contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

2 November 2026 · 6 exploited CVEs added this week

Analysis Report

6 entries added to CISA's exploited list in the week to 2 November 2026. 4 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	2 November 2026
FACTS AS OF	2 November 2026	VERSION	1.0
ACT ON NOW	4 of 6	STATUS	Facts as at 2 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-2026-11-02

The bottom line

> *CVE-2026-111357 in Ivanti Connect Secure reaches its CISA deadline today, 2 November 2026; act now if you run that appliance. The CISA deadlines for GitLab CE/EE (CVE-2026-97229), Cisco ASA and FTD (CVE-2026-76418), and the Linux kernel (CVE-2026-46300) have already passed and still need resolving.*

CISA added 6 vulnerabilities to its exploited list from 28 October 2026 to 2 November 2026. 4 have a deadline within three days or already past, 3 of them past.

Separately, 506 new CVE records were published in the last 30 hours, 75 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

- Deadline passed since: GitLab Community Edition and Enterprise Edition, CVE-2026-97229; Cisco Secure Firewall ASA Software and Cisco Secure FTD Software, CVE-2026-76418.
- Left the seven-day window: 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.

Since the watch of 1 November 2026, no new items were added. The CISA deadlines for CVE-2026-97229 (GitLab CE/EE) and CVE-2026-76418 (Cisco ASA and FTD) passed since yesterday's watch.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
Linux Kernel (CVE-2026-46300)	Today	2 days past CISA's deadline	Fixed stable kernels include 5.10.257, 5.15.208, 6.1.174, 6.6.141, 6.12.91, and 6.18.33; check your distribution's advisory.	0.16
GitLab Community Edition and Enterprise Edition (CVE-2026-97229)	Today	1 day past CISA's deadline	GitLab CE/EE 19.2.8, 19.3.5, and 19.4.2, per the vendor's advisory.	0.27

Cisco Secure Firewall ASA Software and Cisco Secure FTD Software (CVE-2026-76418)	Today	1 day past CISA's deadline	Not stated; see the note	0.01
Ivanti Connect Secure (CVE-2026-111357)	Today	Due today	Not stated; see the note	0.01
Broadcom VMware ESX (CVE-2026-41709)	Next patch cycle	Due in 9 days	ESXi 9.1.0.0-25370933, ESXi 9.0.2.0100-25595025, and ESXi80U3j-25429389, per the CVE record.	0.01
Ivanti Connect Secure (CVE-2026-118527)	Next patch cycle	Due in 11 days	Not stated; see the note	n/a

How the week connects

The two Ivanti Connect Secure flaws chain together — CISA says CVE-2026-118527 and CVE-2026-111357 each enable the other. CVE-2026-46300 in the Linux kernel chains with PHP flaws that have now left this week's list. CVE-2026-41709 is the lowest-scoring item in a VMware advisory that also covers more serious flaws addressed in the same patch. The GitLab and Cisco ASA flaws have little in common with each other or the others.

Do this today, in this order

- Linux Kernel, CVE-2026-46300, 2 days past CISA's deadline. Linux kernel: a missing variable initialisation in the network stack allows local privilege escalation. CISA says it chains with PHP flaws to implant webshells and run commands as root. CVSS 7.8.
- GitLab Community Edition and Enterprise Edition, CVE-2026-97229, 1 day past CISA's deadline. GitLab CE/EE: an unauthenticated attacker can execute code on the server via a crafted regular expression in a CI/CD configuration. CVSS 10. Affects self-managed instances only.
- Cisco Secure Firewall ASA Software and Cisco Secure FTD Software, CVE-2026-76418, 1 day past CISA's deadline. Cisco ASA and FTD: an unauthenticated attacker can force the device to reload by sending a crafted request to the SSL VPN service, causing a denial of service. CVSS 8.6.
- Ivanti Connect Secure, CVE-2026-111357, due today.

The first hour:

- Confirm whether Ivanti Connect Secure runs in your environment; if it does, contact your provider now — CVE-2026-111357's CISA deadline is today, 2 November 2026.
- For self-managed GitLab: confirm the running version is 19.2.8, 19.3.5, or 19.4.2; the CISA deadline for CVE-2026-97229 passed yesterday.

- For Cisco ASA and FTD with SSL VPN enabled: confirm the CVE-2026-76418 patch is applied; that CISA deadline has also passed.
- For Linux servers: compare the running kernel version against the fixed builds for CVE-2026-46300; the CISA deadline passed two days ago.

In the next patch cycle

- Broadcom VMware ESX, CVE-2026-41709, due in 9 days. VMware ESX: an administrator can perform certain operations without them being logged. The same advisory covers more serious flaws in vCenter and ESX. CVSS 2.7.
- Ivanti Connect Secure, CVE-2026-118527, due in 11 days. Ivanti Connect Secure: an authenticated remote attacker can upload files with attacker-controlled content to a known location on disk. CISA says it chains with CVE-2026-111357.

Who can skip most of this

Organisations that run none of Ivanti Connect Secure, self-managed GitLab CE/EE, Cisco ASA or FTD, Linux servers, or VMware ESX can set this week aside. That is not a statement about other vulnerabilities.

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 to confirm our position on this week's CISA-listed flaws. The deadline for CVE-2026-111357 (Ivanti Connect Secure) is today, 2 November 2026. The deadlines for CVE-2026-97229 (GitLab CE/EE), CVE-2026-76418 (Cisco ASA and FTD), and CVE-2026-46300 (Linux kernel) have already passed. Please confirm in writing by 3 November: whether Ivanti Connect Secure is deployed and, if so, which version; whether our GitLab is self-managed and on 19.2.8, 19.3.5, or 19.4.2; whether Cisco ASA or FTD is deployed with SSL VPN and the patch applied; and which kernel versions run on our Linux hosts. CVE-2026-41709 in VMware ESX is due 11 November — please include the ESX build version in your reply.*

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 >= "2026-10-28" and .dateAdded <= "2026-11-02")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 2 November 2026 it printed 6 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-2026-46300,CVE-2026-97229,CVE-2026-76418,CVE-2026-111357,CVE-2026-41709,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-2026-46300 --cve CVE-2026-97229 --cve CVE-2026-76418 --cve CVE-2026-111357 --cve CVE-2026-41709 --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 2 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
31 October 2026	Linux Kernel, CVE-2026-46300: CISA's deadline (added 28 October 2026).
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).
11 November 2026	Broadcom VMware ESX, CVE-2026-41709: CISA's deadline (added 28 October 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/