contact@namiq.io · namiq.io

NamiQ

WEEKLY HIGHLIGHT AND GUIDELINE

Weekly highlight and guideline

Week to 15 November 2026 · 8 exploited, 17 new critical

Analysis Report

The week to 15 November 2026: 8 entries added to CISA's exploited list, 17 new critical records worth reading, the deadlines to watch, and a plan for Monday to Friday.

PREPARED BY	NamiQ	DATE	15 November 2026
FACTS AS OF	15 November 2026	VERSION	1.0
ACT ON FIRST	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/weekly-highlight-2026-11-15

The bottom line

> *Start Monday with Barracuda. CISA's date for both Barracuda flaws, CVE-2026-116606 and CVE-2026-111560, was 13 November 2026 and has passed, and the vendor's advisory says chaining them can give root. Then turn to Check Point and UnrealIRCd, both due 16 November 2026. The rest of this week has more time.*

From 9 November 2026 to 15 November 2026 CISA added 8 vulnerabilities to its exploited list, 4 with a deadline within three days of today or already past. The daily highlights named 17 new critical records that nothing says yet anyone is using.

At a glance

Entry	What it is	Act by	Fixed in	Read next
Barracuda Networks Barracuda Email Security Gateway (ESG), CVE-2026-116606	On CISA's exploited list	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).	Technical Analysis
Barracuda Networks Multiple Products, CVE-2026-111560	On CISA's exploited list	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.	Technical Analysis
Check Point Multiple Products, CVE-2026-123039	On CISA's exploited list	Due tomorrow	Not stated; see the note	Technical Analysis
UnrealIRCd, CVE-2026-114713	On CISA's exploited list	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.	Technical Analysis
Microsoft Office, CVE-2026-124194	On CISA's exploited list	CISA's date 24 November 2026	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.	Technical Analysis

Cisco BroadWorks, CVE-2026-20320	On CISA's exploited list	CISA's date 24 November 2026	RI.2026.07 for all four components — Application Delivery Platform, Application Server, Profile Server, and Xtended Services Platform — per the vendor's advisory.	Technical Analysis
Google Chromium, CVE-2026-125350	On CISA's exploited list	CISA's date 24 November 2026	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.	Technical Analysis
Openwave Messaging Limited Webtop Media Transcoder, CVE-2026-111793	On CISA's exploited list	CISA's date 24 November 2026	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.	Technical Analysis
Fundacja Widzialni WidzialniCMS (CVE-2026-110468)	New record, scored 10	Check this week	Version 2.5, as stated in the CERT Polska advisory published 9 November 2026.	Technical Analysis
Unknown Confection WordPress Cable (CVE-2026-115252)	New record, scored 10	Check this week	No unaffected release is listed in the record. The vendor's page was unreadable, so no fixed version is known from any source we could read.	Technical Analysis
SAP_SE SAP NetWeaver AS ABAP and ABAP Platform (SAML2 Service Provider) (CVE-2026-120017)	New record, scored 10	Check this week	See the note	Technical Analysis
Adobe Connect (CVE-2026-121351)	New record, scored 10	Check this week	Per the vendor's advisory (APSB26-191, 10 November 2026): 12.12.a, 12.11.i, 12.10.f, 12.9.a, and 12.8.a on Windows. The CVE record names 12.8.a as the first unaffected release.	Technical Analysis
D-Link DIR-878 (CVE-2026-124560)	New record, scored 10	Check this week	No fixed version. The record states this product is no longer supported by its maintainer, and no unaffected release is listed.	Technical Analysis
GeoVision Inc. GV-Face (CVE-2026-124600)	New record, scored 10	Check this week	2.2.2 (the record names this as unaffected; no vendor advisory could be read to confirm a release date)	Technical Analysis

