contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

3 November 2026 · 6 exploited CVEs added this week

Analysis Report

6 entries added to CISA's exploited list in the week to 3 November 2026. 4 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	3 November 2026
FACTS AS OF	3 November 2026	VERSION	1.0
ACT ON NOW	4 of 6	STATUS	Facts as at 3 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-2026-11-03

The bottom line

> *CISA added 6 vulnerabilities to its exploited list from 28 October 2026 to 3 November 2026. 4 have a deadline within three days or already past, 4 of them past. Read the exploited list first. It is the work list. Everything else is a reading list.*

Separately, 492 new CVE records were published in the last 30 hours, 76 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: Ivanti Connect Secure, CVE-2026-111357.
- Left the seven-day window: CVE-2026-111497, CVE-2026-48356, 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, CVE-2026-48356, CVE-2026-48356, CVE-2026-111497, CVE-2026-111497, 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.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
Linux Kernel (CVE-2026-46300)	Today	3 days past CISA's deadline	Not stated; see the note	0.16
GitLab Community Edition and Enterprise Edition (CVE-2026-97229)	Today	2 days past CISA's deadline	GitLab CE/EE 19.2.8, 19.3.5, and 19.4.2, per the vendor's advisory.	0.27
Cisco Secure Firewall ASA Software and Cisco Secure FTD Software (CVE-2026-76418)	Today	2 days past CISA's deadline	Not stated; see the note	0.01
Ivanti Connect Secure (CVE-2026-111357)	Today	1 day past CISA's deadline	Not stated; see the note	0.01

Broadcom VMware ESX (CVE-2026-41709)	Next patch cycle	Due in 8 days	Not stated; see the note	0.01
Ivanti Connect Secure (CVE-2026-118527)	Next patch cycle	Due in 10 days	Not stated; see the note	n/a

Do this today, in this order

- Linux Kernel, CVE-2026-46300, 3 days past CISA's deadline.
- GitLab Community Edition and Enterprise Edition, CVE-2026-97229, 2 days past CISA's deadline.
- Cisco Secure Firewall ASA Software and Cisco Secure FTD Software, CVE-2026-76418, 2 days past CISA's deadline.
- Ivanti Connect Secure, CVE-2026-111357, 1 day past CISA's deadline.

In the next patch cycle

- Broadcom VMware ESX, CVE-2026-41709, due in 8 days.
- Ivanti Connect Secure, CVE-2026-118527, due in 10 days.

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 >= "2026-10-28" and .dateAdded <= "2026-11-03")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 3 November 2026 it printed 6 rows, the ones above. A later run may show more.

Check your own project

If you build software, you can compare what a project declares with these CVEs from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE ids leave your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-46300,CVE-2026-97229,CVE-2026-76418,CVE-2026-111357,CVE-2026-41709,CVE-2026-118527
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same ids can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the names of running container images and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-46300 --cve CVE-2026-97229 --cve CVE-2026-76418 --cve CVE-2026-111357 --cve CVE-2026-41709 --cve CVE-2026-118527
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. It reads the names of the running images, not what is inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

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 3 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.

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).

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/