contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

# Daily threat watch

**12 November 2026 · 11 exploited CVEs added this week**

## Analysis Report

11 entries added to CISA's exploited list in the week to 12 November 2026. 6 with a deadline inside three days, in the order to work them.

| | | | |
|---|---|---|---|
| PREPARED BY | NamiQ | DATE | 12 November 2026 |
| FACTS AS OF | 12 November 2026 | VERSION | 1.0 |
| ACT ON NOW | 6 of 11 | STATUS | Facts as at 12 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-2026-11-12

## The bottom line

> *Four listings fall due today, 12 November 2026: IBM Aspera Faspex, OpenSSH, FreeSWITCH and GPUStack. Two chained Barracuda flaws are due tomorrow, 13 November. Patch or mitigate all six first; the rest of the week runs to 20 and 24 November.*

CISA added 11 vulnerabilities to its exploited list from 6 November 2026 to 12 November 2026. 6 have a deadline within three days or already past.

Separately, 694 new CVE records were published in the last 30 hours, 130 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

- 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.

No new listing arrived since yesterday's watch of 11 November 2026. Twenty older listings left the week, and no deadline passed since then.

## At a glance

| Entry | Act | CISA date | Fixed in | EPSS |
|---|---|---|---|---|
| OpenBSD OpenSSH (CVE-2026-123158) | Today | Due today | OpenSSH 10.6p2 (released 5 November 2026). | 0.19 |
| SignalWire FreeSwitch (CVE-2026-116779) | Today | Due today | 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 today | 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 today | 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 tomorrow | ESG 9.4.0.030 (first unaffected version per the CVE record); patch BNSF-40425 for ESG 9.4.017 and later; patch BNSF-40430 for ESG versions earlier than 9.4.017. | 0.09 |
| Barracuda Networks Multiple Products (CVE-2026-111560) | Today | Due tomorrow | Advisory patch IDs: ESG — BNSF-40425 (9.4.017+) or BNSF-40430 (<9.4.017); ADC and WAF — BNADCL-16586; BMA — BNMA-32468; WCC — BNWF-60060; WSG — BNYF-24789. | 0.06 |
| SonicWall SonicOS SSLVPN (CVE-2026-19868) | Next patch cycle | Due in 8 days | Not stated; see the note | 0.01 |
| Microsoft Office (CVE-2026-124194) | Next patch cycle | Due in 12 days | Not stated; see the note | 0.02 |
| Google Chromium (CVE-2026-125350) | Next patch cycle | Due in 12 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 |
| Cisco BroadWorks (CVE-2026-20320) | Next patch cycle | Due in 12 days | RI.2026.07 for all four components: Application Delivery Platform, Application Server, Profile Server, and Xtended Services Platform. The vendor's advisory names this as the first fixed release. | 0.01 |
| Openwave Messaging Limited Webtop Media Transcoder (CVE-2026-111793) | Next patch cycle | Due in 12 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 clearest link is the pair of Barracuda flaws: the record says the authentication bypass, CVE-2026-116606, can be chained with the command injection, CVE-2026-111560, to reach code execution without a login. Separately, several of this week's flaws bypass authentication or authorisation to gain admin access — IBM Aspera Faspex, GPUStack, OpenSSH and SonicWall SSLVPN among them.

## Do this today, in this order

- OpenBSD OpenSSH, CVE-2026-123158, due today. On Linux built with musl libc and without PAM, OpenSSH can accept an over-long password as valid and let someone log in without the real one. Only those hosts are affected.

- SignalWire FreeSwitch, CVE-2026-116779, due today. An authenticated SIP peer can reach FreeSWITCH's command layer and run operating-system commands as the daemon; credential disclosure and call control are also possible.
- IBM Aspera Faspex, CVE-2026-123218, due today. An authenticated IBM Aspera Faspex user can craft a message that skips the authorisation check and gain full admin rights. Versions 5.0.0 to 5.0.19 are affected.
- GPUStack, CVE-2026-102895, due today. An unauthenticated attacker can spoof a loopback address in a header to gain full admin on GPUStack, create lasting API keys and read secrets. The record says this was the default setup.
- Barracuda Networks Barracuda Email Security Gateway (ESG), CVE-2026-116606, due tomorrow. An unauthenticated attacker who can reach the Barracuda ESG admin interface can bypass login and restore a crafted backup, rewriting the appliance's settings. Any ESG operator must act.
- Barracuda Networks Multiple Products, CVE-2026-111560, due tomorrow. An authenticated administrator can inject OS commands that run as root via the timezone field, across seven Barracuda appliance families including ESG, ADC, WAF and Web Security Gateway.

The first hour:

- Confirm the IBM Aspera Faspex version; if it is 5.0.0 to 5.0.19, upgrade to 5.0.19 PL1 — the deadline is today.
- Patch the two Barracuda flaws on ESG and the other listed appliances; if you cannot patch at once, restrict the admin interface to internal networks.
- Update GPUStack to 2.2.0 and FreeSWITCH to 1.11.3; both deadlines are today.
- If any SSH host runs musl libc without PAM, switch off password authentication and update to OpenSSH 10.6p2.

## In the next patch cycle

- SonicWall SonicOS SSLVPN, CVE-2026-19868, due in 8 days. Someone with valid credentials for a non-SAML login method can reach SonicWall SonicOS SSLVPN while skipping the SAML check, bypassing SAML-enforced MFA. SSLVPN operators should look.
- Microsoft Office, CVE-2026-124194, due in 12 days. A missing confirmation step in Outlook lets an attacker spoof over the network without the user acting. Organisations running Microsoft Office Outlook should look.
- Google Chromium, CVE-2026-125350, due in 12 days. A flaw in Chromium's XML handling lets a crafted webpage run code inside the browser sandbox. Chrome, Edge and Opera users, and others on Chromium browsers, should care.
- Cisco BroadWorks, CVE-2026-20320, due in 12 days. An unauthenticated attacker who can reach Cisco BroadWorks's OCI-P service can make the server read back local files, including configuration data. Anyone running BroadWorks should check.

- Openwave Messaging Limited Webtop Media Transcoder, CVE-2026-111793, due in 12 days. An authenticated Openwave Webtop Media Transcoder user can upload a crafted file to bypass file-type limits and reach sensitive data; the advisory says attacks have been observed.

## Who can skip most of this

If you run no Barracuda appliance, IBM Aspera Faspex, GPUStack, FreeSWITCH, Openwave transcoder, Cisco BroadWorks or SonicWall SSLVPN, most of this week passes you by. Chrome and Outlook users still need those two updates.

## 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. Please confirm where we stand on this week's listed exploited flaws. Due today, 12 November 2026: IBM Aspera Faspex (CVE-2026-123218), OpenSSH (CVE-2026-123158), FreeSWITCH (CVE-2026-116779) and GPUStack (CVE-2026-102895). Due tomorrow, 13 November: two chained Barracuda flaws (CVE-2026-116606, CVE-2026-111560). Still open: Cisco BroadWorks (CVE-2026-20320), Chrome (CVE-2026-125350), Outlook (CVE-2026-124194), Openwave transcoder (CVE-2026-111793) and SonicWall SSLVPN (CVE-2026-19868). For each we run, please confirm in writing which version is installed and whether the fix is applied, by 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 >= "2026-11-06" and .dateAdded <= "2026-11-12")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 12 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-2026-124194
```

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-2026-124194
```

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 12 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). |
| 20 November 2026 | SonicWall SonicOS SSLVPN, CVE-2026-19868: CISA's deadline (added 6 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). |
| 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). |

## 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/