contact@namiq.io · namiq.io

NamiQ

WEEKLY HIGHLIGHT AND GUIDELINE

Weekly highlight and guideline

Week to 1 November 2026 · 8 exploited, 6 new critical

Analysis Report

The week to 1 November 2026: 8 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	4 of 8	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

> *On Monday, find out whether you run self-managed GitLab, Cisco ASA or FTD with SSL VPN, Ivanti Connect Secure, or Linux web servers. CISA's dates for GitLab and Cisco are 1 November 2026, Ivanti CVE-2026-111357 is 2 November 2026, and the Linux kernel date, 31 October 2026, has passed. Start with whichever of these you run.*

From 26 October 2026 to 1 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 6 new critical records that nothing says yet anyone is using.

At a glance

Entry	What it is	Act by	Fixed in	Read next
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; check your distribution's advisory	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	The 2026-jul versions, such as 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

Two groups connect. CISA says the three Ivanti Connect Secure flaws (CVE-2026-118527, CVE-2026-111357 and CVE-2026-104935) can be chained. CISA says the Linux kernel flaw can be chained with the PHP flaws CVE-2026-109618 and CVE-2026-109619 to run commands as root. The other items are different products with little in common.

What was added, day by day

- 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

- Linux Kernel, CVE-2026-46300, 1 day past CISA's deadline. A flaw in the Linux kernel's network stack, nicknamed Fragnesia. A local user can alter cached file data. It matters most on web servers, shared build servers and container hosts, where an attacker can get code running as an ordinary user.
- GitLab Community Edition and Enterprise Edition, CVE-2026-97229, due today. A flaw in self-managed GitLab CE and EE that lets someone with no login run code on the server through a crafted regular expression in a CI/CD configuration. The record gives a score of 10.
- Cisco Secure Firewall ASA Software and Cisco Secure FTD Software, CVE-2026-76418, due today. A flaw in Cisco ASA and FTD that lets an unauthenticated attacker reload the firewall through the SSL VPN. The vendor's advisory says it applies with secondary authentication on a tunnel group and that no workarounds exist.
- Ivanti Connect Secure, CVE-2026-111357, due tomorrow. A privilege escalation in Ivanti Connect Secure. Volexity reports it was the last step of a chain that began without a login, so "local" gives little comfort. The sources we read name no fixed version.
- Google Brotli, CVE-2026-111497, due in 9 days. A memory flaw in the Brotli decompression library. Any service that decodes Brotli data from outside is exposed, including Node.js, and copies bundled inside other software do not update with the operating system.
- Adobe Commerce and Magento, CVE-2026-48356, due in 9 days. A file upload flaw in Adobe Commerce and Magento, fixed in Adobe's July 2026 bulletin. Any public store without the 2026-jul patch is exposed. A patched store that sat unpatched for months should also be checked.
- Broadcom VMware ESX, CVE-2026-41709, due in 10 days. A logging gap in VMware ESX: an administrator can do some things without them being logged. Score 2.7, but the same Broadcom advisory also fixes two vCenter flaws scored 9.8 each, so patch the whole advisory.
- Ivanti Connect Secure, CVE-2026-118527, due in 12 days. A flaw in Ivanti Connect Secure that lets a logged-in attacker upload files with content of their choosing to a known place on disk. CISA says it can be chained with two other Ivanti flaws. The record gives no fixed version.

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. A buffer overflow in the TFTP upload handler of the D-Link DIR-505, version 1.10B02. The record says it can be attacked remotely and that the exploit is public. Only owners of this router need to act.

- WAVLINK WL-WN579A3-A, CVE-2026-120195, scored 10. A command injection in the setup wizard of the WAVLINK WL-WN579A3-A. The record says it can be attacked remotely and that the exploit is public. The sources we read name no fixed firmware. 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. A command injection in /protocol.csp on the WAVLINK WL-WN530BE1-A, firmware V251117. The record says it can be attacked remotely and that the exploit is public. No fixed firmware is named. 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, and the server runs it with no sandbox. Who can log in to ThingLinks decides your exposure. 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. A WooCommerce invoice plugin that rebuilds PHP objects from the checkout note field without checking it. The record says no login is needed, so any visitor who can place an order can attack it. 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
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

Ivanti CVE-2026-111357 is due 2 November 2026. GitLab CVE-2026-97229 and Cisco CVE-2026-76418 are due 1 November 2026. Linux Kernel CVE-2026-46300 passed its date of 31 October 2026. Treat all four as late if not yet confirmed fixed.

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 of these you run: GitLab self-managed, Cisco ASA or FTD with SSL VPN, Ivanti Connect Secure, Linux web servers, Magento, VMware ESX.
- Check your GitLab version. If it is not 19.2.8, 19.3.5 or 19.4.2 or later in its line, patch today.
- On Cisco ASA or FTD, check the running configuration for secondary authentication on any tunnel group. Note that the vendor lists no workarounds.
- On Ivanti Connect Secure, record the version and ask for the vendor's mitigations and patch for CVE-2026-111357.

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

- Check Linux kernels against your distribution's advisory for CVE-2026-46300, starting with PHP web servers, build servers and container hosts.
- Confirm Magento stores carry the 2026-jul patch, and find out which services decode Brotli from outside, including Node.js.

- Cut internet access to WAVLINK, D-Link and pgAdmin 4 admin pages, and limit who can log in to ThingLinks. Patch the VMware advisory as a whole.

By Friday

- Get written confirmation of the version and fix state for every product you run from this list.
- Record who checked, when, and which products turned out not to be in use.
- Ask your provider whether any Linux host or Magento store was exposed before patching, and what they looked 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

Who can skip most of this

If you run none of the listed products, you can skip most of this week. That says nothing about other flaws in the systems you do run.

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, please confirm in writing by Wednesday which of these we run, with version and fix status: GitLab (CVE-2026-97229), Cisco ASA or FTD (CVE-2026-76418), Ivanti Connect Secure (CVE-2026-111357, CVE-2026-118527), Linux kernels (CVE-2026-46300), Magento (CVE-2026-48356), VMware ESX (CVE-2026-41709) and Brotli (CVE-2026-111497). CISA's dates for the first three are 1 and 2 November 2026, and the Linux date, 31 October 2026, has passed. 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 8 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
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/