contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

14 November 2026 · 12 exploited CVEs added this week

Analysis Report

12 entries added to CISA's exploited list in the week to 14 November 2026. 8 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	14 November 2026
FACTS AS OF	14 November 2026	VERSION	1.0
ACT ON NOW	8 of 12	STATUS	Facts as at 14 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-2026-11-14

The bottom line

> *Several fixes are already past their deadline: Barracuda email and network appliances, IBM Aspera Faspex, OpenSSH on musl-libc hosts, FreeSWITCH and GPUStack — patch these first if you run them. Check Point and UnrealIRCd are due 16 November; the rest have until 24 November.*

CISA added 12 vulnerabilities to its exploited list from 9 November 2026 to 14 November 2026. 8 have a deadline within three days or already past, 6 of them past.

Separately, 162 new CVE records were published in the last 30 hours, 29 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: Barracuda Networks Barracuda Email Security Gateway (ESG), CVE-2026-116606; Barracuda Networks Multiple Products, CVE-2026-111560.
- Left the seven-day window (21): CVE-2026-19868, 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.

Nothing new was added since yesterday's watch, so there is little to compare. The two Barracuda deadlines (CVE-2026-116606 and CVE-2026-111560) passed on 13 November. Several older items dropped out of the week.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
OpenBSD OpenSSH (CVE-2026-123158)	Today	2 days past CISA's deadline	OpenSSH 10.6p2 (released 5 November 2026).	0.19
SignalWire FreeSwitch (CVE-2026-116779)	Today	2 days past CISA's deadline	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	2 days past CISA's deadline	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	2 days past CISA's deadline	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	1 day past CISA's deadline	ESG firmware 9.4.0.030 or later. The advisory names patches BNSF-40425 (for firmware 9.4.017 and above) and BNSF-40430 (for firmware below 9.4.017).	0.11
Barracuda Networks Multiple Products (CVE-2026-111560)	Today	1 day past CISA's deadline	ESG: patches BNSF-40425 (firmware 9.4.017 and above) and BNSF-40430 (below 9.4.017); ADC and WAF: BNADC-16586; Message Archiver: BNMA-32468; WAF Control Center: BNWF-60060; WSG: BNYF-24789.	0.09
Check Point Multiple Products (CVE-2026-123039)	Today	Due in 2 days	No fixed version is stated in the sources.	0.02
UnrealIRCd (CVE-2026-114713)	Today	Due in 2 days	UnrealIRCd 6.2.7.1 (released 7 November 2026); or the vendor's hot-patch bundle, which the vendor says fixes it without a restart.	0.01
Microsoft Office (CVE-2026-124194)	Next patch cycle	Due in 10 days	Office LTSC 2021: 16.0.14334.21048. Office LTSC 2024: 16.0.17932.21140. Microsoft 365 Apps for Enterprise: the record names no version, only a vendor releases page.	0.02
Cisco BroadWorks (CVE-2026-20320)	Next patch cycle	Due in 10 days	RI.2026.07 for all four components — Application Delivery Platform, Application Server, Profile Server, and Xtended Services Platform — per the vendor's advisory.	0.01
Google Chromium (CVE-2026-125350)	Next patch cycle	Due in 10 days	Google Chrome 157.0.8103.50. The record description states versions prior to this are affected. No source names a fixed version for Microsoft Edge or Opera.	0.01
Openwave Messaging Limited Webtop Media Transcoder (CVE-2026-111793)	Next patch cycle	Due in 10 days	The JVN advisory lists all versions before 1.1.22.0 as affected; 1.1.22.0 is the first version not listed as affected. Contact Openwave to obtain the patch — the advisory gives no further procedural details.	0.01

How the week connects

The two Barracuda flaws chain: the record says the pre-authentication bypass (CVE-2026-116606) and the command injection (CVE-2026-111560) together reach root. Several others turn a login into

full control — Check Point, IBM Aspera Faspex and FreeSWITCH. Cisco BroadWorks and Chromium both mishandle XML, but in different ways, and are not otherwise linked.

