contact@namiq.io · namiq.io

NamiQ

WEEKLY HIGHLIGHT AND GUIDELINE

Weekly highlight and guideline

Week to 1 November 2026 · 10 exploited, 6 new critical

Analysis Report

The week to 1 November 2026: 10 entries added to CISA's exploited list, 6 new critical records worth reading, the deadlines to watch, and a plan for Monday to Friday.

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 November 2026	VERSION	1.0
ACT ON FIRST	6 of 10	STATUS	Facts as at 1 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-2026-11-01

The bottom line

> *Start with PHP, the Linux kernel, GitLab, Cisco ASA/FTD and Ivanti Connect Secure. CISA's dates for PHP (29 October) and the kernel (31 October) have passed. GitLab and Cisco fall due on 1 November, Ivanti CVE-2026-111357 on 2 November. Confirm versions and fixes for each first.*

From 26 October 2026 to 1 November 2026 CISA added 10 vulnerabilities to its exploited list, 6 with a deadline within three days of today or already past. The daily highlights named 6 new critical records that nothing says yet anyone is using.

At a glance

Entry	What it is	Act by	Fixed in	Read next
PHP Group PHP, CVE-2026-109618	On CISA's exploited list	3 days past CISA's deadline	PHP 8.5.12, 8.4.27, 8.3.36, 8.2.35	Our note
PHP Group PHP, CVE-2026-109619	On CISA's exploited list	3 days past CISA's deadline	PHP 8.5.12, 8.4.27, 8.3.36, 8.2.35	Our note
Linux Kernel, CVE-2026-46300	On CISA's exploited list	1 day past CISA's deadline	Stable kernels 5.10.257, 5.15.208, 6.1.174, 6.6.141, 6.12.91, 6.18.33; distributions backport	Our note
GitLab Community Edition and Enterprise Edition, CVE-2026-97229	On CISA's exploited list	Due today	GitLab CE/EE 19.2.8, 19.3.5, 19.4.2 (the vendor's advisory)	Our note
Cisco Secure Firewall ASA Software and Cisco Secure FTD Software, CVE-2026-76418	On CISA's exploited list	Due today	Not stated; see the note	Our note
Ivanti Connect Secure, CVE-2026-111357	On CISA's exploited list	Due tomorrow	Not stated; see the note	Our note
Google Brotli, CVE-2026-111497	On CISA's exploited list	CISA's date 10 November 2026	Brotli 1.0.10, 1.1.1, 1.2.1; Node.js v26.12.1, v24.22.1, v22.23.4	Our note

Adobe Commerce and Magento, CVE-2026-48356	On CISA's exploited list	CISA's date 10 November 2026	2026-jul versions, e.g. 2.4.9-2026-jul and 2.4.8-2026-jul; Commerce Events 1.21.0	Our note
Broadcom VMware ESX, CVE-2026-41709	On CISA's exploited list	CISA's date 11 November 2026	ESXi 9.1.0.0-25370933, ESXi 9.0.2.0100-25595025, ESXi80U3j-25429389	Our note
Ivanti Connect Secure, CVE-2026-118527	On CISA's exploited list	CISA's date 13 November 2026	Not stated; see the note	Our note
D-Link DIR-505 (CVE-2026-120189)	New record, scored 10	Check this week	See the note	Our note
WAVLINK WL-WN579A3-A (CVE-2026-120195)	New record, scored 10	Check this week	See the note	Our note
WAVLINK WL-WN530BE1-A (CVE-2026-120198)	New record, scored 10	Check this week	See the note	Our note
pgadmin.org pgAdmin 4 (CVE-2026-116241)	New record, scored 9.9	Check this week	pgAdmin 4 9.19. The record lists versions before 9.19 as affected. The tracking issue says the fix is pending for 9.19, and no source confirms a release.	Our note
mqttsnet thinglinks (CVE-2026-62853)	New record, scored 9.9	Check this week	ThingLinks 1.4.0 (released 22 July 2026, per the project's release notes)	Our note
addonsorg PDF Invoice for WooCommerce + Drag and Drop Template Builder (CVE-2026-109220)	New record, scored 9.8	Check this week	See the note	Our note

How the week connects

CISA says the two PHP flaws (CVE-2026-109618, CVE-2026-109619) and the Linux kernel flaw CVE-2026-46300 can be chained to implant PHP webshells and run commands as root. CISA also says the

three Ivanti Connect Secure flaws (CVE-2026-118527, CVE-2026-104935, CVE-2026-111357) can be chained. The sources we read link none of the other items.

