CYBERSECURITY RISK ADVISORY

PHP2Shell: Critical Remote Code Execution Flaws in PHP (CVE-2026-109618, CVE-2026-109619)

All sectors · Any organization running websites or applications on PHP, directly or through hosting providers and vendor products

ADVISORY ID	PUBLISHED	CLASSIFICATION	SEVERITY
SCA-ADV-2026-001	October 21, 2026 · v1.4 (updated November 19)	TLP:CLEAR	Critical

STATUS

Actively exploited · in CISA KEV

Developing situation. This advisory reflects public information as of **November 19, 2026, 12:00 PM Eastern Time**. **What changed in v1.4:** PHP fixed the third flaw, CVE-2026-115560, in PHP 8.5.13, 8.4.28, 8.3.37 and 8.2.36, released November 19 together with more than ten other security fixes.[29] Check Point reported that attackers used PHP2Shell to break into Check Point Security Gateways through their Mobile Access portals, gained root through a Check Point flaw (CVE-2026-123039), and at some victims destroyed files on VMware ESXi hosts; CISA added that flaw to its Known Exploited Vulnerabilities catalog on November 13.[5] [30] [31] CISA's catalog also marks both PHP2Shell CVEs as requiring a forensic triage, a check for prior compromise, under its directive BOD 26-04.[5] [32] Details are changing quickly, so each fact carries a numbered citation [1] that links to its source in Appendix A, and claims are attributed to the organization that made them. We deliberately leave out exploit details. TLP:CLEAR means this advisory may be shared without restriction.[16]

1. Executive summary

On October 21, 2026, the PHP project released emergency updates for two critical vulnerabilities in the PHP engine itself, nicknamed **PHP2Shell**. Both are rated **9.2 (Critical) under CVSS v4.0** by the PHP project; some early reports cited 10.0.[1] [4] [11] They can let an

attacker run code on a web server **without logging in**. In the riskiest configuration, a single request can trigger the attack before any website code runs.[1] Details leaked before the planned disclosure. Attacks followed within hours, and on October 26 researchers confirmed a successful takeover of a test server in the wild.[19] [21] The U.K. NCSC and CERT-EU have urged immediate patching or isolation, and CISA issued an alert calling for immediate patching.[2] [3] [4] [8] [9] CISA has since listed both flaws as known exploited, and attackers have used them against firewall management interfaces, combining them with a Linux kernel flaw to take full control.[5] [22] [23] In November, Check Point reported that attackers used them to break into its security gateways and, at some victims, to wipe servers; on November 19 PHP fixed a related third flaw.[29] [30]

Bottom line for executives

- **If you run PHP, assume you are affected.** The PHP project says every installation serving web requests is in scope, which includes WordPress, Drupal, Magento, Joomla and Laravel sites.[1] [13]
- **Patching is the only real fix.** Update to PHP 8.5.13, 8.4.28, 8.3.37 or 8.2.36, released November 19: they include the PHP2Shell fixes and also fix the third flaw and other serious bugs. Configuration workarounds reduce risk but, in the PHP project's words, do not make an installation safe.[1] [29]
- **If you can't patch today, take it offline or isolate it.** That is the guidance from CERT-EU and the U.K.'s National Cyber Security Centre, and several European governments took public websites offline as a precaution.[3] [4] [15]
- **Check firewalls and appliances, not just websites.** Internet-exposed Palo Alto Networks PAN-OS management interfaces were attacked through PHP2Shell, and Panorama is also affected; install the PAN-OS or Panorama hotfix and keep management interfaces off the internet.[23] [24] [26]
- **Patch Linux kernels too.** Attackers paired PHP2Shell with Fragnesia (CVE-2026-46300), a Linux kernel flaw that turns a web foothold into root access. CISA lists it as exploited.[5] [22]
- **Check Point gateways were attacked too.** Attackers used PHP2Shell through Mobile Access portals, then a Check Point flaw to gain root, and wiped files on a VMware ESXi host at some victims. Install the Check Point Jumbo Hotfix that fixes CVE-2026-123039 and check for compromise.[30] [31]