Do this today, in this order

- OpenBSD OpenSSH, CVE-2026-123158, 2 days past CISA's deadline. On Linux built with musl libc and without PAM, sshd can accept an over-long password as valid, letting someone log in without the real one. Matters only to those hosts.
- SignalWire FreeSwitch, CVE-2026-116779, 2 days past CISA's deadline. An authenticated SIP account whose inbound message is accepted can reach FreeSWITCH's command layer, including operating-system commands. Matters to anyone running FreeSWITCH.
- IBM Aspera Faspex, CVE-2026-123218, 2 days past CISA's deadline. An authenticated Faspex user can craft a message that skips the authorisation check and gains administrative rights. Matters to anyone running IBM Aspera Faspex.
- GPUStack, CVE-2026-102895, 2 days past CISA's deadline. An unauthenticated attacker can spoof a loopback address in a request header to gain full admin access to GPUStack. The record says this has been exploited. Matters to anyone running GPUStack.
- Barracuda Networks Barracuda Email Security Gateway (ESG), CVE-2026-116606, 1 day past CISA's deadline. An unauthenticated attacker who can reach the ESG admin interface can load a crafted backup and overwrite the appliance's configuration. Matters to anyone running Barracuda Email Security Gateway.
- Barracuda Networks Multiple Products, CVE-2026-111560, 1 day past CISA's deadline. An admin on a Barracuda appliance can enter a crafted timezone value that runs operating-system commands as root. Affects ESG, Load Balancer ADC, WAF, WSG, Message Archiver and WAF Control Center.
- Check Point Multiple Products, CVE-2026-123039, due in 2 days. A user already logged in to a Check Point firewall or management server can send a command to a local system service and have it run as root. Matters to anyone running Check Point gear.
- UnrealIRCd, CVE-2026-114713, due in 2 days. An ordinary user on an UnrealIRCd network that links two or more servers can smuggle in commands that run with server authority. Matters to anyone running a linked UnrealIRCd network.

The first hour:

- Patch Barracuda Email Security Gateway and its other appliances now (CVE-2026-116606 and CVE-2026-111560) — both are past the 13 November deadline and together reach root.
- Update GPUStack to 2.2.0 (CVE-2026-102895); the record says it has been exploited and its 12 November deadline has passed.
- Then patch IBM Aspera Faspex, OpenSSH on musl-libc hosts and FreeSWITCH — all past their 12 November deadline; move to the fixed versions.

- Before 16 November, update Check Point gear (CVE-2026-123039) and any linked UnrealIRCd network (CVE-2026-114713).

In the next patch cycle

- Microsoft Office, CVE-2026-124194, due in 10 days. Outlook does not warn before a potentially unsafe action, so a crafted message can spoof over a network — but the user still has to open or click something. Matters to Outlook users.
- Cisco BroadWorks, CVE-2026-20320, due in 10 days. An attacker who can reach BroadWorks's Open Client Interface, with no login, can send crafted XML and read files from the server. Matters to anyone running Cisco BroadWorks.
- Google Chromium, CVE-2026-125350, due in 10 days. A use-after-free in Chromium's XML component lets a crafted webpage run code inside the browser sandbox. Matters to anyone using Chrome or another Chromium-based browser.
- Openwave Messaging Limited Webtop Media Transcoder, CVE-2026-111793, due in 10 days. An authenticated user can upload a crafted file to bypass the transcoder's file-type limits and reach data it holds. Matters to anyone running Webtop Media Transcoder.

Who can skip most of this

If you run none of these products — Barracuda, Check Point, Cisco BroadWorks, IBM Aspera Faspex, OpenSSH, FreeSWITCH, GPUStack, UnrealIRCd, Openwave Webtop or Outlook — most of this week does not apply. Chrome is the likely exception; check it either way.

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. Could you confirm whether we run any of these, and if so what version and whether the fix is applied? The deadlines below have passed or are close. Past deadline: Barracuda email and network appliances (CVE-2026-116606 and CVE-2026-111560, due 13 November), IBM Aspera Faspex (CVE-2026-123218), OpenSSH (CVE-2026-123158), FreeSWITCH (CVE-2026-116779) and GPUStack (CVE-2026-102895, all due 12 November). Due 16 November: Check Point (CVE-2026-123039) and UnrealIRCd (CVE-2026-114713). Please reply in writing with the version of each and confirmation that the fix is in place by end of day tomorrow. 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 >= "2026-11-09" and .dateAdded <= "2026-11-
14")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 14 November 2026 it printed 12 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-2026-123039,CVE-2026-114713
```

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-2026-123039 --cve CVE-2026-
114713
```

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 14 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
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).
16 November 2026	Check Point Multiple Products, CVE-2026-123039: CISA's deadline (added 13 November 2026).
16 November 2026	UnrealIRCd, CVE-2026-114713: CISA's deadline (added 13 November 2026).
24 November 2026	Microsoft Office, CVE-2026-124194: CISA's deadline (added 10 November 2026).
24 November 2026	Cisco BroadWorks, CVE-2026-20320: CISA's deadline (added 10 November 2026).
24 November 2026	Google Chromium, CVE-2026-125350: 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).

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/