

DAILY THREAT WATCH

Daily threat watch

30 October 2026 · 10 exploited CVEs added this week

Analysis Report

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

PREPARED BY	NamiQ	DATE	30 October 2026
FACTS AS OF	30 October 2026	VERSION	1.0
ACT ON NOW	6 of 10	STATUS	Facts as at 30 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-2026-10-30

The short version

Start with PHP and GitLab. Both PHP flaws are past CISA's deadline and allow remote code execution without a login, and the GitLab flaw scores 10. Then check the Cisco firewall, the Linux kernel and Ivanti Connect Secure.

CISA added 10 vulnerabilities to its exploited list from 24 October 2026 to 30 October 2026. 6 have a deadline within three days or already past, 2 of them past.

Separately, 769 new CVE records were published in the last 30 hours, 121 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 the week has in common

Both PHP flaws share the same weaknesses, and the two Ivanti Connect Secure flaws are listed as chainable with each other. The other entries are different products and have little in common.

Do this today, in this order

- PHP Group PHP, CVE-2026-109618, 1 day past CISA's deadline. PHP flaw, score 9.8, that allows remote code execution without a login. The record points to out-of-memory corruption. Anyone running PHP must look. EPSS 1.00.
- PHP Group PHP, CVE-2026-109619, 1 day past CISA's deadline. PHP flaw, score 8.1, that allows remote code execution without a login. The record points to stale internal request state. Anyone running PHP must look. EPSS 1.00.
- Linux Kernel, CVE-2026-46300, due tomorrow. Linux kernel flaw, score 7.8. Network packet handling can end up changing data held in the page cache. Anyone running Linux servers should look. EPSS 0.16.
- GitLab Community Edition and Enterprise Edition, CVE-2026-97229, due in 2 days. GitLab flaw, score 10. Someone with no account can run code on the server through a crafted regular expression in a CI/CD configuration. Anyone running GitLab must look. EPSS 0.27.
- Cisco Secure Firewall ASA Software and Cisco Secure FTD Software, CVE-2026-76418, due in 2 days. Cisco ASA and FTD firewalls: a remote attacker with no login can make the device reload, which is a denial of service. Anyone with these firewalls must look. EPSS 0.01.
- Ivanti Connect Secure, CVE-2026-111357, due in 3 days. Ivanti Connect Secure flaw that lets a local, logged-in attacker raise their privileges. The record says it chains with CVE-2026-104935 and CVE-2026-118527. Ivanti users should look. EPSS 0.00.

The first hour:

- List where you run PHP, GitLab, Cisco ASA or FTD, Linux servers and Ivanti Connect Secure.

- Check PHP and GitLab first, then the Cisco firewalls and the Linux kernel, against the vendors' fixes.
- Ask your IT provider which of these they manage and when each will be done.
- Then check Ivanti, Adobe Commerce and Magento, and Brotli. The VMware ESX logging flaw can wait.

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 11 days. Brotli decompression library: a crafted compressed stream from a remote attacker can corrupt memory and possibly run code. Score 9.8. Check what you run that uses Brotli. EPSS 0.83.
- Adobe Commerce and Magento, CVE-2026-48356, due in 11 days. Adobe Commerce and Magento: an unrestricted file upload that can lead to code execution, score 9.3. Anyone running a shop on this platform must look. EPSS 0.45.

In the next patch cycle

- Broadcom VMware ESX, CVE-2026-41709, due in 12 days. VMware ESX flaw, score 2.7. An administrator can do certain things without them being logged. It matters mainly if you rely on ESX logs for audit. EPSS 0.01.
- Ivanti Connect Secure, CVE-2026-118527, due in 14 days. Ivanti Connect Secure flaw that lets a logged-in remote attacker upload files to a known location. The record says it chains with CVE-2026-104935 and CVE-2026-111357. Ivanti users should look.

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 >= "2026-10-24" and .dateAdded <= "2026-10-30")' \
| [.cveID, .dateAdded, .dueDate, .vendorProject, .product] | @tsv | sort -k2
```

Run on 30 October 2026 it printed 10 rows, the ones above. A later run may show more.

What we could not confirm

- CISA records ransomware use for each entry. Where it says unknown, that means not recorded, not that none has happened.
- EPSS is a probability for the next 30 days, recalculated daily. The figures are as at 30 October 2026 and will have moved.
- The exploited list names no attacker, so we do not guess one.
- The action order is a rule on CISA's own dates and EPSS. It is not a verdict on your estate. Check what you run first.
- The sentences about what each flaw is, what the week has in common and the first hour 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/>