- **The third flaw is now fixed.** PHP fixed CVE-2026-115560 in its November 19 releases. Until you install them, keep session upload progress off (`session.upload_progress.enabled=0`).[17] [18] [29]
- **A patch is not proof you are clean.** CISA requires federal agencies to carry out a forensic triage, a check for whether systems were already compromised, for both PHP2Shell flaws. Do the same for any PHP system or appliance that was exposed before you patched.[5] [32]

2. What happened

WHEN (2026)	EVENT	SOURCE
Oct 17	Amazon Threat Intelligence recorded an exploit attempt against one of its honeypots, four days before public disclosure. It could not explain how the actor got exploit details during the embargo.	[19]
Oct 20	A post claiming two critical PHP flaws would be disclosed on October 22 appeared online and was taken down, but screenshots spread. Researchers at watchTowr said the flaws were real and under embargo.	[12] [14]
Oct 20, 19:33 UTC	The PHP security team announced an emergency release for October 21 at 14:00 UTC, a day earlier than the original embargo, addressing two flaws rated CVSS v4.0 9.2.	[1] [12]
Oct 20–21	CERT-EU published Security Advisory 2026-018, advising organizations to patch immediately or "consider isolating internet-facing applications from public networks until a fix can be applied."	[4]
Oct 21, 07:34 UTC	WordPress security firm Patchstack said hosting partners had reported multiple active exploitation incidents to it, before the official patch.	[13]
Oct 21	PHP released 8.5.12, 8.4.27, 8.3.36 and 8.2.35 with a security advisory urging users to update now.	[1]
Oct 21	The U.K. NCSC issued an alert, and CISA published "Critical Vulnerabilities in PHP Require Immediate Patching." Cloudflare said it was seeing early attacks and deployed protective firewall rules for all customers.	[2] [3] [7] [8]
Oct 21	Government bodies in the Netherlands, Finland, Denmark, France, Germany and Belgium took some websites and services offline as a precaution, according to news reports.	[15]
Oct 22	watchTowr reported in-the-wild exploitation of both CVEs, first seen by its honeypots on October 21.	[9]

WHEN (2026)	EVENT	SOURCE
Oct 23	PHP warned of a third flaw, CVE-2026-115560, not fixed by the October 21 releases. It needs an unusual combination of settings and application code, and PHP will fix it in its next regular release. The Canadian Centre for Cyber Security updated its alert.	[17] [18]
Oct 23–24	According to security firm Dream, an attacker used a custom PHP2Shell exploit and the Fragnesia kernel flaw to gain root on servers in the U.S., Japan, Taiwan and South Korea, 25 in all. Exploitation began on October 23; three of the servers were in a U.S. government-affiliated environment: firewalls rooted on October 23 and 24, and an internal server the attacker then reached through a tunnel.	[22] [24]
Oct 26	A researcher reported confirmed remote code execution against a honeypot running PHP 8.4.26 with Apache mod_php, and an Expel researcher called it the strongest confirmation of in-the-wild exploitation so far. The researcher noted the honeypot was set up to be easy to attack, so it does not show how reliable the exploit is elsewhere.	[21]
Oct 26	CISA added CVE-2026-109618 and CVE-2026-109619 to its Known Exploited Vulnerabilities catalog, with a federal due date of October 29.	[5] [22]
Oct 28	Palo Alto Networks updated its advisory to confirm active exploitation against PAN-OS management interfaces exposed to the internet. CISA added Fragnesia (CVE-2026-46300) to the KEV catalog, noting it can be chained with PHP2Shell to plant web shells and run commands as root.	[5] [22] [23] [26]
Oct 29–30	Reporting on Dream's research identified the targets as Palo Alto Networks firewalls running PAN-OS, and Palo Alto Networks' Unit 42 team independently verified the attacker's tools and confirmed Dream's results. PAN-OS fixes were available for all affected branches by October 30, according to The Hacker News.	[23] [24]
Oct 30 – Nov 2	According to Check Point Research, an attacker exploited unpatched Check Point Security Gateways through their Mobile Access portals with PHP2Shell, beginning October 30 against Israeli organizations, with destructive activity against some of them. A broader second wave on November 2 hit organizations in several countries, with no evidence of destructive activity.	[30]
Nov 8–12	Check Point published support article sk1000362 for CVE-2026-123039, a flaw that lets code already running on a gateway gain root, saying it had observed an active exploit "against a couple of dozen customers." Check Point Research published its analysis of the campaign on November 12.	[30] [31]
Nov 10–17	A November check found PHP's official releases were still the October 21 builds; as of November 17, PHP's source repository showed only release candidates (8.5.13RC1, 8.4.28RC1, 8.6.0RC7) after those builds, so CVE-2026-115560 remained without a fix release.	[28]

