contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

1 November 2026 · 10 exploited CVEs added this week

Analysis Report

10 entries added to CISA's exploited list in the week to 1 November 2026. 6 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 November 2026	VERSION	1.0
ACT ON NOW	6 of 10	STATUS	Facts as at 1 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-2026-11-01

The bottom line

> *Patch PHP (CVE-2026-109618, CVE-2026-109619) and the Linux kernel (CVE-2026-46300) first, because their CISA deadlines have passed. GitLab and Cisco ASA/FTD are due 1 November 2026, and Ivanti Connect Secure CVE-2026-111357 on 2 November 2026.*

CISA added 10 vulnerabilities to its exploited list from 26 October 2026 to 1 November 2026. 6 have a deadline within three days or already past, 3 of them past.

Separately, 117 new CVE records were published in the last 30 hours, 24 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: Linux Kernel, CVE-2026-46300.
- Left the seven-day window: CVE-2026-104935, CVE-2026-104935, CVE-2026-104935, CVE-2026-104935, CVE-2026-59309, CVE-2026-59310, CVE-2026-47876, CVE-2026-59309, CVE-2026-59310, CVE-2026-47876, CVE-2026-41703.

No new entries since the watch of 31 October 2026. Several listings dropped out of the week, including CVE-2026-104935 and CVE-2026-41703. The CISA deadline for CVE-2026-46300 has passed.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
PHP Group PHP (CVE-2026-109618)	Today	3 days past CISA's deadline	PHP 8.5.12, 8.4.27, 8.3.36, 8.2.35	1.00
PHP Group PHP (CVE-2026-109619)	Today	3 days past CISA's deadline	PHP 8.5.12, 8.4.27, 8.3.36, 8.2.35	1.00
Linux Kernel (CVE-2026-46300)	Today	1 day past CISA's deadline	Stable kernels incl. 5.10.257, 5.15.208, 6.1.174, 6.6.141, 6.12.91, 6.18.33	0.16
GitLab Community Edition and Enterprise Edition (CVE-2026-97229)	Today	Due today	GitLab CE/EE 19.2.8, 19.3.5, 19.4.2 (the vendor's advisory)	0.27
Cisco Secure Firewall ASA Software and Cisco Secure FTD Software (CVE-2026-76418)	Today	Due today	Not stated; see the note	0.01

Ivanti Connect Secure (CVE-2026-111357)	Today	Due tomorrow	Not stated; see the note	0.01
Google Brotli (CVE-2026-111497)	This week	Due in 9 days	Brotli 1.0.10, 1.1.1, 1.2.1	0.83
Adobe Commerce and Magento (CVE-2026-48356)	This week	Due in 9 days	2026-jul versions, e.g. 2.4.9-2026-jul, 2.4.8-2026-jul; Commerce Events 1.21.0	0.45
Broadcom VMware ESX (CVE-2026-41709)	Next patch cycle	Due in 10 days	ESXi 9.1.0.0-25370933, 9.0.2.0100-25595025, ESXi80U3j-25429389	0.01
Ivanti Connect Secure (CVE-2026-118527)	Next patch cycle	Due in 12 days	Not stated; see the note	n/a

How the week connects

CISA says CVE-2026-46300 (Linux kernel) can be chained with the two PHP flaws to implant webshells and run commands as root. It also says the two Ivanti Connect Secure flaws chain with CVE-2026-104935. The ESX flaw sits in an advisory that also fixes vCenter flaws. The rest have little in common.