What was added, day by day

- 26 October 2026: PHP Group PHP, CVE-2026-109618; PHP Group PHP, CVE-2026-109619.
- 27 October 2026: Google Brotli, CVE-2026-111497; Adobe Commerce and Magento, CVE-2026-48356.
- 28 October 2026: Linux Kernel, CVE-2026-46300; Broadcom VMware ESX, CVE-2026-41709.
- 29 October 2026: GitLab Community Edition and Enterprise Edition, CVE-2026-97229; Cisco Secure Firewall ASA Software and Cisco Secure FTD Software, CVE-2026-76418.
- 30 October 2026: Ivanti Connect Secure, CVE-2026-111357; Ivanti Connect Secure, CVE-2026-118527.

The exploited list: what to do with each

- PHP Group PHP, CVE-2026-109618, 3 days past CISA's deadline. A PHP memory flaw that allows unauthenticated remote code execution, and one half of the chain CISA describes with the kernel flaw. Fixed releases exist for 8.2 to 8.5; older branches depend on your distribution.
- PHP Group PHP, CVE-2026-109619, 3 days past CISA's deadline. A PHP flaw that allows unauthenticated remote code execution, and one half of the chain CISA describes with the kernel flaw. Fixed releases exist for 8.2 to 8.5; older branches depend on your distribution.
- Linux Kernel, CVE-2026-46300, 1 day past CISA's deadline. A Linux kernel flaw, nicknamed Fragnesia, that lets a local user alter cached file pages. CISA says it chains with the PHP flaws to give root. Matters most on web servers, CI runners and container hosts.
- GitLab Community Edition and Enterprise Edition, CVE-2026-97229, due today. The vendor says an unauthenticated user could run code on a self-managed GitLab server through a crafted regular expression in a CI/CD configuration. The record scores it 10. GitLab.com and Dedicated users can skip it.
- Cisco Secure Firewall ASA Software and Cisco Secure FTD Software, CVE-2026-76418, due today. The vendor's advisory says an unauthenticated attacker can make a Cisco ASA or FTD firewall reload with a crafted request to the SSL VPN, when secondary authentication is set on a tunnel group. It says no workarounds exist.
- Ivanti Connect Secure, CVE-2026-111357, due tomorrow. The record says a logged-in attacker can gain root on Ivanti Connect Secure. Volexity reports it was the last step of a chain that began without a login, so 'logged in' gives little comfort. Anyone running the appliance.
- Google Brotli, CVE-2026-111497, due in 9 days. A flaw in the Brotli decompression library: a crafted stream can corrupt memory, crash a process or possibly run code. Matters to any service that decodes Brotli data from outside, including Node.js and bundled copies.

- Adobe Commerce and Magento, CVE-2026-48356, due in 9 days. An upload flaw in Adobe Commerce and Magento that can lead to code execution. The attacker needs no account, but a victim must visit a crafted URL or interact with a compromised page. Fixed in Adobe bulletin APSB26-73.
- Broadcom VMware ESX, CVE-2026-41709, due in 10 days. A VMware ESX flaw: an administrator can do certain things without them being logged. It scores only 2.7, but the same advisory fixes more serious vCenter and VM escape flaws, so patch to the build covering all of it.
- Ivanti Connect Secure, CVE-2026-118527, due in 12 days. CISA says a logged-in attacker can upload files of their choosing to a known place on the Ivanti Connect Secure disk. It says this can be chained with CVE-2026-104935 and CVE-2026-111357. Anyone running the appliance should look.

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.

- D-Link DIR-505, CVE-2026-120189, scored 10. D-Link DIR-505 1.10B02 has a stack overflow in its TFTP upload handler that can be attacked remotely. The record says the exploit is public and scores it 10. Matters to anyone still running this router.
- WAVLINK WL-WN579A3-A, CVE-2026-120195, scored 10. The WAVLINK WL-WN579A3-A setup wizard lets an attacker run operating system commands through the wlan_ssid value. The record says it is remote, the exploit is public, and it scores 10. If you run a WAVLINK WL-WN579A3-A, find out this week whether its admin pages can be reached from the internet, and ask your supplier for a fixed firmware. If you do not run this model, you can stop reading.
- WAVLINK WL-WN530BE1-A, CVE-2026-120198, scored 10. The WAVLINK WL-WN530BE1-A (V251117) lets an attacker run commands through arguments to /protocol.csp. The record says it is remote, the exploit is public, and it scores 10. If you run a WAVLINK WL-WN530BE1-A on firmware V251117, find out this week whether its web interface can be reached from outside, and cut that access first. If you have no such device, you can stop reading.
- pgadmin.org pgAdmin 4, CVE-2026-116241, scored 9.9. A user with an ordinary database role can make pgAdmin 4's Import/Export tool run an operating-system command on the pgAdmin host. The record lists versions before 9.19 as affected. If you run pgAdmin 4 before 9.19, act now: limit who can sign in to it, and ask your IT provider to move to 9.19 once it is released. No release is confirmed yet. If you do not run pgAdmin 4, stop here.
- mqttsnet thinglinks, CVE-2026-62853, scored 9.9. A logged-in ThingLinks user can send Groovy code to the rule engine's script test endpoint. The server runs it with no sandbox, so it can run any code. Matters to anyone running ThingLinks. If you run ThingLinks, update to 1.4.0 this week and first find out who can log in to it. If you do not run ThingLinks, you can stop reading.
- addonsorg PDF Invoice for WooCommerce + Drag and Drop Template Builder, CVE-2026-109220, scored 9.8. The record says the PDF Invoice plugin for WooCommerce passes checkout note text into code that rebuilds PHP objects, unchecked. Someone with no account can place