D-Link M60 (CVE-2026-125086)	New record, scored 10	Check this week	No unaffected or patched version is listed in the CVE record. The researcher's notes and the record name only firmware 1.12.B01; no source names a fixed release.	Technical Analysis
Linksys EA8100 (CVE-2026-127275)	New record, scored 10	Check this week	See the note	Technical Analysis
TRENDnet TEW-657BRM (CVE-2026-129351)	New record, scored 10	Check this week	See the note	Technical Analysis
D-Link DIR-600L (CVE-2026-129353)	New record, scored 10	Check this week	See the note	Technical Analysis
D-Link DSL-6740C (CVE-2026-129444)	New record, scored 10	Check this week	See the note	Technical Analysis
STAGGS (CVE-2026-78287)	New record, scored 10	Check this week	3.4.0, per the Patchstack advisory published 9 November 2026.	Technical Analysis
Red Hat OpenShift Update Service (CVE-2026-110697)	New record, scored 9.9	Check this week	Red Hat Quay 3.9.28, 3.10.28, 3.12.24, 3.14.10, 3.15.9, 3.16.7, 3.17.7, or 3.18.3, per the vendor's advisory. Quay.io has already been fixed by Red Hat.	Technical Analysis
Jet Admin Cloud Platform (CVE-2026-123965)	New record, scored 9.9	Check this week	No fixed version is named in the record; remediation status is 'none available'. A source states mitigation via a sandbox component around 29 October 2026, but no release number is given.	Technical Analysis
themagnifico52 Hotel Booking Lite (CVE-2026-125851)	New record, scored 9.9	Check this week	No official patch is available. The CVE record lists no unaffected version. Patchstack reported this on 11 November 2026 and states no patch exists.	Technical Analysis
Zohocorp M365 Manager Plus (CVE-2026-12591)	New record, scored 9.9	Check this week	M365 Manager Plus build 4818 (the vendor's advisory says it was fixed on 24 June 2026; builds 4817 and earlier are affected).	Technical Analysis

Edimax BR6478ACV2 (CVE-2026-129250)	New record, scored 9.9	Check this week	See the note	Technical Analysis

How the week connects

The two Barracuda entries belong together. CISA says CVE-2026-116606 can be chained with CVE-2026-111560: a way in without a login, then commands run as root. Check Point and UnrealIRCd have the same result but different weaknesses: an ordinary user gains root or server authority. Chromium and BroadWorks both involve XML handling, but the weaknesses differ. Four of the new high-scoring entries are D-Link devices. Two of them have built-in credentials, and none has a recorded fix.

What was added, day by day

- 10 November 2026: Barracuda Networks Barracuda Email Security Gateway (ESG), CVE-2026-116606; Barracuda Networks Multiple Products, CVE-2026-111560; Microsoft Office, CVE-2026-124194; Cisco BroadWorks, CVE-2026-20320; Google Chromium, CVE-2026-125350; Openwave Messaging Limited Webtop Media Transcoder, CVE-2026-111793.
- 13 November 2026: Check Point Multiple Products, CVE-2026-123039; UnrealIRCd, CVE-2026-114713.

The exploited list: what to do with each

- Barracuda Networks Barracuda Email Security Gateway (ESG), CVE-2026-116606, 2 days past CISA's deadline. An attacker with no login who can reach the Barracuda ESG Admin UI can import a crafted backup and rewrite the appliance's configuration. The advisory says chaining it with CVE-2026-111560 can give root.
- Barracuda Networks Multiple Products, CVE-2026-111560, 2 days past CISA's deadline. An administrator on Barracuda ESG, Load Balancer, ADC, WAF, WSG, Message Archiver or WAF Control Center can inject OS commands through a timezone value, and they run as root.
- Check Point Multiple Products, CVE-2026-123039, due tomorrow. On Check Point Gaia devices, an ordinary logged-in user can send a command to a local socket and have it run as root. Anyone running Check Point firewalls or management servers must look.
- UnrealIRCd, CVE-2026-114713, due tomorrow. On an UnrealIRCd network with two or more linked servers, any user can inject server-to-server commands that run with server authority. This matters to anyone hosting UnrealIRCd.
- Microsoft Office, CVE-2026-124194, due in 9 days. The record says Outlook does not warn before a potentially unsafe action, so a crafted message can pass as trustworthy. The user still has to click or open something.

