contact@namiq.io · namiq.io

NamiQ

NAMIQ MONTHLY HIGHLIGHT · FOR EVERY COMPANY THAT RUNS IT

October 2026 Security Highlight

What changed in the vulnerabilities attackers are using, and what you must decide and do about it

For CISOs, IT heads and the people who answer to them. The month's figures, the five pain points they point at, the decisions for the next thirty days, and a brief you can forward to your IT manager: what CISA's BOD 26-04 asks, and what to do this week.

PREPARED BY	NamiQ	ISSUED	1 November 2026
PERIOD	October 2026, 1st to month end	DATA	CISA catalogue to 30 October 2026
FOR	CISO, IT head, owner, risk lead	INSIDE	36 entries, 5 pain points, BOD 26-04 brief, 5 figures

NamiQ © 2026 NamiQ. All rights reserved. This document may be shared unaltered, with attribution. Figures are CISA's public catalogue as read on 30 October 2026, directional and not a statement about your estate. Web edition: namiq.io/resources/monthly-highlight

The month on a page

OCTOBER 2026

> CISA's median window to fix a newly listed flaw is now 3 days, against 14 across the last 12 months and 21 in October 2025. In October 2026, 29 of 36 entries gave 7 days or fewer and none gave more than 14. First decision: agree who can patch internet-facing systems inside 3 days, and how.

Our reading. The paragraph above is our interpretation of the figures below.

ADDED TO CISA'S LIST

36

September 2026: 43 (-16.3%). October 2025: 31 (+16.1%).

MEDIAN WINDOW TO FIX

3 days

The twelve months before: 14 days. 29 of 36 gave 7 days or fewer.

RANSOMWARE USE RECORDED

0 of 36

0% this month, 10.4% over the twelve months before. "Not recorded" is not "none".

NETWORK EDGE AND REMOTE ACCESS

16.7%

6 of 36. The twelve months before: 11.7%. A keyword rule, see Appendix B.

OLDER THAN THREE YEARS

13.9%

5 of 36 named a CVE from 2026 minus three or earlier. The twelve months before: 16.9%.

ENTRIES THAT NAME A CHAIN

12 of 36

CISA's description says the flaw can be chained with another.

Decisions for the next thirty days

Decision	Owner	By	Why it is worth doing
Set up a 3-day emergency patch route for internet-facing systems, with a named approver	CISO	within 30 days	The median window is 3 days, and 29 of 36 entries in October 2026 gave 7 days or fewer.
Check whether you run Ivanti Connect Secure, AhsayCBS, Zammad, PHP, Plex Media Server or Linux, and which versions	IT head	this week	These products make up this month's top five and 6 chains, covering 12 of 36 entries.
Check Ivanti Connect Secure first: version, patch, and signs of compromise	IT provider	this week	It ranks first with 8 points. Our note says to find your version and get it patched and checked for compromise.
Patch every member of a named chain in one change, not one at a time	security lead	within 30 days	6 chains cover 12 of 36 entries, 33.3%, against 2.3% over 12 months.
List old software still in service and decide to replace it or isolate it	IT head	within 30 days	5 of 36 entries (13.9%) are older than last year. The oldest is CVE-2015-3306, from 2015.

Sections marked **Our reading** are our interpretation of the figures, checked by code against them; they are not a statement by CISA or any vendor. Pages 3 to 5 can be forwarded to your IT manager. Every CVE and report named here links to its page on namiq.io (Appendix A).

Your five pain points this month

These are the five things a security leader loses sleep over, with what this month's figures say about each, what to do, and what proof to keep. The wording is ours, written from the figures; the figures are CISA's.

1. We cannot fix things in days.

THE FIGURES	October 2026: 36 entries, a median of 3 days from CISA adding an entry to its due date, against 14 over the twelve months before. 29 of 36 gave 7 days or fewer. For a federal agency, CISA's rule (BOD 26-04, Table 1) is 3 days, with a check for compromise, when an exposed system carries a listed flaw that an attacker can automate and that gives total control.
DO	Name the person who can approve an emergency change and write down the route. Then take the last entry that applied to you and time it from the day it was listed to the day it was fixed.
KEEP	The dated record: listed on, fixed on, version, who approved.

2. We do not know what we run.

THE FIGURES	A list of 36 new entries a month cannot be matched to systems nobody has counted. BOD 26-04 asks agencies to identify and tag every asset reachable from outside, with its environment, its exposure (public or internal) and its type (server, application or network device).
DO	One line per system: what it is, the version, who owns it, whether it is reachable from the internet, production or not. Start with what faces the internet.
KEEP	The list, with the date it was last reviewed.

3. What faces the internet is what gets hit first.

THE FIGURES	6 of 36 entries (16.7%) were in network-edge and remote-access products, against 11.7% over the twelve months before. CISA's own text for BOD 26-04 counts removing a system from the internet as a valid mitigation, because that changes the timeline that applies to it.
DO	List every firewall, VPN, gateway, router and remote-access product you run. Ask of each: does it need to face the internet, and who patches it?
KEEP	The list of internet-facing products, with versions and the date each was last updated.

4. Old software nobody remembers.

THE FIGURES	5 of 36 entries (13.9%) named a CVE from three or more years earlier; the oldest was CVE-2015-3306. The twelve months before: 16.9%. An old flaw on the list means an unpatched or unsupported system somewhere.
DO	Find what is past end of support or has not been updated in a year. Retire it, replace it, or take it off the network, and write down which.
KEEP	The decision for each old system, with a date.

