contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

13 November 2026 · 12 exploited CVEs added this week

Analysis Report

12 entries added to CISA's exploited list in the week to 13 November 2026. 8 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	13 November 2026
FACTS AS OF	13 November 2026	VERSION	1.0
ACT ON NOW	8 of 12	STATUS	Facts as at 13 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-2026-11-13

The bottom line

> *CISA's deadline for both Barracuda CVEs (CVE-2026-116606 and CVE-2026-111560) falls today, 13 November 2026; patch all affected Barracuda appliances now. Four deadlines also passed on 12 November — IBM Aspera Faspex, OpenSSH, FreeSWITCH, and GPUStack — act on those immediately; Check Point and UnrealIRCd fall due 16 November.*

CISA added 12 vulnerabilities to its exploited list from 8 November 2026 to 13 November 2026. 8 have a deadline within three days or already past, 4 of them past.

Separately, 879 new CVE records were published in the last 30 hours, 218 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: Check Point Multiple Products, CVE-2026-123039; UnrealIRCd, CVE-2026-114713.
- Deadline passed since: 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 (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.

Two CVEs entered the watch since 12 November: CVE-2026-123039 (Check Point, deadline 16 November) and CVE-2026-114713 (UnrealIRCd, deadline 16 November). Twenty-one dropped out. Four deadlines passed on 12 November: IBM Aspera Faspex, OpenSSH, FreeSWITCH, and GPUStack.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
OpenBSD OpenSSH (CVE-2026-123158)	Today	1 day past CISA's deadline	OpenSSH 10.6p2 (released 5 November 2026).	0.19
SignalWire FreeSwitch (CVE-2026-116779)	Today	1 day 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	1 day 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	1 day 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	Due today	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	Due today	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 3 days	No source names a fixed version; the record lists only affected ranges and the unaffected array for both products is empty.	0.01
UnrealIRCd (CVE-2026-114713)	Today	Due in 3 days	UnrealIRCd 6.2.7.1, released 7 November 2026. A hot-patch requiring no restart is also available for UnrealIRCd 6, per the vendor's advisory.	0.00
Microsoft Office (CVE-2026-124194)	Next patch cycle	Due in 11 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 11 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 11 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 11 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 Barracuda pair (CVE-2026-116606 and CVE-2026-111560) are explicitly chained in the advisory: pre-authentication config bypass plus OS command injection gives root on the same appliance. CVE-2026-123218 (IBM Aspera), CVE-2026-123158 (OpenSSH), and CVE-2026-102895 (GPUStack) each bypass or mishandle authentication or authorisation. The other items are distinct products with no recorded connection.

Do this today, in this order

- OpenBSD OpenSSH, CVE-2026-123158, 1 day past CISA's deadline. On Linux with musl libc and without PAM, sshd accepts an over-long password as valid, allowing login without knowing the real password. Not applicable where glibc or PAM is in use.
- SignalWire FreeSwitch, CVE-2026-116779, 1 day past CISA's deadline. An authenticated SIP peer can reach FreeSWITCH's API command layer via the inbound MESSAGE handler and run OS commands as the daemon; the record also names credential and configuration disclosure.
- IBM Aspera Faspex, CVE-2026-123218, 1 day past CISA's deadline. An authenticated Faspex user can craft a message to bypass authorisation and gain full administrator privileges. The record scores this 9.8; CISA's deadline of 12 November has passed.
- GPUStack, CVE-2026-102895, 1 day past CISA's deadline. An unauthenticated attacker can gain full GPUStack administrative access by spoofing a loopback header; the record says exploitation was observed against version 2.1.1. Fixed in 2.2.0.
- Barracuda Networks Barracuda Email Security Gateway (ESG), CVE-2026-116606, due today. An unauthenticated attacker reaching the ESG Admin UI can overwrite Barracuda ESG's global configuration via a crafted backup archive. The advisory says chaining with CVE-2026-111560 gives root access.
- Barracuda Networks Multiple Products, CVE-2026-111560, due today. An authenticated Barracuda admin can inject OS commands via a crafted timezone value, run as root. Affects ESG, ADC, WAF, WSG, Message Archiver, and WAF Control Center; chains with CVE-2026-116606.
- Check Point Multiple Products, CVE-2026-123039, due in 3 days. An authenticated local user on Check Point gateway and security management appliances can send commands to the world-writable, unauthenticated Gaia OS DynamicCLI socket and have them executed as root.
- UnrealIRCd, CVE-2026-114713, due in 3 days. Any user on a linked UnrealIRCd network can inject commands processed with server authority across all linked servers. The CVSS score is 8.6; fixed in UnrealIRCd 6.2.7.1.

The first hour:

- Apply Barracuda patches for CVE-2026-116606 (BNSF-40425 or BNSF-40430 on ESG) and CVE-2026-111560 (named patches per appliance type) — both CISA deadlines fall today, 13 November.

- If IBM Aspera Faspex, OpenSSH on musl libc, FreeSWITCH, or GPUStack were not patched by 12 November, act on those next — their CISA deadlines have passed.
- Confirm UnrealIRCd version and apply the hot-patch or upgrade to 6.2.7.1; identify Check Point Jumbo Hotfix Takes on each appliance — both have CISA deadlines on 16 November.
- Update Google Chrome to 157.0.8103.50, then plan Cisco BroadWorks, Microsoft Outlook, and Openwave Webtop patches before 24 November 2026.

In the next patch cycle

- Microsoft Office, CVE-2026-124194, due in 11 days. Outlook does not warn before a potentially unsafe action, so a crafted message can spoof over the network. The user must open it; applies to Microsoft 365 Apps and Office LTSC 2021 and 2024.
- Cisco BroadWorks, CVE-2026-20320, due in 11 days. An unauthenticated attacker reaching the Cisco BroadWorks OCI-P port can read server files via crafted XML; the vendor's advisory says external entity resolution is on by default.
- Google Chromium, CVE-2026-125350, due in 11 days. A use-after-free in Chromium's XML component lets a remote attacker run code inside the browser sandbox via a crafted webpage. The record says Chrome, Edge, and Opera may be affected.
- Openwave Messaging Limited Webtop Media Transcoder, CVE-2026-111793, due in 11 days. An authenticated user of Webtop Media Transcoder can upload a crafted file to bypass file-type restrictions set by the administrator. The JVN advisory states exploitation has been observed.

Who can skip most of this

Teams running none of these products — Check Point, UnrealIRCd, Cisco BroadWorks, Chrome, Microsoft Office, Barracuda appliances, Openwave Webtop, IBM Aspera Faspex, OpenSSH, FreeSWITCH, or GPUStack — can stop here.

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.

> *We need written confirmation of patch status for several CISA-listed CVEs. Two Barracuda CVEs had a deadline today, 13 November 2026: CVE-2026-116606 (ESG auth bypass) and CVE-2026-111560 (command injection on ESG, ADC, WAF, WSG, Message Archiver, WCC). Four deadlines passed on 12 November: CVE-2026-123218 (IBM Aspera Faspex), CVE-2026-123158 (OpenSSH), CVE-2026-116779 (FreeSWITCH), and CVE-2026-102895 (GPUStack). Check Point and UnrealIRCd (CVE-2026-123039 and CVE-2026-114713) fall due 16 November. Chrome, Cisco BroadWorks, and Microsoft Outlook (CVE-2026-125350, CVE-2026-20320, CVE-2026-124194) fall due 24 November. Please confirm in writing by 15 November 2026 which of these products we run, the installed version, and the fix status for each.*

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 >= "2026-11-08" and .dateAdded <= "2026-11-
13")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 13 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 13 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/