WHEN (2026)	EVENT	SOURCE
Nov 13	CISA added CVE-2026-123039 to its Known Exploited Vulnerabilities catalog, with a federal due date of November 16, and marked it as requiring forensic triage.	[5]
Nov 19	PHP released 8.5.13, 8.4.28, 8.3.37 and 8.2.36, fixing CVE-2026-115560 and more than ten other security issues, including others that PHP says can lead to remote code execution. The new major version, PHP 8.6.0, released the same day, also includes the fix.	[29]

3. The vulnerabilities

Both flaws involve how PHP handles memory when a request ends abnormally.[8] The PHP project describes them as follows.[1] They were found by researchers at Calif, Wiz and OpenAI.[8]

CVE	WHAT GOES WRONG	SEVERITY	ACCESS NEEDED	IMPACT
`CVE-2026-109618`	Running out of memory can interrupt PHP while internal request data is only partly set up; cleanup may then treat that invalid data as valid.	CVSS v4.0 9.2	None (unauthenticated, over the network)	Remote code execution
`CVE-2026-109619`	Internal state belonging to one request can survive after its memory is freed, and a later request on the same worker may use it before it is reset.	CVSS v4.0 9.2	None (unauthenticated, over the network)	Remote code execution

- **Who's affected:** all PHP installations that serve web requests, including PHP-FPM, Apache with mod_php, php-cgi, FrankenPHP and LiteSpeed.[1] [7]
- **Highest risk:** Apache with mod_php, where "an unauthenticated request can trigger the attack before any application code runs."[1]
- **Default settings help attackers:** one confirmed attack path relies on a PHP feature (session upload progress) that is on by default, but watchTowr notes it is not the only path.[9]
- **Related flaw, CVE-2026-115560 (Oct 23):** affects applications that switch PHP's session serialization handler at runtime while session upload progress is on. PHP calls this setup unlikely and recommends `session.upload_progress.enabled=0`. That setting was already advised for CVE-2026-109619, so keep it if you applied it.[17] [18] No fixed PHP release had

been published as of November 17, 2026.[28] No exploitation of it had been reported when it was disclosed.[17]

- **Hidden PHP counts too:** many appliances, control panels and vendor products include PHP. The NCSC advises watching for updates from those vendors.[3] Palo Alto Networks firewalls and Panorama are a confirmed example: their management web interface and XML API run a vendor-supplied PHP, and Palo Alto says traffic passing through the firewall is not affected.[23] [26]
- **Fragnesia (CVE-2026-46300):** a Linux kernel flaw, rated CVSS 7.8, disclosed with a public proof of concept on May 13, 2026, that lets a local user become root; fixed distribution kernels began shipping in mid-May. On its own it needs local access; PHP2Shell supplies that access. BleepingComputer reports that kernels released before May 13, 2026 are affected, but not every older kernel is (Red Hat, for example, says RHEL 6 and 7 are not), so check your distribution's advisory. The fix is a kernel update.[22] [27]

4. Affected and fixed versions

PHP BRANCH	VULNERABLE	FIXED IN	NOTES
8.5	8.5.11 and earlier	`8.5.12` · **`8.5.13`**	Supported
8.4	8.4.26 and earlier	`8.4.27` · **`8.4.28`**	Supported
8.3	8.3.35 and earlier	`8.3.36` · **`8.3.37`**	Supported
8.2	8.2.34 and earlier	`8.2.35` · **`8.2.36`**	Reaches end of life December 31, 2026; plan an upgrade.[1]
8.1, 8.0, 7.4	All	No official release	The PHP project no longer supports these. It published minimal source patches for those building from source; Linux distributions and long-term support vendors may offer backported packages.[1] [7] [8]
7.3 and older	All	None	Unsupported. Upgrade or isolate.[9]

