contact@namiq.io · namiq.io

NamiQ

DAILY THREAT WATCH

Daily threat watch

15 November 2026 · 8 exploited CVEs added this week

Analysis Report

8 entries added to CISA's exploited list in the week to 15 November 2026. 4 with a deadline inside three days, in the order to work them.

PREPARED BY	NamiQ	DATE	15 November 2026
FACTS AS OF	15 November 2026	VERSION	1.0
ACT ON NOW	4 of 8	STATUS	Facts as at 15 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-2026-11-15

The bottom line

> *Barracuda appliance owners are past CISA's 13 November 2026 deadline for two linked flaws, CVE-2026-116606 and CVE-2026-111560: close the Admin UI to the internet and patch first. Check Point and UnrealIRCd owners have until 16 November 2026, which is tomorrow.*

CISA added 8 vulnerabilities to its exploited list from 10 November 2026 to 15 November 2026. 4 have a deadline within three days or already past, 2 of them past.

Separately, 120 new CVE records were published in the last 30 hours, 22 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 (25): CVE-2026-123158, CVE-2026-116779, CVE-2026-123218, CVE-2026-102895, 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.

No entries were added since the watch of 14 November 2026. Several older entries have dropped out of the week's list. No deadline has passed since that watch.

At a glance

Entry	Act	CISA date	Fixed in	EPSS
Barracuda Networks Barracuda Email Security Gateway (ESG) (CVE-2026-116606)	Today	2 days 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	2 days 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 tomorrow	Not stated; see the note	0.02

UnrealIRCd (CVE-2026-114713)	Today	Due tomorrow	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 9 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 9 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 9 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 9 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 is the clear link. The record says CVE-2026-116606 can be chained with CVE-2026-111560, and the vendor's advisory says the two together can give root on Email Security Gateway. Check Point and UnrealIRCd both let an ordinary logged-in user gain root or server authority, but through unrelated weaknesses. The other items have little in common beyond this week.

Do this today, in this order

- Barracuda Networks Barracuda Email Security Gateway (ESG), CVE-2026-116606, 2 days past CISA's deadline. An attacker with no login who reaches the Barracuda Email Security Gateway Admin UI can load a crafted backup and overwrite the appliance's whole configuration.
- Barracuda Networks Multiple Products, CVE-2026-111560, 2 days past CISA's deadline. An administrator on several Barracuda appliances can inject OS commands through a timezone value, and they run as root. Chained with CVE-2026-116606 on ESG, no valid login is needed.
- Check Point Multiple Products, CVE-2026-123039, due tomorrow. The record says a logged-in local user on Check Point firewalls and management servers can send commands to an unprotected root service and have them run as root.
- UnrealIRCd, CVE-2026-114713, due tomorrow. Any user on an UnrealIRCd network that links two or more servers can inject server-to-server commands that run with server authority.

Anyone hosting UnrealIRCd must look.

The first hour:

- Barracuda: check whether any appliance's Admin UI can be reached from the internet. Limit it to internal networks, then apply the patch that matches your firmware.
- Check Point: confirm whether you run Check Point gateways or management servers. The sources we read name no fixed version, so ask your provider for the vendor's fix.
- UnrealIRCd: if you host it, upgrade to 6.2.7.1 or apply the vendor's hot-patch. The vendor says the hot-patch needs no restart.
- Chrome and Outlook: check the browser and Office versions on every machine and make sure updates have been installed.

In the next patch cycle

- Microsoft Office, CVE-2026-124194, due in 9 days. The record says Outlook can skip a warning before an unsafe action, which lets an attacker spoof over a network. The user still has to act. This affects Outlook users.
- Cisco BroadWorks, CVE-2026-20320, due in 9 days. An attacker with no login who can reach Cisco BroadWorks can send crafted XML to it and read sensitive configuration. Anyone running BroadWorks must look.
- Google Chromium, CVE-2026-125350, due in 9 days. A crafted webpage can run code inside the browser sandbox in Chromium-based browsers, including Chrome, Edge and Opera. Almost every office needs to check its browsers.
- Openwave Messaging Limited Webtop Media Transcoder, CVE-2026-111793, due in 9 days. An authenticated user of Openwave Webtop Media Transcoder can get round file-type limits. The JVN advisory says this may expose sensitive information. Only Openwave customers need to look.

Who can skip most of this

If you run no Barracuda, Check Point, UnrealIRCd, Cisco BroadWorks or Openwave systems, only the Chrome and Outlook items apply to you. That does not protect you from other flaws.

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.

> *Hello, could you please check the following for us this morning? Barracuda appliances (CVE-2026-116606 and CVE-2026-111560): CISA's date of 13 November 2026 has passed. Check Point gateways or management servers (CVE-2026-123039) and UnrealIRCd (CVE-2026-114713): CISA's date is 16 November 2026. Also, due 24 November 2026: Cisco BroadWorks (CVE-2026-20320), Google Chrome and other Chromium browsers (CVE-2026-125350), Outlook (CVE-2026-124194) and Openwave Webtop Media Transcoder (CVE-2026-111793). For each one, please confirm in writing by 16 November 2026 whether we run it, which version we have and whether the fix is in place. 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 >= "2026-11-10" and .dateAdded <= "2026-11-
15")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 15 November 2026 it printed 8 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-2026-116606,CVE-2026-111560,CVE-2026-123039,CVE-2026-
114713,CVE-2026-124194,CVE-2026-20320,CVE-2026-125350,CVE-2026-111793
```

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-2026-116606 --cve CVE-2026-111560 --cve CVE-2026-123039 --cve CVE-2026-114713 --cve CVE-2026-124194 --cve CVE-2026-20320 --cve CVE-2026-125350 --cve CVE-2026-111793
```

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 15 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
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/