Do this today, in this order

- PHP Group PHP, CVE-2026-109618, 3 days past CISA's deadline. PHP: an out-of-memory corruption flaw allowing unauthenticated remote code execution. Affected range runs from 5.4 to 8.5.11, so most PHP installs are in scope.
- PHP Group PHP, CVE-2026-109619, 3 days past CISA's deadline. PHP: a stale request-state flaw allowing unauthenticated remote code execution. CISA says it chains with the kernel flaw CVE-2026-46300 to run commands as root.
- Linux Kernel, CVE-2026-46300, 1 day past CISA's deadline. Linux kernel flaw, nicknamed Fragnesia. A local low-privilege user can alter cached file data. Web servers, shared build hosts, CI runners and container hosts matter most, especially where PHP runs.
- GitLab Community Edition and Enterprise Edition, CVE-2026-97229, due today. Self-managed GitLab CE and EE: an unauthenticated user can run code on the server through a crafted regular expression in CI/CD configuration. The record gives a score of 10.
- Cisco Secure Firewall ASA Software and Cisco Secure FTD Software, CVE-2026-76418, due today. Cisco ASA and FTD: an unauthenticated attacker can reload the firewall through the SSL VPN. The advisory ties it to secondary authentication on a tunnel group and says no workarounds exist.
- Ivanti Connect Secure, CVE-2026-111357, due tomorrow. Ivanti Connect Secure: a logged-in attacker can gain root. Volexity reports it was the last step of a chain that began without a

login, so the login condition gives little comfort.

The first hour:

- List every host running PHP, and check the version against 8.5.12, 8.4.27, 8.3.36 or 8.2.35. Patch, then restart PHP-FPM, Apache and long-running workers.
- Check Linux web servers and CI hosts for a kernel carrying the CVE-2026-46300 fix, using your distribution's advisory.
- Confirm whether you run self-managed GitLab, Cisco ASA/FTD with SSL VPN, or Ivanti Connect Secure. Patch or mitigate any you do.
- Find out which ESX, Adobe Commerce and Brotli-using services you run, and record their versions.

This week

These are not due yet, but the estimated chance of exploitation in the next 30 days (EPSS) is 0.40 or more.

- Google Brotli, CVE-2026-111497, due in 9 days. Google Brotli decoder: a crafted compressed stream can corrupt memory, leak data, crash a service or possibly run code. Any service that decodes Brotli from outside sources is exposed, including bundled copies.
- Adobe Commerce and Magento, CVE-2026-48356, due in 9 days. Adobe Commerce and Magento: an unrestricted file upload can lead to code execution. The attacker needs no account, but a victim must visit a crafted URL or interact with a compromised page.

In the next patch cycle

- Broadcom VMware ESX, CVE-2026-41709, due in 10 days. VMware ESX: an administrator can perform some operations without them being logged. Low score, but listed as exploited. The same advisory fixes more serious vCenter and VM-escape flaws.
- Ivanti Connect Secure, CVE-2026-118527, due in 12 days. Ivanti Connect Secure: a logged-in attacker can upload files with content they choose to a known place on disk. CISA says it chains with CVE-2026-104935 and CVE-2026-111357.

Who can skip most of this

If you run none of PHP, Linux servers, GitLab, Cisco ASA/FTD, Ivanti Connect Secure, VMware ESX, Adobe Commerce or Magento, or software that decodes Brotli, most of this week does not apply. Other flaws may still.

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.

> *Hello, CISA lists these as exploited. Please confirm in writing, by Wednesday, whether we run each one, and give the version and fix status: PHP (CVE-2026-109618, CVE-2026-109619), Linux kernel (CVE-2026-46300), GitLab (CVE-2026-97229), Cisco ASA/FTD (CVE-2026-76418), Ivanti Connect Secure (CVE-2026-111357, CVE-2026-118527), VMware ESX (CVE-2026-41709), Adobe Commerce/Magento (CVE-2026-48356) and Brotli (CVE-2026-111497). The PHP and kernel deadlines have passed. GitLab and Cisco were due 1 November 2026, and Ivanti CVE-2026-111357 is due 2 November 2026. 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 >= "2026-10-26" and .dateAdded <= "2026-11-
01")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 1 November 2026 it printed 10 rows, the ones above. A later run may show more.

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 1 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

29 October 2026	PHP Group PHP, CVE-2026-109618: CISA's deadline (added 26 October 2026).
29 October 2026	PHP Group PHP, CVE-2026-109619: CISA's deadline (added 26 October 2026).
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).
10 November 2026	Google Brotli, CVE-2026-111497: CISA's deadline (added 27 October 2026).
10 November 2026	Adobe Commerce and Magento, CVE-2026-48356: CISA's deadline (added 27 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/