contact@namiq.io · namiq.io

NamiQ

WEEKLY HIGHLIGHT AND GUIDELINE

Weekly highlight and guideline

Week to 8 November 2026 · 3 exploited, 20 new critical

Analysis Report

The week to 8 November 2026: 3 entries added to CISA's exploited list, 20 new critical records worth reading, the deadlines to watch, and a plan for Monday to Friday.

PREPARED BY	NamiQ	DATE	8 November 2026
FACTS AS OF	8 November 2026	VERSION	1.0
ACT ON FIRST	1 of 3	STATUS	Facts as at 8 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-2026-11-08

The bottom line

> *From 2 November 2026 to 8 November 2026 CISA added 3 vulnerabilities to its exploited list, 1 with a deadline within three days of today or already past. The daily highlights named 20 new critical records that nothing says yet anyone is using. Start Monday with the exploited list. It is the work list; the new records are a reading list.*

At a glance

Entry	What it is	Act by	Fixed in	Read next
WordPress Core, CVE-2026-119977	On CISA's exploited list	2 days past CISA's deadline	WordPress 7.1.4	Technical Analysis
Apple Multiple Products, CVE-2024-27834	On CISA's exploited list	CISA's date 18 November 2026	Safari 17.5; iOS 16.7.8 and 17.5; iPadOS 16.7.8 and 17.5; macOS Sonoma 14.5; tvOS 17.5; watchOS 10.5 (per the CVE record, published 13 May 2024).	Technical Analysis
SonicWall SonicOS SSLVPN, CVE-2026-19868	On CISA's exploited list	CISA's date 20 November 2026	The record does not name a fixed version; the unaffected list is empty. No vendor advisory could be read. Contact SonicWall for the first version that removes this flaw.	Technical Analysis
Microsoft Entra Device Registration (CVE-2026-109469)	New record, scored 10	Check this week	See the note	Technical Analysis
Unknown WP Libre Form (CVE-2026-118423)	New record, scored 10	Check this week	See the note	Technical Analysis
WAVLINK WN536AX6-A (CVE-2026-120276)	New record, scored 10	Check this week	See the note	Technical Analysis
Linksys E8450 (CVE-2026-120283)	New record, scored 10	Check this week	See the note	Technical Analysis

WAVLINK WN551X3-A (CVE-2026-120344)	New record, scored 10	Check this week	See the note	Technical Analysis
Apache Software Foundation Apache Juneau (CVE-2026-121489)	New record, scored 10	Check this week	Apache Juneau 9.2.1, as stated in the CVE record.	Technical Analysis
Qihoo 360 D621-2 (CVE-2026-121606)	New record, scored 10	Check this week	None. The researcher's disclosure states the flaw is present in all obtained firmware versions from 6.0.24 to 6.4.9 and that 6.4.9 remains unfixed.	Technical Analysis
Qihoo 360 D603-2 (CVE-2026-121607)	New record, scored 10	Check this week	See the note	Technical Analysis
Qihoo 360 Whole Home Router M5 (CVE-2026-121609)	New record, scored 10	Check this week	See the note	Technical Analysis
Linksys E5350 (CVE-2026-121932)	New record, scored 10	Check this week	See the note	Technical Analysis
Comfast CF-WR632AX (CVE-2026-122013)	New record, scored 10	Check this week	See the note	Technical Analysis
OpenIdentityPlatform OpenAM (CVE-2026-123551)	New record, scored 10	Check this week	OpenAM 16.1.4 — packages openam-federation-library, openam-notifications-websocket, and openam-server-only (advisory GHSA-5c3q-hp86-xjr8, published 22 October 2026).	Technical Analysis
Tenda AC19 (CVE-2026-123966)	New record, scored 10	Check this week	See the note	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
open-wanderer wanderer (CVE-2026-71495)	New record, scored 10	Check this week	0.20.0, released 7 July (per the v0.20.0 release notes on GitHub)	Technical Analysis

TOTOLINK A950RG (CVE-2026-121597)	New record, scored 9.9	Check this week	See the note	Technical Analysis
TOTOLINK CA300-PoE (CVE-2026-123957)	New record, scored 9.9	Check this week	See the note	Technical Analysis
kyverno (CVE-2026-124440)	New record, scored 9.9	Check this week	1.19.2 (GitHub advisory GHSA-39w8-hv5g-f73w, published 23 October 2026)	Technical Analysis
SolarWinds Dameware (CVE-2026-28336)	New record, scored 9.9	Check this week	SolarWinds Dameware 2026.3.1 (vendor's advisory published 3 November 2026).	Technical Analysis
Emerson Ovation (CVE-2022-29966)	New record, scored 9.8	Check this week	Emerson Ovation 3.8.0 Feature Pack 3, as stated in the CVE record.	Technical Analysis

What was added, day by day

- 3 November 2026: WordPress Core, CVE-2026-119977.
- 4 November 2026: Apple Multiple Products, CVE-2024-27834.
- 6 November 2026: SonicWall SonicOS SSLVPN, CVE-2026-19868.

The exploited list: what to do with each

- WordPress Core, CVE-2026-119977, 2 days past CISA's deadline.
- Apple Multiple Products, CVE-2024-27834, due in 10 days.
- SonicWall SonicOS SSLVPN, CVE-2026-19868, due in 12 days.

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.