5. We cannot show an auditor, an insurer or a customer that we acted.

THE FIGURES	Questionnaires, audits and cyber-insurance forms ask what you run, how fast you fix, and what proof you hold. The answer that survives is a dated record, not a statement. BOD 26-04 itself asks agencies for internal tracking and reporting, and for a written forensic triage report on the fastest cases.
DO	For each entry that applied to you this month, write one line: listed on, fixed on, version fixed in, proof (a command's output or a screenshot, with the date).
KEEP	A single monthly record, kept where an auditor can be given it.

For your IT manager: what BOD 26-04 asks, and what to do this week

BOD 26-04 is a directive CISA issued on 10 June 2026 to federal civilian agencies. It binds them, not a private company; it is the best public benchmark there is for how fast an exploited flaw should be dealt with.

It replaced two earlier directives, BOD 22-01 (which created the exploited list) and BOD 19-02. CISA sets the fix time by four questions: is the asset publicly exposed, is the flaw on the exploited list, can an attacker automate every step, and how much control does exploitation give.

CISA publishes the answers to the second, third and fourth for each CVE; you answer the first for your own systems.

CISA's Table 1: how fast, by four questions

As CISA publishes it in the directive of 10 June 2026 (read 1 November 2026). Days are calendar days. "& forensic triage" means the fix or mitigation and a check for compromise, both inside the timeline. The timeline starts when CISA adds the entry to the exploited list, or when an agency finds the flaw on an asset, whichever is first. Read the directive.

#	Publicly exposed?	On CISA's list?	Can an attacker automate it?	Technical impact	Timeline
1	**Yes**	**Yes**	**Yes**	**Total control**	**3 days & forensic triage**
2	**Yes**	**Yes**	**Yes**	**Partial control**	**3 days**
3	**Yes**	**Yes**	**No**	**Total control**	**3 days & forensic triage**
4	Yes	Yes	No	Partial control	14 days
5	**Yes**	**No**	**Yes**	**Total control**	**3 days**
6	Yes	No	Yes	Partial control	14 days
7	Yes	No	No	Total control	14 days
8	Yes	No	No	Partial control	60 days
9	**No**	**Yes**	**Yes**	**Total control**	**3 days & forensic triage**
10	No	Yes	Yes	Partial control	14 days
11	No	Yes	No	Total control	14 days
12	No	Yes	No	Partial control	14 days
13	No	No	Yes	Total control	60 days
14	No	No	Yes	Partial control	60 days
15	No	No	No	Total control	Fix on system upgrade
16	No	No	No	Partial control	Fix on system upgrade

Removing a system from the internet changes "publicly exposed" and so changes the timeline that applies. That is a valid mitigation in CISA's own words.

This week, in order

- [ ] List what faces the internet: product, version, owner, production or not. CISA defines 'publicly exposed' as reachable by unauthenticated or untrusted parties over a public network.
- [ ] Compare that list with Appendix A, and with the weekly and daily lists linked in this document. Mark every match.

- [ ] For each match, find its row in Table 1 and write the timeline next to it. If the row says forensic triage, collect evidence before you patch (steps 1 and 2).
- [ ] Fix or mitigate within that timeline, or take the system off the internet and write down that you did. Keep the version output or a screenshot, with the date.
- [ ] Sign up for CISA's email alerts for new entries, and name who reads them. The sign-up is on CISA's directive page.
- [ ] At the end of the week, write the month's record: entries that applied, listed on, fixed on, proof. File it where an auditor can be given it.

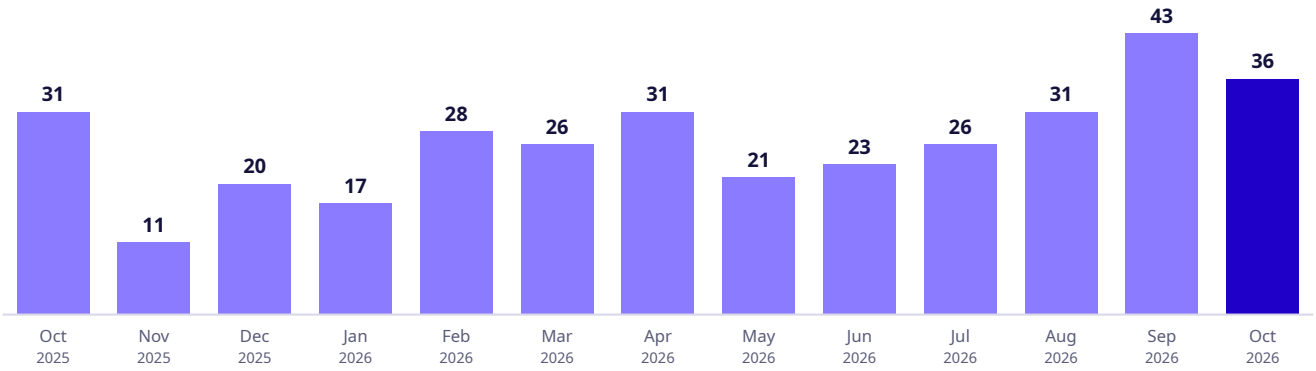
If a row says forensic triage: CISA's six steps

From CISA's implementation guidance (read it). The timelines are CISA's recommended practice, not a requirement; the requirement is that an adequate triage is done. Counted from the day the entry is added.

