contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

1 November 2026 · 8 exploited CVEs added this week

Analysis Report

8 entries added to CISA's exploited list in the week to 1 November 2026. 4 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	4 of 8	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

> *Self-managed GitLab (CVE-2026-97229) and Cisco ASA/FTD (CVE-2026-76418) reached CISA's date on 1 November 2026. Ivanti Connect Secure CVE-2026-111357 is due 2 November 2026. Confirm versions with your provider first. The Linux kernel flaw CVE-2026-46300 is past its date.*

CISA added 8 vulnerabilities to its exploited list from 27 October 2026 to 1 November 2026. 4 have a deadline within three days or already past, 1 of them past.

Separately, 104 new CVE records were published in the last 30 hours, 25 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-2026-109618, 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.

No new entries since the watch of 31 October 2026. CVE-2026-46300 has passed its CISA date. Earlier entries left the week, among them CVE-2026-104935, CVE-2026-109618, CVE-2026-109619, CVE-2026-59309, CVE-2026-59310 and CVE-2026-47876.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
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; Node.js v26.12.1, v24.22.1, v22.23.4	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, ESXi 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

Two links are stated by CISA. The three Ivanti Connect Secure flaws in this list can be chained with each other and with CVE-2026-104935. CVE-2026-46300 can be chained with the PHP flaws CVE-2026-109618 and CVE-2026-109619 to run commands as root. The ESX note sits in an advisory that also fixes CVE-2026-59309, CVE-2026-59310 and CVE-2026-47876. The rest have little in common.

Do this today, in this order

- Linux Kernel, CVE-2026-46300, 1 day past CISA's deadline. Linux kernel, nicknamed Fragnesia. A local user can 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 today. 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. 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 with SSL VPN: an unauthenticated attacker can make the firewall reload. The vendor's advisory says it applies when secondary authentication is set on a tunnel group, and that no workarounds exist.
- Ivanti Connect Secure, CVE-2026-111357, due tomorrow. Ivanti Connect Secure: a logged-in attacker can gain root, the record says. Volexity reports it was the last step of a chain that began without a login, so "logged in" gives little comfort.

The first hour:

- List where you run self-managed GitLab, Cisco ASA or FTD with SSL VPN, and Ivanti Connect Secure, with the version of each.
- GitLab: move to 19.2.8, 19.3.5 or 19.4.2, the versions the vendor's advisory names.

- Cisco ASA/FTD: check the running configuration for secondary authentication on any tunnel group. The vendor's advisory says no workarounds exist.
- Ivanti: ask for the patch Ivanti published on 29 October 2026. No fixed version is stated here, so get your provider to confirm it in writing.

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 stream can corrupt memory and may allow code execution. Any service that decodes Brotli data from outsiders is exposed, including Node.js and 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. It needs a user to visit a crafted URL. Stores unpatched since before July may already have been hit.

In the next patch cycle

- Broadcom VMware ESX, CVE-2026-41709, due in 10 days. VMware ESX: an administrator can do certain things without them being logged. The score is low, but the same advisory fixes two vCenter flaws scored 9.8, so patch to the build covering all.
- 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 GitLab, Cisco ASA or FTD, Ivanti Connect Secure, Linux servers, VMware ESX, Adobe Commerce or Magento, or software that decodes Brotli, you can skip most of this. Other flaws may still 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.

> *Hello, please confirm in writing, as soon as you can, whether we run these and which version and fix each has: self-managed GitLab (CVE-2026-97229), Cisco ASA or FTD with SSL VPN (CVE-2026-76418), Ivanti Connect Secure (CVE-2026-111357, CVE-2026-118527), the Linux kernel (CVE-2026-46300), VMware ESX (CVE-2026-41709), Adobe Commerce or Magento (CVE-2026-48356) and Brotli (CVE-2026-111497). CISA's dates are 1 November 2026 for GitLab and Cisco, 2 November 2026 for CVE-2026-111357, and 31 October 2026 for the kernel flaw, now past. 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-
01")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 1 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 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

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/