contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

2 November 2026 · 8 exploited CVEs added this week

Analysis Report

8 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 8	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; if you run this appliance, contact your provider now. Deadlines for GitLab (CVE-2026-97229), Cisco ASA/FTD (CVE-2026-76418) and the Linux kernel (CVE-2026-46300) have all passed.*

CISA added 8 vulnerabilities to its exploited list from 27 October 2026 to 2 November 2026. 4 have a deadline within three days or already past, 3 of them past.

Separately, 231 new CVE records were published in the last 30 hours, 42 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-2026-109618, 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.

Since the 1 November watch, no new entries were added. CVE-2026-97229 (GitLab) and CVE-2026-76418 (Cisco ASA/FTD) moved to past deadline. CVE-2026-109618, CVE-2026-109619, CVE-2026-104935, CVE-2026-59309, CVE-2026-59310, CVE-2026-47876 and CVE-2026-41703 left the list.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
Linux Kernel (CVE-2026-46300)	Today	2 days past CISA's deadline	Stable kernels including 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, 19.4.2 (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 in the sources read.	0.01
Ivanti Connect Secure (CVE-2026-111357)	Today	Due today	Not stated in the sources read.	0.01
Google Brotli (CVE-2026-111497)	This week	Due in 8 days	Brotli 1.0.10, 1.1.1 or 1.2.1. Node.js v26.12.1, v24.22.1 or v22.23.4 (21 October 2026 security release), per the record.	0.83
Adobe Commerce and Magento (CVE-2026-48356)	This week	Due in 8 days	Adobe Commerce 2.4.9-2026-jul, 2.4.8-2026-jul and equivalent 2026-jul releases for each supported line; Commerce Events 1.21.0.	0.45
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 or ESXi80U3j-25429389, per the record.	0.01
Ivanti Connect Secure (CVE-2026-118527)	Next patch cycle	Due in 11 days	Not stated in the sources read.	n/a

How the week connects

The two Ivanti items share a product and a chain: CISA says CVE-2026-118527 and CVE-2026-111357 each chain with CVE-2026-104935. The Linux kernel flaw (CVE-2026-46300) chains with PHP flaws per CISA. The remaining items — GitLab, Cisco ASA/FTD, VMware ESX, Adobe Commerce, Brotli — cover different product families and share no stated connection.

Do this today, in this order

- Linux Kernel, CVE-2026-46300, 2 days past CISA's deadline. Linux kernel (3.9 up to the fixed builds): a network flaw alters page-cache data invisibly to file-integrity tools. CISA says it chains with PHP flaws to implant webshells and run commands as root.
- GitLab Community Edition and Enterprise Edition, CVE-2026-97229, 1 day past CISA's deadline. Self-managed GitLab CE/EE: an unauthenticated attacker can execute code on the server using a crafted CI/CD regular expression. The record gives a score of 10. Fixed in 19.2.8, 19.3.5 or 19.4.2.
- Cisco Secure Firewall ASA Software and Cisco Secure FTD Software, CVE-2026-76418, 1 day past CISA's deadline. Cisco ASA and FTD with SSL VPN and secondary authentication on a tunnel

group: an unauthenticated attacker can cause the device to reload. The vendor's advisory says no workaround exists.
- Ivanti Connect Secure, CVE-2026-111357, due today. Ivanti Connect Secure: a locally authenticated attacker can escalate to root because a broker trusts data it should not. Volexity says this was the final step of a chain that began without any login.

The first hour:

- Check whether Ivanti Connect Secure is deployed anywhere in your estate; if it is, contact your provider now — the CISA deadline for CVE-2026-111357 is today, 2 November 2026.
- Confirm self-managed GitLab CE/EE is running 19.2.8, 19.3.5 or 19.4.2 for CVE-2026-97229; the CISA deadline was 1 November 2026.
- Confirm Cisco ASA or FTD has the fix for CVE-2026-76418 if SSL VPN with secondary authentication is in use; the CISA deadline was 1 November 2026.
- Check the running kernel on Linux servers against the fixed builds for CVE-2026-46300; use your distribution's advisory rather than upstream version numbers alone.

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 8 days. Brotli and services that use it, including Node.js: a crafted compressed stream corrupts decoder memory, potentially executing code. Score 9.8. Any service decoding Brotli from untrusted input is exposed.
- Adobe Commerce and Magento, CVE-2026-48356, due in 8 days. Adobe Commerce and Magento: no login is needed to upload a file that runs code as a logged-in user. Score 9.3. Stores that were exposed before the patch should be checked for unexpected files.

In the next patch cycle

- Broadcom VMware ESX, CVE-2026-41709, due in 9 days. VMware ESX: an administrator can perform operations that leave no log entry. The same advisory covers two vCenter flaws scored 9.8 and a VM escape scored 9.3; patch to the build that fixes all.
- Ivanti Connect Secure, CVE-2026-118527, due in 11 days. Ivanti Connect Secure: a logged-in attacker can upload files with chosen content to a known location on disk. CISA says this chains with CVE-2026-104935 and CVE-2026-111357.

Who can skip most of this

If you run no Ivanti Connect Secure, self-managed GitLab, Cisco ASA or FTD, Linux servers, VMware ESX, Adobe Commerce, or Magento, and no service that decodes Brotli from outside your control,

most items here do not apply.

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 on several CISA-listed vulnerabilities, some with deadlines that have already passed. Please confirm the version running and whether the fix is in place for each: - Ivanti Connect Secure: CVE-2026-111357 (CISA deadline today, 2 November 2026) and CVE-2026-118527 (13 November 2026) - Self-managed GitLab CE/EE: CVE-2026-97229 (deadline was 1 November 2026) - Cisco ASA/FTD: CVE-2026-76418 (deadline was 1 November 2026) - Linux servers: CVE-2026-46300 (deadline was 31 October 2026) - VMware ESX: CVE-2026-41709 (11 November 2026) - Adobe Commerce/Magento: CVE-2026-48356 (10 November 2026) - Node.js or any Brotli service: CVE-2026-111497 (10 November 2026) Please reply with written confirmation for each item by end of day today. 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 >= "2026-10-27" and .dateAdded <= "2026-11-02")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 2 November 2026 it printed 8 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 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).
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/