- Cisco BroadWorks, CVE-2026-20320, due in 9 days. An attacker with no login who can reach the Cisco BroadWorks OCI-P service can read configuration and files through its XML parser. The vendor's advisory says this is on by default.
- 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. Every office that uses these browsers should check.
- Openwave Messaging Limited Webtop Media Transcoder, CVE-2026-111793, due in 9 days. A logged-in user who bypasses Webmail can make Openwave Webtop Media Transcoder handle file types the administrator blocked. The JVN advisory says attacks have been observed.

New critical records worth reading

None of these is on CISA's exploited list when we read it, so a score here is the record's author describing the worst case. Read the condition before you act on the number.

- Fundacja Widzialni WidzialniCMS, CVE-2026-110468, scored 10. Before version 2.5, anyone can upload executable files anywhere on a WidzialniCMS server and run code. The permission check happens only in the browser. Anyone running WidzialniCMS before version 2.5 must update — the record scores this 10 on CVSS 4.0, and no login is needed to upload executable files and run code on the server. Update to version 2.5 first.
- Unknown Confection WordPress Cable, CVE-2026-115252, scored 10. In Confection WordPress Cable 0.4.0 to 0.4.7, a visitor with no login can write settings into a PHP file that the site then runs. Any WordPress site running the Confection WordPress Cable plugin at versions 0.4.0 to 0.4.7 must act now; no fixed version is recorded in the CVE record or any source we could read. Disable and remove the plugin as the first step.
- SAP_SE SAP NetWeaver AS ABAP and ABAP Platform (SAML2 Service Provider), CVE-2026-120017, scored 10. Where the SAML2 Service Provider is active, crafted assertions can get past the login and be accepted as any user, including administrators. This affects SAP NetWeaver AS ABAP on SAP_BASIS 702 to 754. Any organisation running SAP NetWeaver AS ABAP on SAP_BASIS 702 to 754 with the SAML2 Service Provider active must act without delay; the record scores this at 10. First, confirm whether SAML2 SP is enabled and restrict network access to the ABAP stack until SAP publishes a patch.
- Adobe Connect, CVE-2026-121351, scored 10. A path traversal flaw lets a network attacker with no account read files outside the area Adobe Connect should reach. This matters to anyone running Adobe Connect on Windows. Any organisation running Adobe Connect on Windows should act now: the record scores this 10.0 with no login required. Find your installed version first — the vendor's advisory (APSB26-191, 10 November 2026) names fixed releases for each supported branch.
- D-Link DIR-878, CVE-2026-124560, scored 10. A crafted HNAP request with an oversized uid value overflows heap memory on the D-Link DIR-878 and may let an attacker run code. The record says the product is no longer supported.