- Microsoft Entra Device Registration, CVE-2026-109469, scored 10. Anyone running Microsoft Entra Device Registration must act: the record scores this 10 and requires no authentication. No fixed version is recorded; confirm whether this service is running and reachable from untrusted networks, then watch for Microsoft guidance.
- Unknown WP Libre Form, CVE-2026-118423, scored 10. Anyone running WP Libre Form 1.5.0.1 on a WordPress site must act without delay; the record scores this 10 and no fixed version is named. Disable the plugin now and watch the vendor's channel for a patched release.

- WAVLINK WN536AX6-A, CVE-2026-120276, scored 10. Anyone running WAVLINK WN536AX6-A on firmware V260507_2.0.0 should act this week: the record scores 10 on CVSS 4.0 and a working exploit is publicly available. No fixed version is known from any source; take the web management interface off any untrusted network as the first step.
- Linksys E8450, CVE-2026-120283, scored 10. Anyone running a Linksys E8450 on firmware 1.2.00.360516 should act now; the record scores this at 10 out of 10 under CVSS 4.0 and no patch exists. The vendor did not respond to disclosure, so check immediately whether the router's management interface is reachable from outside your network.
- WAVLINK WN551X3-A, CVE-2026-120344, scored 10.
- Apache Software Foundation Apache Juneau, CVE-2026-121489, scored 10. Operators of Apache Juneau must check whether DirectoryResource's view, upload, or delete settings are enabled — if none are, there is nothing to do. The record gives a maximum severity score of 10; if any of those settings are on, upgrade to version 9.2.1 at once.
- Qihoo 360 D621-2, CVE-2026-121606, scored 10. Anyone running a Qihoo 360 D621-2, D603-2, D600-2, D619, D606-6, or D706 camera on firmware 6.0.24 to 6.4.9 must act now: no fix exists and the exploit is public. Isolate the camera from untrusted networks immediately.
- Qihoo 360 D603-2, CVE-2026-121607, scored 10. Anyone running a Qihoo 360 D603-2, D600-2, D606-6, or D706 camera on firmware 6.4.0 to 6.4.7 should act now; no fixed version has been confirmed. Isolate the camera from untrusted networks immediately.
- Qihoo 360 Whole Home Router M5, CVE-2026-121609, scored 10. Anyone running a Qihoo 360 Whole Home Router M5 on firmware 4.0.17.1566 should act now; no fixed version has been published and the record says the exploit is publicly available. First, confirm your firmware version and whether the device has completed initial setup.
- Linksys E5350, CVE-2026-121932, scored 10. Owners of a Linksys E5350 on firmware 1.0.00.037 should act now: the exploit is public, no patch exists, and the vendor has not responded. Check first whether the router's admin interface is reachable from outside the local network, and restrict it if so.
- Comfast CF-WR632AX, CVE-2026-122013, scored 10.
- OpenIdentityPlatform OpenAM, CVE-2026-123551, scored 10. Organisations not running OpenIdentityPlatform OpenAM can stop reading. Those on versions 14.0.0 to 16.1.3 must upgrade to 16.1.4 promptly — the record scores this 10.0 and no login is needed to exploit it. Verify the installed version first.
- Tenda AC19, CVE-2026-123966, scored 10.
- D-Link DIR-878, CVE-2026-124560, scored 10.
- open-wanderer wanderer, CVE-2026-71495, scored 10. Anyone running a self-hosted Wanderer instance below 0.20.0 with PUBLIC_PRIVATE_INSTANCE not set to true should update to 0.20.0 now; the fix has been available since 7 July. Start by confirming the version and that setting in your docker-compose or environment file.
- TOTOLINK A950RG, CVE-2026-121597, scored 9.9.
- TOTOLINK CA300-PoE, CVE-2026-123957, scored 9.9. Anyone running TOTOLINK CA300-PoE on firmware 6.2c.884 should act now: the record scores this 9.9 and states the exploit is publicly

available, with no fixed firmware recorded. Check whether the management interface is reachable from outside your network and block that access immediately.

- kyverno, CVE-2026-124440, scored 9.9. Any team running Kyverno 1.19.1 on a multi-tenant cluster where namespace tenants can create policies must update to 1.19.2. The first step is to confirm which version is deployed — only 1.19.1 is listed as affected.
- SolarWinds Dameware, CVE-2026-28336, scored 9.9. Anyone running SolarWinds Dameware 2026.3 or earlier needs to act: the vendor's advisory, published 3 November 2026, recommends upgrading to version 2026.3.1 as soon as is practical. Start by confirming which version is installed across every host running Dameware.
- Emerson Ovation, CVE-2022-29966, scored 9.8. Any site running Emerson Ovation up to and including Version 3.8.0 Feature Pack 1 should plan to upgrade; the record scores this 9.8 because no login is needed to reach the affected protocols. Check which Feature Pack is installed first, then apply Feature Pack 3.

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
6 November 2026	WordPress Core, CVE-2026-119977	2 days past CISA's deadline

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.

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.

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

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 >= "2026-11-02" and .dateAdded <= "2026-11-
08")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 8 November 2026 it printed 3 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-2026-119977,CVE-2024-27834,CVE-2026-19868
```

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-2026-119977 --cve CVE-2024-27834 --cve CVE-2026-19868
```

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 8 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.

Appendix 1. Timeline

Date	Event
6 November 2026	WordPress Core, CVE-2026-119977: 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/