Step	When	What
1. Scope	within 2 hours	Work out which systems and services are in scope. Set up a way to talk that does not depend on systems that may be compromised.
2. Preserve and collect evidence	2 to 24 hours	Capture volatile data (memory, connections) first, and do not alter or fix the system before collecting when you can avoid it. Keep a log of what was collected, from where, when and by whom.
3. Patch and stabilise	2 to 24 hours	After the evidence is collected, apply the critical patch, and keep the business systems that depend on it working.
4. Contain and control	6 to 24 hours	Isolate affected and suspect systems, coordinated with evidence collection and patching. Contain in a way that does not tell an intruder they have been seen.
5. Analyse	24 to 48 hours	Look for unauthorised access, an intruder's presence, movement to other systems, persistence, and data staged or taken. Check whether the indicators exist elsewhere.
6. Decide on escalation	48 to 72 hours	Write the timeline and findings (who, what, where, when) and decide: no evidence of compromise, suspected, or confirmed, and who to tell.

1. What changed

Entries added to CISA's exploited list, by month, October 2025 to October 2026



Source: CISA Known Exploited Vulnerabilities catalogue, by the date CISA added each entry. October 2026 is a full month. Average of the twelve months before: 25.7 a month; the three before: 33.3.

Measure	October 2026	September 2026	October 2025	Twelve-month average before
Entries added	36	43	31	25.7
Median days from added to CISA's due date	3	3	21	14
Entries with a due date of 7 days or fewer	29	34	0	n/a
Ransomware use recorded as known	0 (0%)	n/a	n/a	10.4%
Network edge and remote access	6 (16.7%)	n/a	n/a	11.7%

Our reading: what changed

Median fix window is 3 days, down from 21 a year ago

The median was 21 days in October 2025 and has been 3 days every month since June 2026. In October 2026, 29 of 36 entries gave 7 days or fewer, 7 gave 8 to 14 days and none gave more. A weekly patch cycle no longer fits.

Entries naming a chain: 12 of 36, from 1 of 43 in September

CISA's entries that name a chain were 1 of 43 in September 2026 and are 12 of 36 in October 2026. That is 33.3%, against 2.3% over 12 months. One product can now need several patches in the same change.

Edge share is 16.7% (6 entries), against 11.7% over 12 months

The share of edge products rose above its 12-month level. Edge entries are the ones to check first, because the top-ranked entry this month, Ivanti Connect Secure, is one of them.

36 entries: 7 fewer than September, 40.1% above the 12-month average

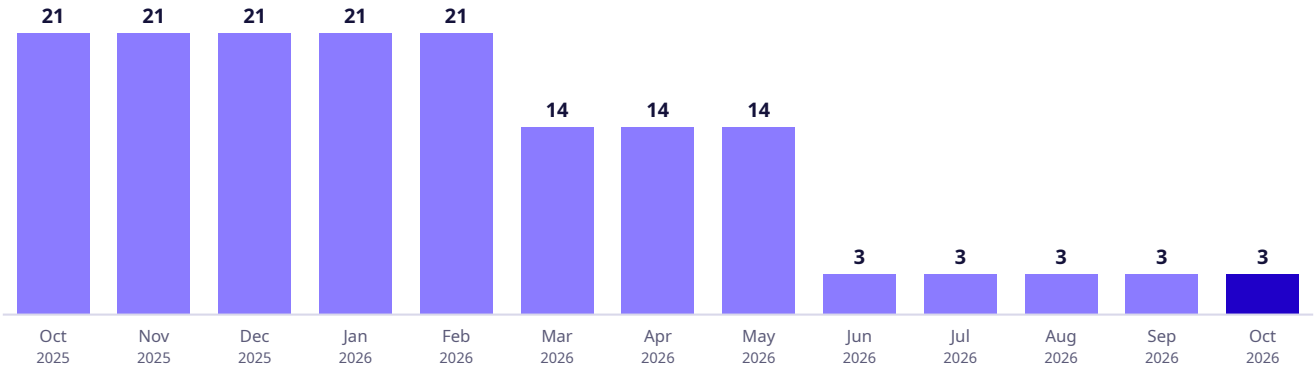
September 2026 had 43 and October 2025 had 31. The 12-month average is 25.7. Volume eased from last month but is still well above the usual level for a team that must patch each one.

Against September 2026, 36 entries is 36 (-7). Against October 2025 it is +16.1%. The busiest day was 20 October 2026 with 6 entries. By part of the month: 1st to 7th, 4; 8th to 14th, 11; 15th to 21st, 9; 22nd to month end, 12.

2. The patching clock

CISA gives each entry a due date. The gap between the day it adds an entry and that date is the window a federal agency has to fix it, and the nearest thing there is to a public benchmark for how fast an exploited flaw should be dealt with.

Median days from CISA adding an entry to its due date, by month



Median of the entries added in each month. Entries with no due date are left out.

October 2026: how long CISA gave

7 days or fewer	**29 entries**
8 to 14 days	**7 entries**
15 to 21 days	**0 entries**
More than 21 days	**0 entries**

The shortest window in October 2026 was 3 days (CVE-2015-3306).

The required-action text on the entries changed in step. 11 June 2026 is the first day CISA's required action cited **BOD 26-04**, its directive on prioritising security updates by risk. 36 of the 36 entries added in October 2026 cite it; by month: Oct 0 of 31, Nov 0 of 11, Dec 0 of 20, Jan 0 of 17, Feb 0 of 28, Mar 0 of 26, Apr 0 of 31, May 0 of 21, Jun 13 of 23, Jul 26 of 26, Aug 31 of 31, Sep 43 of 43, Oct 36 of 36.

Our reading: the trends

The fix window has shortened in steps

The median was 21 days from October 2025 to February 2026, 14 from March to May, and 3 from June onward. Entries with 7 days or fewer went from 0 in October 2025 to 29 in October 2026. This is a steady change, not one odd month. Plan for 3 days as normal.