an order and run code on the server. If you run a WordPress shop with WooCommerce and this invoice plugin, act today: the record says no login is needed to attack it. First find out whether the plugin is installed and which version. If you do not use it, you can stop reading.

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
29 October 2026	PHP Group PHP, CVE-2026-109618	3 days past CISA's deadline
29 October 2026	PHP Group PHP, CVE-2026-109619	3 days past CISA's deadline
31 October 2026	Linux Kernel, CVE-2026-46300	1 day past CISA's deadline
1 November 2026	Cisco Secure Firewall ASA Software and Cisco Secure FTD Software, CVE-2026-76418	Due today
1 November 2026	GitLab Community Edition and Enterprise Edition, CVE-2026-97229	Due today
2 November 2026	Ivanti Connect Secure, CVE-2026-111357	Due tomorrow

CISA dates falling next: Ivanti CVE-2026-111357 on 2 November 2026; GitLab CVE-2026-97229 and Cisco CVE-2026-76418 on 1 November 2026. Already past: Linux kernel CVE-2026-46300 on 31 October 2026; PHP CVE-2026-109618 and CVE-2026-109619 on 29 October 2026.

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

- Ask which hosts run PHP. Confirm 8.2.35, 8.3.36, 8.4.27, 8.5.12 or a distribution backport, and that PHP-FPM and Apache were restarted.
- Check Linux web servers and CI runners for the CVE-2026-46300 kernel fix, using your distribution's advisory, not a version number alone.
- Check self-managed GitLab is on 19.2.8, 19.3.5 or 19.4.2, and whether Cisco ASA/FTD has secondary authentication on an SSL VPN tunnel group.

- Find the Ivanti Connect Secure version and ask for the patch Ivanti published on 29 October 2026.

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 note 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

- Book updates for Adobe Commerce or Magento (2026-jul), Brotli carriers such as Node.js, and ESX to the build that covers the whole advisory.
- Make sure WAVLINK and D-Link router admin pages, pgAdmin 4 and ThingLinks cannot be reached from the internet, and limit who can sign in.
- If you run the WooCommerce PDF invoice plugin, find its version and ask the supplier for a fixed one.

By Friday

- Have written confirmation of the running version and fix for each product in your message, with the date it was applied.
- Record whether hosts exposed to the PHP flaws before patching were checked for webshells and files that should not be there.
- Record each product with no stated fixed version, the exposure you cut instead, and who owns it.

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

You can skip most of this if you run none of these: PHP, Linux servers, GitLab, Cisco ASA/FTD, Ivanti Connect Secure, ESX, Adobe Commerce, Brotli carriers or the named routers. That does not make you safe from other flaws.

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, could you confirm in writing by Wednesday which of these we run, with the version and fix applied? PHP (CVE-2026-109618, CVE-2026-109619; CISA date 29 October 2026). Linux kernel (CVE-2026-46300; 31 October 2026). GitLab (CVE-2026-97229; 1 November 2026). Cisco ASA/FTD (CVE-2026-76418; 1 November 2026). Ivanti Connect Secure (CVE-2026-111357, CVE-2026-118527; 2 November 2026 for the first). Please also check ESX, Adobe Commerce and Brotli (CVE-2026-41709, CVE-2026-48356, CVE-2026-111497). 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 >= "2026-10-26" and .dateAdded <= "2026-11-01")
    | [.cveID,.dateAdded,.dueDate,.vendorProject,.product] | @tsv' | sort -k2
```

Run on 1 November 2026 it printed 10 rows, the ones above. A later run may show more.

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 1 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
29 October 2026	PHP Group PHP, CVE-2026-109619: CISA's deadline.
29 October 2026	PHP Group PHP, CVE-2026-109618: CISA's deadline.
31 October 2026	Linux Kernel, CVE-2026-46300: CISA's deadline.
1 November 2026	GitLab Community Edition and Enterprise Edition, CVE-2026-97229: CISA's deadline.
1 November 2026	Cisco Secure Firewall ASA Software and Cisco Secure FTD Software, CVE-2026-76418: CISA's deadline.
2 November 2026	Ivanti Connect Secure, CVE-2026-111357: 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/