- GeoVision Inc. GV-Face, CVE-2026-124600, scored 10. GeoVision GV-Face 2.2.1 sends credentials over unencrypted HTTP, so anyone on the same network segment can read them. Anyone running GeoVision GV-Face at version 2.2.1 must act; the record scores this 10 on CVSS 4.0, the maximum. The record names 2.2.2 as unaffected. Find which version is installed first.
- D-Link M60, CVE-2026-125086, scored 10. D-Link M60 firmware 1.12.B01 has a fixed credential for its mesh control service. Any device that can reach TCP port 1883 can send commands to root processes. Anyone running a D-Link M60 on firmware 1.12.B01 where untrusted devices share the same network should act now — no patched version is listed in the record. First, check whether anything untrusted can reach TCP port 1883 on the router and block that path at the VLAN or firewall boundary.
- Linksys EA8100, CVE-2026-127275, scored 10. Two JNAP functions on the Linksys EA8100 do not check the caller. Anyone who can reach the router can change its remote-management and WiFi-warning settings without logging in. If you run a Linksys EA8100 router, check its firmware now. CISA has not listed this, but working attack code is public and there is no fix, so make sure the router's management cannot be reached from the internet first.
- TRENDnet TEW-657BRM, CVE-2026-129351, scored 10. The record says a remote request to the TEW-657BRM's setup page can write out of bounds. The vendor says the product has been out of support for more than 15 years. Replace any still in use. If you still have a TRENDnet TEW-657BRM in use, plan to replace it: the vendor says it has been out of support for more than 15 years and no fix is recorded. First, find it and make sure its web interface cannot be reached from the internet. If you have none, you can stop reading.
- D-Link DIR-600L, CVE-2026-129353, scored 10. On D-Link DIR-600L firmware 2.17 and 2.17b02, crafted id or password values overflow a stack buffer remotely. The record says the exploit is public. Act if you run a D-Link DIR-600L router on firmware 2.17 or 2.17b02; the record says a working exploit is public. First, find whether any such router is in use and on that firmware. If you run no D-Link DIR-600L, you can stop here.
- D-Link DSL-6740C, CVE-2026-129444, scored 10. The record says D-Link DSL-6740C firmware 20131126 has a hard-coded FTP credential that can be used over the network, and that the exploit is public. If you use a D-Link DSL-6740C on firmware 20131126, act this week, because no source names a fixed firmware. First, make sure nobody outside your network can reach the router's FTP service. If you do not use this model, you can stop reading.
- STAGGS, CVE-2026-78287, scored 10. A visitor with no account can inject and run code on WordPress sites running STAGGS 3.3.0 or earlier. If your site runs the STAGGS WordPress plugin at version 3.3.0 or earlier, update to 3.4.0 immediately — no login is needed to exploit it. The first step is to check which version of STAGGS is installed across your WordPress sites.
- Red Hat OpenShift Update Service, CVE-2026-110697, scored 9.9. An ordinary account can put an underscore in a namespace name to read other tenants' robot tokens and images. The record lists OpenShift Update Service. The vendor's advisory names Red Hat Quay fixes. If you do not run Red Hat Quay or an OpenShift integrated registry, nothing to do. Anyone who does and shares it across teams should update to the patched release now; the vendor's advisory scores this 9.9 and needs only a basic account. Start by confirming which version is in use.

- Jet Admin Cloud Platform, CVE-2026-123965, scored 9.9. A remote attacker with a free Jet Admin Cloud Platform account can use prompt injection to expose its configuration files and the credentials stored in them. Anyone running Jet Admin Cloud Platform must act now: the record scores this 9.9 CRITICAL and states no fixed version exists. Contact Jet Admin to confirm the sandbox mitigation of around 29 October 2026 covers your deployment, and rotate any credentials stored in .env files immediately.
- themagnifico52 Hotel Booking Lite, CVE-2026-125851, scored 9.9. On sites running Hotel Booking Lite 2.5.1 or earlier, a subscriber-level WordPress account can upload a PHP web shell. Patchstack says no patch exists. Hotel Booking Lite at version 2.5.1 or earlier has no official patch and a subscriber-level account is enough to exploit it; the Patchstack source warns this type of flaw is used in mass-exploit campaigns against thousands of sites regardless of size. Check whether the theme is installed, then disable user registration until a patch is released.
- Zohocorp M365 Manager Plus, CVE-2026-12591, scored 9.9. In M365 Manager Plus builds 4817 and earlier, a logged-in technician can get past weak permission checks, exceed their role and possibly run code on the server. If you run ManageEngine M365 Manager Plus, find your build and upgrade to 4818; builds 4817 and earlier are affected. It is not on CISA's list, and the flaw needs a logged-in technician account, so a server with no delegated technicians can wait for the next cycle.
- Edimax BR6478ACV2, CVE-2026-129250, scored 9.9. The record scores this 9.9 for the Edimax BR6478ACV2 and gives no further detail here. If you use one, check the vendor's notice and keep its management off the internet.

Deadlines to watch

CISA's own deadlines for entries on its list, including ones added before this week. A date in the past means the deadline has already gone.

CISA's date	Entry	Where it stands
13 November 2026	Barracuda Networks Multiple Products, CVE-2026-111560	2 days past CISA's deadline
13 November 2026	Barracuda Networks Barracuda Email Security Gateway (ESG), CVE-2026-116606	2 days past CISA's deadline
16 November 2026	UnrealIRCd, CVE-2026-114713	Due tomorrow
16 November 2026	Check Point Multiple Products, CVE-2026-123039	Due tomorrow

Check Point (CVE-2026-123039) and UnrealIRCd (CVE-2026-114713) are due 16 November 2026. Both Barracuda entries, CVE-2026-116606 and CVE-2026-111560, passed their 13 November 2026 date. Carry them forward until each fix is confirmed.

