contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

10 November 2026 · 11 exploited CVEs added this week

Analysis Report

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

PREPARED BY	NamiQ	DATE	10 November 2026
FACTS AS OF	10 November 2026	VERSION	1.0
ACT ON NOW	6 of 11	STATUS	Facts as at 10 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-2026-11-10

The bottom line

> *CISA added 11 vulnerabilities to its exploited list from 5 November 2026 to 10 November 2026. 6 have a deadline within three days or already past. Read the exploited list first. It is the work list. Everything else is a reading list.*

Separately, 2360 new CVE records were published in the last 30 hours, 444 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

- New: Cisco BroadWorks, CVE-2026-20320; Google Chromium, CVE-2026-125350; Microsoft Office, CVE-2026-124194; Barracuda Networks Barracuda Email Security Gateway (ESG), CVE-2026-116606; Openwave Messaging Limited Webtop Media Transcoder, CVE-2026-111793; Barracuda Networks Multiple Products, CVE-2026-111560; IBM Aspera Faspex, CVE-2026-123218; OpenBSD OpenSSH, CVE-2026-123158; SignalWire FreeSwitch, CVE-2026-116779; GPUStack, CVE-2026-102895.
- Left the seven-day window (20): CVE-2026-119977, CVE-2024-27834, CVE-2026-111357, CVE-2026-118527, CVE-2026-97229, CVE-2026-76418, CVE-2026-46300, CVE-2026-41709, CVE-2026-111497, CVE-2026-48356, CVE-2026-109618, CVE-2026-109619, CVE-2026-104935, CVE-2026-59309, CVE-2026-59310, CVE-2026-47876, CVE-2026-41703, CVE-2024-27833, CVE-2024-27851, CVE-2024-27808.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
OpenBSD OpenSSH (CVE-2026-123158)	Today	Due in 2 days	OpenSSH 10.6p2, released 5 November 2026. The vendor's advisory describes this as a workaround release; the root cause is stated to lie outside OpenSSH itself.	0.17
SignalWire FreeSwitch (CVE-2026-116779)	Today	Due in 2 days	FreeSWITCH 1.11.3, released 28 August per the vendor's release notes on GitHub. The record lists all versions below 1.11.3 as affected.	0.02
IBM Aspera Faspex (CVE-2026-123218)	Today	Due in 2 days	IBM Aspera Faspex 5.0.19 PL1 (Linux). The vendor's advisory says to validate that the faspex-core container image is at 5.0.19 (image id 1ce4b13, Fix Pack: 1).	0.01

GPUStack (CVE-2026-102895)	Today	Due in 2 days	GPUStack 2.2.0. The record says this issue is fixed in version 2.2.0.	0.01
Barracuda Networks Barracuda Email Security Gateway (ESG) (CVE-2026-116606)	Today	Due in 3 days	ESG firmware 9.4.0.030 (record); apply patch BNSF-40425 if running firmware 9.4.017 or above, or BNSF-40430 if below 9.4.017, per the vendor's advisory.	0.02
Barracuda Networks Multiple Products (CVE-2026-111560)	Today	Due in 3 days	ESG: BNSF-40425 or BNSF-40430; ADC and WAF: BNADC-16586; Message Archiver: BNMA-32468; WAF Control Center: BNWF-60060; WSG: BNYF-24789. The advisory names patch IDs, not firmware version numbers.	0.01
SonicWall SonicOS SSLVPN (CVE-2026-19868)	Next patch cycle	Due in 10 days	Not stated; see the note	0.01
Cisco BroadWorks (CVE-2026-20320)	Next patch cycle	Due in 14 days	RI.2026.07 for all four components: Application Delivery Platform, Application Server, Profile Server, and Xtended Services Platform. Advisory first published 19 August 2026.	0.00
Openwave Messaging Limited Webtop Media Transcoder (CVE-2026-111793)	Next patch cycle	Due in 14 days	The record lists all versions before 1.1.22.0 as affected; 1.1.22.0 is the first version not listed as affected. The JVN advisory says to contact the developer for patch details.	0.00
Microsoft Office (CVE-2026-124194)	Next patch cycle	Due in 14 days	Office LTSC 2021: 16.0.14334.21048; Office LTSC 2024: 16.0.17932.21140. For Microsoft 365 Apps for Enterprise the record does not state a fixed build number.	n/a
Google Chromium (CVE-2026-125350)	Next patch cycle	Due in 14 days	Google Chrome 157.0.8103.50. The CVE record names versions prior to this as affected. The source does not name a fixed version for Microsoft Edge or Opera.	n/a

Do this today, in this order

- OpenBSD OpenSSH, CVE-2026-123158, due in 2 days.
- SignalWire FreeSwitch, CVE-2026-116779, due in 2 days.
- IBM Aspera Faspex, CVE-2026-123218, due in 2 days.
- GPUStack, CVE-2026-102895, due in 2 days.
- Barracuda Networks Barracuda Email Security Gateway (ESG), CVE-2026-116606, due in 3 days.
- Barracuda Networks Multiple Products, CVE-2026-111560, due in 3 days.

In the next patch cycle

- SonicWall SonicOS SSLVPN, CVE-2026-19868, due in 10 days.
- Cisco BroadWorks, CVE-2026-20320, due in 14 days.
- Openwave Messaging Limited Webtop Media Transcoder, CVE-2026-111793, due in 14 days.
- Microsoft Office, CVE-2026-124194, due in 14 days.
- Google Chromium, CVE-2026-125350, due in 14 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 >= "2026-11-05" and .dateAdded <= "2026-11-
10")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 10 November 2026 it printed 11 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-2026-123158,CVE-2026-116779,CVE-2026-123218,CVE-2026-
102895,CVE-2026-116606,CVE-2026-111560,CVE-2026-19868,CVE-2026-20320
```

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 hardware (maker, model, firmware), the running container images with their operating system and packages, 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-2026-123158 --cve CVE-2026-116779 --cve CVE-2026-123218 --cve CVE-2026-102895 --cve CVE-2026-116606 --cve CVE-2026-111560 --cve CVE-2026-19868 --cve CVE-2026-20320
```

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. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages 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 10 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
12 November 2026	OpenBSD OpenSSH, CVE-2026-123158: CISA's deadline (added 9 November 2026).
12 November 2026	SignalWire FreeSwitch, CVE-2026-116779: CISA's deadline (added 9 November 2026).
12 November 2026	IBM Aspera Faspex, CVE-2026-123218: CISA's deadline (added 9 November 2026).
12 November 2026	GPUStack, CVE-2026-102895: CISA's deadline (added 9 November 2026).
13 November 2026	Barracuda Networks Barracuda Email Security Gateway (ESG), CVE-2026-116606: CISA's deadline (added 10 November 2026).
13 November 2026	Barracuda Networks Multiple Products, CVE-2026-111560: CISA's deadline (added 10 November 2026).

20 November 2026	SonicWall SonicOS SSLVPN, CVE-2026-19868: CISA's deadline (added 6 November 2026).
24 November 2026	Cisco BroadWorks, CVE-2026-20320: CISA's deadline (added 10 November 2026).
24 November 2026	Openwave Messaging Limited Webtop Media Transcoder, CVE-2026-111793: CISA's deadline (added 10 November 2026).
24 November 2026	Microsoft Office, CVE-2026-124194: CISA's deadline (added 10 November 2026).
24 November 2026	Google Chromium, CVE-2026-125350: CISA's deadline (added 10 November 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/