Volume has stayed high for three months

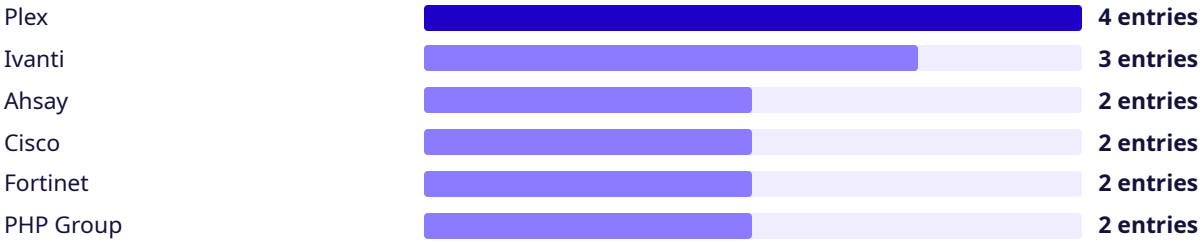
August, September and October 2026 had 31, 43 and 36 entries. The average of the last three months is 33.3, against 25.7 over 12 months. Earlier months ran from 11 to 28. Three months is a short run, so treat it as a warning, not a settled level.

Weakness groups moved, but the counts are small

Files, paths and uploads reached 16.7% of entries, against 7% in the previous three months. Command Injection (CWE-77) had 3 entries, against an average of 0.3. With counts this small, one month is too little to call a trend.

3. Where the pressure was

Vendors with the most entries in October 2026



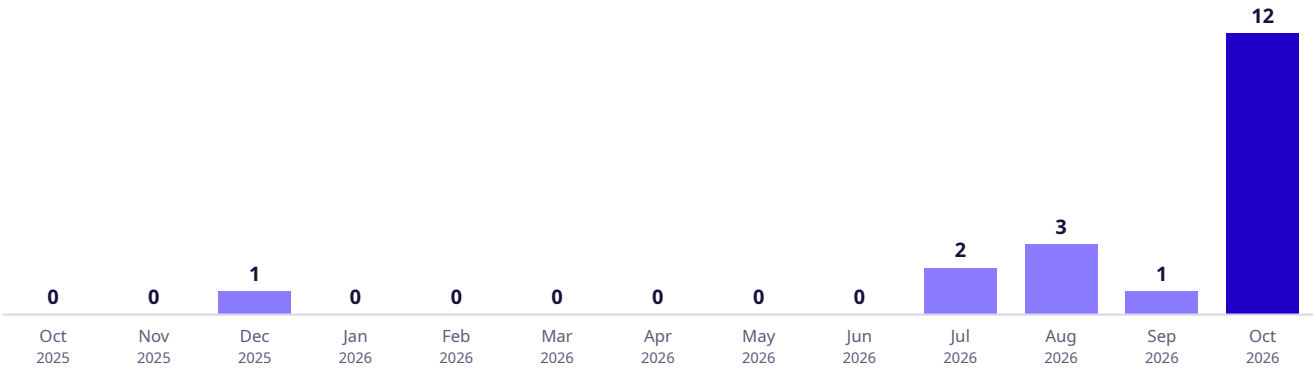
26 different vendors in all. The top three account for 25% of the month's entries.

6 of 36 entries (16.7%) are in products that sit on the network edge or give remote access, against 11.7% over the twelve months before. Those are the products that face the internet by design, which is why a team's inventory matters most there.

Chains: an exploit trend

12 of 36 entries added in October 2026 (33.3%) say in CISA's description that the flaw can be chained with another, against 2.3% over the twelve months before. A chain means fixing one flaw of the set is not the end of the work: the entry flaw gets an attacker in, and the next one gives them more.

Entries whose CISA description names a chain, by month



Oct 0 of 31; Nov 0 of 11; Dec 1 of 20; Jan 0 of 17; Feb 0 of 28; Mar 0 of 26; Apr 0 of 31; May 0 of 21; Jun 0 of 23; Jul 2 of 26; Aug 3 of 31; Sep 1 of 43; Oct 12 of 36. This counts how CISA words its entries, which may not equal what attackers do.

Our reading: the trend

Entries naming a chain were 0 in most months from October 2025 to June 2026, 1 in December 2025, then 2 in July, 3 in August and 1 in September 2026. In October 2026 there were 12 of 36 entries, across 6 chains. That is 33.3%, against 2.3% over 12 months. The count reflects how CISA words its entries and may not equal what attackers do.

