CVE-2026-104935.

Who can skip most of this

Organisations running none of WordPress, Ivanti Connect Secure, GitLab CE/EE, or Cisco ASA/FTD can set this week's items aside. That does not mean they face no other exposure.

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.

> *Good morning. We need written confirmation of the following by end of 5 November 2026, as several CISA deadlines are approaching or have passed. Please confirm the installed version and patch status for each: - WordPress Core (CVE-2026-119977, deadline 6 November 2026): confirm 7.1.4 is applied on each site. - Ivanti Connect Secure (CVE-2026-118527, deadline 13 November; CVE-2026-111357, deadline 2 November — now past): confirm 25.1.1.3 or 22.8R2.6 and that CVE-2026-111357 is resolved. - GitLab CE/EE (CVE-2026-97229, deadline 1 November — now past): confirm 19.2.8, 19.3.5, or 19.4.2. - Cisco ASA/FTD (CVE-2026-76418, deadline 1 November — now past): confirm patch status. 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 >= "2026-10-29" and .dateAdded <= "2026-11-03")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 3 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 3 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/