The guideline: your week, in order

Thirty minutes on Monday does most of the work. The rest of the week is waiting, and then proving it is done.

Monday, for this week's list

- Barracuda: CISA's 13 November 2026 date has passed. Limit each appliance's Admin UI to internal networks, then apply the advisory's named patch for your firmware.
- Check Point: find out whether you run Quantum Security Gateway or Security Management on the listed Jumbo Hotfix levels. No source names a fixed version, so ask Check Point.
- UnrealIRCd: upgrade to 6.2.7.1, or apply the vendor's hot-patch, which the vendor says needs no restart. Do networks that link servers first.
- Chrome: check the installed version on every machine and update anything below 157.0.8103.50.

The routine, every week

- List what you run: servers, firewalls, VPNs, hypervisors, apps, and who looks after each. One line each is enough, and it is the step most firms skip.
- Compare that list with the table above, product by product. Read each version from the product itself, not from an old inventory.
- For each product that matches, read the fixed version in our technical analysis or the vendor's page, and reduce exposure first if you cannot update today.
- Book the update. Write down who owns it and the date. A change with no name and no date does not happen.
- Save the proof: the version output or a screenshot, with the date. That is what an auditor, an insurer or a customer will ask for.

By Wednesday

- Outlook: compare each machine's Office build with the fixed LTSC builds. Ask the provider what applies to Microsoft 365 Apps, because the record names no version.
- Routers: find any D-Link, Linksys, TRENDnet or Edimax models listed here. Keep their management off the internet, and book replacements where no fix is recorded.
- Websites and servers: ask whether you run STAGGS, Confection WordPress Cable, Hotel Booking Lite, Adobe Connect or SAP NetWeaver with SAML2, and book the updates.

By Friday

- Written confirmation from the provider of each listed product you run, its version and the fix applied, with the date.
- A record of anything still without a fix, such as Check Point, the routers and SAP: what was done to limit access, and who will check again.
- A note of the listed products you do not run, so next week's list is quicker to check.

Keep a weekly record

One row per product you run that appears above. Fill it in as you go and keep it: it is the evidence that the week was handled.

Product	Version found	Fixed version	Owner	Done on

Who can skip most of this

Most of this week does not apply if you run no Barracuda, Check Point, UnrealIRCd, BroadWorks or Openwave products, none of the listed routers or web software, and Chrome and Outlook are kept up to date. Other flaws still may apply.

Send this to your IT provider on Monday

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. CISA has listed several flaws as exploited this week, and we would like to know where we stand. Please confirm whether we run any of these, and if so the version and the fix: Barracuda Email Security Gateway and other Barracuda appliances (CVE-2026-116606, CVE-2026-111560), CISA date 13 November 2026, now past; Check Point (CVE-2026-123039) and UnrealIRCd (CVE-2026-114713), due 16 November 2026; Google Chrome (CVE-2026-125350) and Outlook (CVE-2026-124194), due 24 November 2026. Please also tell us whether any D-Link, Linksys, TRENDnet or Edimax routers are in use. We would be grateful for written confirmation of each version and fix by Friday. Thank you.*

Check it yourself in two minutes

Everything above comes from public sources. This command prints CISA's additions in the same seven days 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-
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.
- Figures are as at 15 November 2026: EPSS and scores move, and a new record can change in its first days. Nothing here has been tested, and the order is a rule on CISA's dates, not a verdict on your estate. Check what you run first.
- The bottom line, how the week connects, the plan by day, the carry-over and the message are our interpretation of the records and the vendors' pages, 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.
13 November 2026	Barracuda Networks Multiple Products, CVE-2026-111560: CISA's deadline.
16 November 2026	Check Point Multiple Products, CVE-2026-123039: CISA's deadline.
16 November 2026	UnrealIRCd, CVE-2026-114713: CISA's deadline.

Appendix 2. Definition of done

- Every product above was checked against what you run, and the list is dated.
- 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 limit on exposure.
- The weekly record is filled in and kept.

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/