The chains of October 2026

Chain	Members	Added	What CISA says
Plex Media Server 4 entries, one product	CVE-2026-96652 CVE-2026-96654 CVE-2026-96655 CVE-2026-96656	20 October	This vulnerability can be chained with CVE-2026-96652, CVE-2026-96654, and CVE-2026-96655. **Our reading:** CISA's descriptions for these four Plex Media Server flaws cover two request-forgery flaws, a way to call other plugins' functions, and a way for an admin user to write files that may be executed on load. CISA says all four chain. Our record names no fixed version here, so patch all four together and limit who can reach the server.
Ivanti Connect Secure 3 entries, one product	CVE-2026-104935 CVE-2026-118527 CVE-2026-111357	13 October over 17 days	This vulnerability can be chained with CVE-2026-104935 and CVE-2026-111357. **Our reading:** CISA says CVE-2026-104935 lets a remote unauthenticated attacker run commands. CVE-2026-118527 then lets an authenticated attacker upload files to a known location, and CVE-2026-111357 lets a local authenticated user escalate privileges. Fix CVE-2026-104935 first, as the entry point. Our note lists 25.1.3.0, 25.1.3.1, 22.8R2.5 and 22.7R2.14 as unaffected.
PHP Group PHP + Linux Kernel 3 entries, across products	CVE-2026-109618 CVE-2026-109619 CVE-2026-46300	26 October over 2 days	This vulnerability can be chained with CVE-2026-109618 and CVE-2026-109619 to implant PHP webshells and run commands as root. **Our reading:** CISA says the two PHP flaws allow unauthenticated remote code execution. It says the Linux kernel flaw CVE-2026-46300 can be chained with them to implant PHP webshells and run commands as root. Fix the two PHP flaws first, as the entry, then the kernel. Our note on the PHP flaws covers fixed versions.
Zammad GmbH Zammad 2 entries, one product	CVE-2026-102489 CVE-2026-102490	2 October	This vulnerability can be chained with CVE-2026-102489. **Our reading:** CISA says the Zammad session fixation flaw can lead to remote code execution as the zammad user. CVE-2026-102490 then lets that local user escalate to root. Fix CVE-2026-102489 first, as the entry. Our note says the vendor treats 7.0 and later as not exploitable in practice, and names no fix for 6.5 or earlier.
Ahsay AhsayCBS 2 entries, one product	CVE-2026-105133 CVE-2026-105134	14 October	This vulnerability can be chained with CVE-2026-105133. **Our reading:** CISA says both AhsayCBS flaws are entry points: an authentication bypass in checkSysPwd, and command injection that runs operating system commands. Together they let a remote attacker get past login and run commands. Fix both at once. Our note names 9.15.2.70 and 10.3.4.45, a vendor hotfix.
Strapi Strapi 1 entries, one product	CVE-2023-22894 also CVE-2023-22621 (not in the catalogue)	8 October	This vulnerability can be chained with CVE-2023-22621 to achieve remote code execution. **Our reading:** CISA says this Strapi flaw lets someone with admin panel access find sensitive user details, and can be chained with CVE-2023-22621 to achieve remote code execution. CVE-2023-22621 is not in this month's list. CISA says the product could be end-of-life. Our record names no fixed version, so check whether your Strapi is supported.

A sample attack path: Ivanti Connect Secure

ENTRY

CVE-2026-104935
Ivanti Connect Secure, added 13 October

Ivanti Connect Secure contains an authentication bypass by spoofing vulnerability that allows a remote unauthenticated attacker to execute arbitrary commands.

Break it here: patch it, or take the product off the internet.

→

MIDDLE STEP

CVE-2026-118527
Ivanti Connect Secure, added 30 October

Ivanti Connect Secure contains a generation of predictable numbers or identifiers vulnerability that allows a remote authenticated attacker to upload files with attacker-controlled content to a known location on disk. This vulnerability can be chained with ...

Break it here: patch it, and check who can reach it.

→

ESCALATION

CVE-2026-111357
Ivanti Connect Secure, added 30 October

Ivanti Connect Secure contains a missing authentication for critical function vulnerability that could allow a local authenticated attacker to escalate their privileges. This vulnerability can be chained with CVE-2026-104935 and CVE-2026-118527.

Break it here: patch the host, and limit who can sign in to it.

→

WHAT CISA SAYS IT GIVES

CISA names these entries as one chain and does not say what it achieves.

Check for it: files and accounts that should not be there (CISA's triage steps 2 and 5).

Illustrative. Built only from the CISA descriptions of CVE-2026-104935, CVE-2026-118527, CVE-2026-111357, read 30 October 2026. It is not a how-to, and the order and the steps in a real incident can differ.

A sample attack path: PHP Group PHP + Linux Kernel

ENTRY

CVE-2026-109618 PHP Group PHP, added 26 October

PHP contains an out-of-memory corruption vulnerability that allows for unauthenticated remote code execution.

CVE-2026-109619 PHP Group PHP, added 26 October

PHP contains a stale internal request-state vulnerability that allows for unauthenticated remote code execution.

Break it here: patch it, or take the product off the internet.

→

ESCALATION

CVE-2026-46300 Linux Kernel, added 28 October

Linux Kernel contains a missing initialization of a variable vulnerability that could allow for unintended modification of page-cache-backed data via failure to preserve the shared-fragment marker during socket buffer coalescing, causing ESP input processing ...

Break it here: patch the host, and limit who can sign in to it.

→

WHAT CISA SAYS IT GIVES

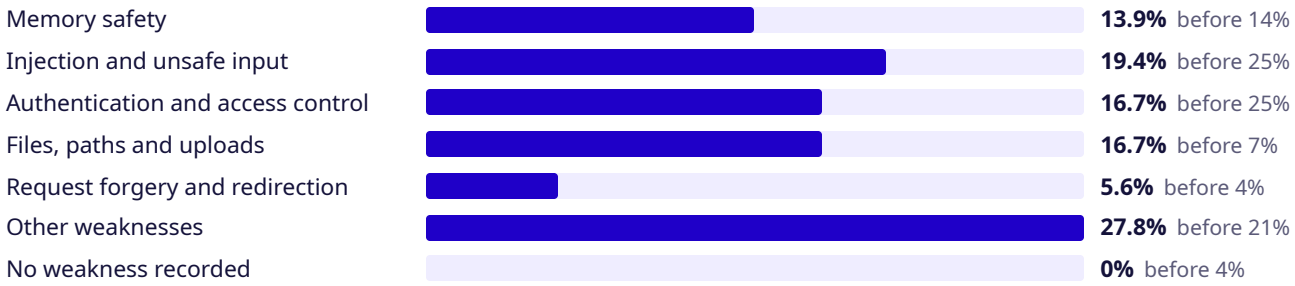
implant PHP webshells and run commands as root

Check for it: files and accounts that should not be there (CISA's triage steps 2 and 5).

Illustrative. Built only from the CISA descriptions of CVE-2026-109618, CVE-2026-109619, CVE-2026-46300, read 30 October 2026. It is not a how-to, and the order and the steps in a real incident can differ.

