

DAILY THREAT WATCH

Daily threat watch

31 October 2026 · 10 exploited CVEs added this week

Analysis Report

10 entries added to CISA's exploited list in the week to 31 October 2026. 6 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	31 October 2026
FACTS AS OF	31 October 2026	VERSION	1.0
ACT ON NOW	6 of 10	STATUS	Facts as at 31 October 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-2026-10-31

The bottom line

Update PHP and Linux kernels first: CISA's deadlines for them have passed or fall today. GitLab and Cisco ASA/FTD are due 1 November 2026, and Ivanti CVE-2026-111357 on 2 November 2026. Confirm which of these you run before anything else.

CISA added 10 vulnerabilities to its exploited list from 25 October 2026 to 31 October 2026. 6 have a deadline within three days or already past, 2 of them past.

Separately, 605 new CVE records were published in the last 30 hours, 124 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

Nothing new was added and no deadline passed.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
PHP Group PHP (CVE-2026-109618)	Today	2 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	2 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	Due today	Stable kernels 5.10.257, 5.15.208, 6.1.174, 6.6.141, 6.12.91, 6.18.33; distributions backport	0.16
GitLab Community Edition and Enterprise Edition (CVE-2026-97229)	Today	Due tomorrow	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 tomorrow	Not stated; see the note	0.01
Ivanti Connect Secure (CVE-2026-111357)	Today	Due in 2 days	Not stated; see the note	0.00
Google Brotli (CVE-2026-111497)	This week	Due in 10 days	Brotli 1.0.10, 1.1.1, 1.2.1; Node.js v26.12.1, v24.22.1, v22.23.4	0.83

Adobe Commerce and Magento (CVE-2026-48356)	This week	Due in 10 days	2026-jul versions, e.g. 2.4.9-2026-jul and 2.4.8-2026-jul; Commerce Events 1.21.0	0.45
Broadcom VMware ESX (CVE-2026-41709)	Next patch cycle	Due in 11 days	ESXi 9.1.0.0-25370933, ESXi 9.0.2.0100-25595025, ESXi80U3j-25429389	0.01
Ivanti Connect Secure (CVE-2026-118527)	Next patch cycle	Due in 13 days	Not stated; see the note	n/a

How the week connects

CISA says the Linux kernel flaw CVE-2026-46300 can be chained with the two PHP flaws, CVE-2026-109618 and CVE-2026-109619, to implant webshells and run commands as root. The Ivanti pair, CVE-2026-111357 and CVE-2026-118527, can also be chained, per CISA. The other items are unrelated products.

Do this today, in this order

- PHP Group PHP, CVE-2026-109618, 2 days past CISA's deadline. PHP: an out-of-memory corruption flaw allows unauthenticated remote code execution. Same fix as CVE-2026-109619, and PHP 7.x and older get no official release.
- PHP Group PHP, CVE-2026-109619, 2 days past CISA's deadline. PHP: a stale request-state flaw allows unauthenticated remote code execution. Any PHP site, container image or vendor appliance with PHP inside is in scope.
- Linux Kernel, CVE-2026-46300, due today. Linux kernel flaw, nicknamed Fragnesia, that lets a local low-privilege user alter cached file data. Matters most on web servers, shared build hosts, CI runners and container hosts.
- GitLab Community Edition and Enterprise Edition, CVE-2026-97229, due tomorrow. Self-managed GitLab CE and EE: the vendor says an unauthenticated user can run code on the server through a crafted regular expression in a CI/CD configuration. Score 10.
- Cisco Secure Firewall ASA Software and Cisco Secure FTD Software, CVE-2026-76418, due tomorrow. Cisco ASA and FTD: an unauthenticated attacker can reload the firewall during an SSL VPN connection. The vendor's advisory ties it to secondary authentication on a tunnel group and names no workaround.
- Ivanti Connect Secure, CVE-2026-111357, due in 2 days. Ivanti Connect Secure: the record says a logged-in local user can become root. It is the last step of a chain, so anyone running the appliance should treat it as more than its score of 7.

The first hour:

- Find every PHP install, including containers and vendor appliances. Update to 8.2.35, 8.3.36, 8.4.27 or 8.5.12, or your distribution's patch, then restart PHP workers.
- Check Linux kernels against your distribution's advisory for CVE-2026-46300, starting with web servers that run PHP.
- Self-managed GitLab: move to 19.2.8, 19.3.5 or 19.4.2. Cisco ASA or FTD: check the running configuration for secondary authentication on a tunnel group.
- Ivanti Connect Secure: confirm whether it runs and which version, then ask for the vendor's mitigations for CVE-2026-111357 and CVE-2026-118527.

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 10 days. Google Brotli decoder: a crafted compressed stream can corrupt memory or run code. Reaches you through Node.js, system libraries and any software that bundles its own copy.
- Adobe Commerce and Magento, CVE-2026-48356, due in 10 days. Adobe Commerce and Magento: an unrestricted file upload can lead to code execution. Stores patched late may already have been hit, so look for files that should not be there.

In the next patch cycle

- Broadcom VMware ESX, CVE-2026-41709, due in 11 days. VMware ESX: an administrator can perform some actions without them being logged. Score 2.7, but the same advisory fixes more serious vCenter and VM escape flaws, so patch to cover all of it.
- Ivanti Connect Secure, CVE-2026-118527, due in 13 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. No fixed version is stated.

Who can skip most of this

If you run none of PHP, Linux servers, self-managed GitLab, Cisco ASA or FTD, Ivanti Connect Secure, VMware ESX, Adobe Commerce or Magento, or software that decodes Brotli, you can skip most of this. That says nothing about other flaws.

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, could you confirm by Wednesday, in writing, our exposure to this week's CISA-listed flaws? Please give the running version and fix status for PHP (CVE-2026-109618, CVE-2026-109619; deadline 29 October 2026, passed), the Linux kernel (CVE-2026-46300; 31 October 2026), GitLab (CVE-2026-97229) and Cisco ASA/FTD (CVE-2026-76418), both due 1 November 2026, and Ivanti Connect Secure (CVE-2026-111357; 2 November 2026). Please also cover VMware ESX (CVE-2026-41709), Adobe Commerce/Magento (CVE-2026-48356) and Brotli (CVE-2026-111497). 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 >= "2026-10-25" and .dateAdded <= "2026-10-31")
| [.cveID, .dateAdded, .dueDate, .vendorProject, .product] | @tsv' | sort -k2
```

Run on 31 October 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 31 October 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/>