Weaknesses

Weakness classes, October 2026 against the three months before (share of entries)



An entry falls in the first class that holds one of its CWE ids (Appendix B).

Weakness	Entries	Per month, the three months before
CWE-22 Path Traversal	3	1.3
CWE-77 Command Injection	3	0.3
CWE-78 OS Command Injection	3	2
CWE-290 Authentication Bypass by Spoofing	2	0
CWE-416 Use After Free	2	0.3
CWE-755 Improper Handling of Exceptional Conditions	2	0
CWE-824 Access of Uninitialized Pointer	2	0
CWE-918 Server-Side Request Forgery	2	1.3

How old the flaws are

Of 36 entries, 30 name a CVE from 2026, 1 from the year before, and 5 from three or more years earlier (the oldest, CVE-2015-3306). That is 13.9% against 16.9% over the twelve months before. An old flaw on the list is an unpatched system, not a new discovery.

4. The five entries to know this month

Chosen by a printed rule, not by feel: EPSS 0.90 or more 4 points, 0.50 or more 3, 0.10 or more 2, otherwise 0; named in a chain by CISA 3; network edge or remote access 2; ransomware use known 1. One entry per product; ties go to the higher EPSS, then the lower CVE number. EPSS is FIRST's estimate of the chance of exploitation in the next 30 days, as scored on 31 October 2026; it moves daily.

#	Entry	EPSS	In a chain	Edge	Points
1	Ivanti Connect Secure (CVE-2026-104935)	0.868	yes (+3)	yes (+2)	8 (EPSS 3)
2	PHP Group PHP (CVE-2026-109618)	1.000	yes (+3)	no	7 (EPSS 4)
3	Ahsay AhsayCBS (CVE-2026-105134)	0.818	yes (+3)	no	6 (EPSS 3)
4	Zammad GmbH Zammad (CVE-2026-102489)	0.225	yes (+3)	no	5 (EPSS 2)
5	Linux Kernel (CVE-2026-46300)	0.161	yes (+3)	no	5 (EPSS 2)

1. Ivanti Connect Secure, CVE-2026-104935

What it is. Ivanti Connect Secure contains an authentication bypass by spoofing vulnerability that allows a remote unauthenticated attacker to execute arbitrary commands.

Why it ranks. Added 13 October 2026; CISA gave 3 days; EPSS 0.868; named in a chain with CVE-2026-118527, CVE-2026-111357; a network-edge or remote-access product.

Our reading. Ivanti Connect Secure authentication bypass that lets a remote unauthenticated attacker run commands. It ranks first with 8 points: 3 for EPSS, 3 for chain, 2 for edge. It starts a chain with CVE-2026-118527 and CVE-2026-111357. Anyone running Connect Secure looks first. Our note: find your version, and if it is below 25.1.3.0 on the 25.1 line, patch it and check for compromise.

Our note says. If you run Ivanti Connect Secure, treat this as urgent: CISA's deadline of 16 October 2026 has already passed. First find your version, and if it is below 25.1.3.0 on the 25.1 line, get it patched and checked for compromise.

Fixed in. Unaffected per the record: 25.1.3.0, 25.1.3.1, 22.8R2.5 and 22.7R2.14. No vendor advisory could be read to confirm the fix.

Read our note · Analysis report

2. PHP Group PHP, CVE-2026-109618

What it is. PHP contains an out-of-memory corruption vulnerability that allows for unauthenticated remote code execution.

Why it ranks. Added 26 October 2026; CISA gave 3 days; EPSS 1.000; named in a chain with CVE-2026-109619, CVE-2026-46300.

Our reading. PHP out-of-memory corruption that allows unauthenticated remote code execution. It scores 7 points: 4 for EPSS and 3 for chain. CISA says it chains with CVE-2026-109619 and the Linux kernel flaw CVE-2026-46300 to run commands as root. Anyone running PHP servers looks first. Our note covers fixed versions, how to check a server, and what to do if you cannot patch today.

Our note says. Two critical bugs in PHP itself affect almost every PHP release since 2012. Which versions fix them, how to check a server without being fooled by your package manager, and what to do if you cannot patch today.

Read our note · Analysis report

3. Ahsay AhsayCBS, CVE-2026-105134

What it is. Ahsay AhsayCBS contains a command injection vulnerability that could allow a remote attacker to execute operating system commands via manipulation of the random parameter in the Replication Receiver component's /rps/api/json/UpdateReceivers.do endpoint. This vulnerability can be chained with CVE-2026-105133.

Why it ranks. Added 14 October 2026; CISA gave 3 days; EPSS 0.818; named in a chain with CVE-2026-105133.

Our reading. AhsayCBS command injection that lets a remote attacker run operating system commands. It scores 6 points: 3 for EPSS and 3 for chain, with CVE-2026-105133. Anyone running AhsayCBS looks first. Our note: check your version, and if it is below 9.15.2.70 or 10.3.4.45, ask your provider for the vendor hotfix, which needs a reboot.

Our note says. If you run AhsayCBS, act now: CISA's date of 17 October 2026 has already passed. Check your version, and if it is below 9.15.2.70 or 10.3.4.45, ask your provider for the vendor hotfix today. If you do not run AhsayCBS, you can stop reading.

Fixed in. AhsayCBS 9.15.2.70 and 10.3.4.45 (vendor hotfix, partner login required, reboot after applying; advisory of 12 October 2026).

Read our note · Analysis report

4. Zammad GmbH Zammad, CVE-2026-102489

What it is. Zammad GmbH Zammad contains a session fixation vulnerability that can lead to remote code execution as the zammad user. This vulnerability can be chained with CVE-2026-102490.

Why it ranks. Added 2 October 2026; CISA gave 3 days; EPSS 0.225; named in a chain with CVE-2026-102490.

Our reading. Zammad session fixation that can lead to remote code execution as the zammad user. It scores 5 points: 2 for EPSS and 3 for chain, with CVE-2026-102490, which reaches root. Anyone running Zammad 6.5 or earlier looks first. Our note: move to a supported release. No fix is named for 6.5 or earlier. The vendor says 7.0 and later are not affected in practice.

Our note says. If you run Zammad 6.5 or earlier, act now: CISA's date has already passed. Move to a supported release. If you run 7.0 or later, the vendor says this flaw cannot be exploited there, so you can stop reading.

Fixed in. No fix for 6.5 or earlier is named for this CVE. The vendor says 7.0 and later are not affected in practice, with a hardening change in 7.2.0 (advisory, 5 October 2026).

Read our note · Analysis report

5. Linux Kernel, CVE-2026-46300

What it is. Linux Kernel contains a missing initialization of a variable vulnerability that could allow for unintended modification of page-cache-backed data via failure to preserve the shared-fragment marker during socket buffer coalescing, causing ESP input processing to decrypt shared fragments in place. This vulnerability can ...

Why it ranks. Added 28 October 2026; CISA gave 3 days; EPSS 0.161; named in a chain with CVE-2026-109618, CVE-2026-109619.

Our reading. Linux kernel local privilege escalation. It scores 5 points: 2 for EPSS and 3 for chain. Our note says it was scored 7.8. CISA says it chains with the two PHP flaws to plant a webshell and run commands as root. Anyone running PHP on Linux looks first. Patch it alongside the PHP flaws. Our note sets out the order.

Our note says. A local privilege escalation from May, scored 7.8, was added to CISA's exploited list on 28 October with a three-day deadline. CISA says it can be chained with the two PHP flaws to plant a webshell and run commands as root. What to patch, in what order, and what the chain changes.

Read our note · Analysis report

5. For your next leadership meeting

Questions to put to your IT team or provider

1. Which of our internet-facing systems could we patch within 3 days, and which could not?
2. Do we run Ivanti Connect Secure, AhsayCBS, Zammad, PHP or Plex Media Server, and on which versions?
3. When a vendor names several linked flaws, do we patch every one in the same change?
4. Who can approve an emergency change out of hours, and how long does that take?

What to watch next month

Watch whether the median stays at 3 days and whether entries with 7 days or fewer stay near 29 of 36. Watch whether chained entries stay at 12 or fall back toward the 1 to 3 seen from July to September. Watch whether the edge share stays above 11.7%.

Keep reading on namiq.io

The month is one document; the week and the day are where the next entry shows up first. Each page below links to the notes and the reports for the CVEs it names.

- Weekly highlight and guideline, 1 November 2026
- Daily threat watch, 30 October 2026
- Daily threat watch, 31 October 2026
- Daily CVE highlight, 30 October 2026
- Daily CVE highlight, 31 October 2026
- Today's mission: every exploited vulnerability from the last seven days, in the order their deadlines fall
- All the weekly highlights and guidelines
- The CVE Triage Handbook: how to read a record, find the condition and decide what to do first
- CISA's Known Exploited Vulnerabilities catalogue

What these figures cannot tell you

These figures count CISA's list, not every exploited flaw. They show how CISA words entries and sets deadlines. They say nothing about your own estate or whether you run an affected product.

Sections marked **Our reading** are our interpretation of the figures in this document, checked by code against them. They are not a statement by CISA or any vendor.

Appendix A. Every entry added in October 2026

Where we have written a note on an entry, the CVE links to it and the last column links to its analysis report. Where we have not, the CVE links to the CVE record.

Added	CVE	Vendor and product	Due	Days	Ransomware	Our page
1 October	CVE-2026-104286	Fortinet FortiMail	4 October	3	Not recorded	Note · Report
2 October	CVE-2026-102489	Zammad GmbH Zammad	5 October	3	Not recorded	Note · Report
2 October	CVE-2026-102490	Zammad GmbH Zammad	5 October	3	Not recorded	Note · Report
4 October	CVE-2026-88779	Citrix NetScaler	7 October	3	Not recorded	Note · Report
8 October	CVE-2015-3306	ProFTPD ProFTPD	11 October	3	Not recorded	Note · Report
8 October	CVE-2015-5477	ISC BIND	11 October	3	Not recorded	Note · Report
8 October	CVE-2016-3081	Apache Struts	11 October	3	Not recorded	Note · Report
8 October	CVE-2021-3199	ONLYOFFICE Docs	11 October	3	Not recorded	Note · Report
8 October	CVE-2023-22894	Strapi Strapi	11 October	3	Not recorded	Note · Report
13 October	CVE-2026-104935	Ivanti Connect Secure	16 October	3	Not recorded	Note · Report
13 October	CVE-2026-96951	Microsoft Windows	16 October	3	Not recorded	Note · Report
14 October	CVE-2026-0322	Palo Alto Networks PAN-OS	17 October	3	Not recorded	Note · Report
14 October	CVE-2026-105133	Ahsay AhsayCBS	17 October	3	Not recorded	Note · Report
14 October	CVE-2026-105134	Ahsay AhsayCBS	17 October	3	Not recorded	Note · Report
14 October	CVE-2026-76519	Cisco Secure Email Gateway	17 October	3	Not recorded	Note · Report
15 October	CVE-2026-21589	Atlassian Multiple Products	18 October	3	Not recorded	Note · Report
16 October	CVE-2025-61624	Fortinet Multiple Products	19 October	3	Not recorded	Note · Report
16 October	CVE-2026-102764	BeyondTrust Remote Support	19 October	3	Not recorded	Note · Report
20 October	CVE-2026-106931	EG Secure Solutions SiteGuard Server Edition	23 October	3	Not recorded	Note · Report
20 October	CVE-2026-110936	Siemens Software Center	3 November	14	Not recorded	Note · Report
20 October	CVE-2026-96652	Plex Media Server	3 November	14	Not recorded	Note · Report

20 October	CVE-2026-96654	Plex Media Server	23 October	3	Not recorded	Note · Report
20 October	CVE-2026-96655	Plex Media Server	3 November	14	Not recorded	Note · Report
20 October	CVE-2026-96656	Plex Media Server	23 October	3	Not recorded	Note · Report
23 October	CVE-2026-110447	Collabora Collabora Online – Built-in CODE Server	26 October	3	Not recorded	Note · Report
23 October	CVE-2026-114625	Arista VeloCloud Orchestrator	26 October	3	Not recorded	Note · Report
26 October	CVE-2026-109618	PHP Group PHP	29 October	3	Not recorded	Note · Report
26 October	CVE-2026-109619	PHP Group PHP	29 October	3	Not recorded	Note · Report
27 October	CVE-2026-111497	Google Brotli	10 November	14	Not recorded	Note · Report
27 October	CVE-2026-48356	Adobe Commerce and Magento	10 November	14	Not recorded	Note · Report
28 October	CVE-2026-41709	Broadcom VMware ESX	11 November	14	Not recorded	Note · Report
28 October	CVE-2026-46300	Linux Kernel	31 October	3	Not recorded	Note · Report
29 October	CVE-2026-76418	Cisco Secure Firewall ASA Software and Cisco Secure FTD Software	1 November	3	Not recorded	Note · Report
29 October	CVE-2026-97229	GitLab Community Edition and Enterprise Edition	1 November	3	Not recorded	Note · Report
30 October	CVE-2026-111357	Ivanti Connect Secure	2 November	3	Not recorded	Note · Report
30 October	CVE-2026-118527	Ivanti Connect Secure	13 November	14	Not recorded	Note · Report

Appendix B. Method, definitions and limits

- **Source.** CISA's Known Exploited Vulnerabilities catalogue, 1766 entries as read through 30 October 2026. A month is the date CISA added the entry, in the catalogue's own dates.
- **Window.** The days from the date added to CISA's due date. A median is used so one outlier does not move it. The twelve-month figures are the twelve full months before October 2026.
- **Ransomware.** CISA's own field. "Known" means CISA recorded use; anything else is "not recorded", which is not the same as none.
- **Network edge and remote access.** An entry whose vendor, product or CISA title matches this rule: `firewall|\bvpn\b|gateway|router|secure access|connect secure|\basa\b|\bftd\b|fortigate|fortios|fortiweb|netscaler|big-ip|load balancer|\bsd-wan\b|access point|ssl|remote access|appliance|\bedge\b|zero trust`. It is a keyword rule and will misplace some products.
- **Weakness classes.** By CWE id, an entry in the first class that holds one of its ids: Memory safety (CWE-119, CWE-120, CWE-121, CWE-122, CWE-125, CWE-190, CWE-191, CWE-415, CWE-416, CWE-476, CWE-787, CWE-824); Injection and unsafe input (CWE-20, CWE-74, CWE-77, CWE-78, CWE-79, CWE-88, CWE-89, CWE-90, CWE-91, CWE-94, CWE-95, CWE-98, CWE-502, CWE-611, CWE-917); Authentication and access control (CWE-200, CWE-269, CWE-276, CWE-284, CWE-285, CWE-287, CWE-288, CWE-290, CWE-294, CWE-306, CWE-311, CWE-345, CWE-522, CWE-639, CWE-732, CWE-798, CWE-862, CWE-863, CWE-922); Files, paths and uploads (CWE-22, CWE-23, CWE-36, CWE-59, CWE-73, CWE-434); Request forgery and redirection (CWE-352, CWE-601, CWE-918). Entries with other ids are "Other weaknesses".
- **Age.** The year in the CVE identifier against the year of the month reported. Three years or more earlier counts as old.
- **Chain.** An entry whose CISA description contains the word chain, chained or chaining. Entries that name each other are grouped into one chain; a CVE named but not in the catalogue is listed as such. The order of the steps in a sample path (entry, middle, escalation) follows a keyword rule on CISA's wording: "unauthenticated", "authentication bypass", "session fixation" or "remote attacker" for entry; "escalate", "privilege" or "as root" for escalation. It shows how CISA describes the flaws, not a reconstruction of an attack. The count of entries naming a chain reflects how CISA words its entries and may not equal what attackers do.
- **The five entries.** EPSS 0.90 or more 4 points, 0.50 or more 3, 0.10 or more 2, otherwise 0; named in a chain by CISA 3; network edge or remote access 2; ransomware use known 1. One entry per product; ties go to the higher EPSS, then the lower CVE number. The weights are ours and are a choice, not a measurement. EPSS is FIRST's public score file as produced on the date shown.
- **Figures** are public, directional and not audited. Percentages are rounded to one decimal. A small month moves them a long way.
- **This is not** a statement about your estate, a forecast of attacks, legal advice or an attestation of any kind.

Sources

- CISA Known Exploited Vulnerabilities catalogue: cisa.gov/known-exploited-vulnerabilities-catalog
- CISA BOD 26-04, Prioritizing Security Updates Based on Risk: cisa.gov/news-events/directives
- CWE, MITRE: cwe.mitre.org