PHP2Shell (CVE-2026-109618, CVE-2026-109619) is fixed from the October 21 releases. CVE-2026-115560 and the other flaws fixed on November 19 need the newer releases (in

bold), which we recommend. PHP 8.6.0 also includes the fixes.[1] [29]

Version table from the PHP project and Plesk's advisory.[1] [6] **Plesk users:** Plesk has released fixed Linux and Windows PHP builds, and fixes for its own internal PHP engine (sw-engine) are out in 18.0.81 Update 4 and 18.0.80 Update 11. Its older 7.4, 8.0 and 8.1 builds are fixed only if built on October 21, 2026.[6]

Palo Alto Networks PAN-OS and Panorama: PAN-OS 10.2, 11.1, 11.2, 12.1 and 12.2 are affected. PAN-OS 12.2 is fixed in 12.2.4-h1 or later; other branches need the hotfix Palo Alto lists for each maintenance release, and fixes for all branches were out by October 30. GlobalProtect portal, gateway and Clientless VPN are not affected.[23] [26]

Check Point: CVE-2026-123039 affects R82.20, R82.10, R82, R81.20, R81.10 and R81 on Check Point Force Firewalls, Management and Log Servers, Multi-Domain servers and Maestro Orchestrator; Spark Firewalls and Smart-1 Cloud are not affected. It is fixed in the Jumbo Hotfix Accumulator for R82.20 from Take 14, R82.10 from Take 52, R82 from Take 132 and R81.20 from Take 174; Check Point lists R81 and R81.10 as end of support. Its interim mitigation is to stop the `dynamic_server` process, which disables Dynamic CLI commands.[31] Check Point Research says the late-October attacks began about a week after a security fix became available.[30]

5. Exploitation and exposure

- **Before the patch:** watchTowr and Huntress said they had not seen in-the-wild exploitation, and Check Point reported none at the time, although exploit-tool screenshots and proof-of-concept code were circulating.[12] [14]
- **Now:** Cloudflare's CTO said the company was seeing early attacks against both flaws; Patchstack said hosting partners reported multiple exploitation incidents to it.[8] [13] As of October 22, watchTowr reports in-the-wild exploitation of both CVEs, and Amazon says the flaws are now broadly exploited.[9] [11]
- **Confirmed success (Oct 26):** a honeypot running PHP 8.4.26 with Apache mod_php was taken over through remote code execution, the first high-quality confirmation of a working attack in the wild. Before that, Dataminr had described activity as scanning and non-working exploits.[21]
- **Hard to spot:** Amazon saw a probe on October 17, before disclosure, and several threat actors attempting exploits from October 21. CrowdStrike notes exploitation leaves few traces because application code never runs.[19]

- **CISA's Known Exploited Vulnerabilities catalog:** CISA added CVE-2026-109618 and CVE-2026-109619 on October 26, 2026 (federal due date October 29), Fragnesia (CVE-2026-46300) on October 28 (due October 31), and Check Point's CVE-2026-123039 on November 13 (due November 16). CISA marks all four as requiring forensic triage. CVE-2026-115560 is not listed. Ransomware use is recorded as "Unknown" for all four.[5]
- **Targeted campaign against firewalls:** Dream reports that a suspected China-nexus actor rooted 25 servers, mostly firewalls, starting October 23, then deployed web shells, opened reverse SSH tunnels, took an LDAP service-account password and ran password spraying and reconnaissance against Active Directory. Palo Alto Networks' Unit 42 independently verified the tooling.[24] [26]
- **Check Point gateways and destructive attacks:** Check Point Research reports that after PHP2Shell access and root through CVE-2026-123039, the attacker planted web shells and a persistent backdoor (TSGA, with a hidden proxy component) that can tamper with firewall logs and persist through backups and snapshots, scanned the internal network, moved over SSH to a VMware ESXi host and ran a wiper, leaving a politically themed note. The tools match a malware family previously linked to a China-nexus group, but Check Point says the evidence does not allow a high-confidence assessment of who was behind it or why.[30]

22.6 million
exposed instances potentially vulnerable, per Palo Alto Networks telemetry[10]

5.1 million+
PHP hosts exposed online, per VirusTotal[8]

25
servers rooted in one PHP2Shell + Fragnesia campaign, per Dream[24]

~884,000
internet-facing hosts advertising PHP 8.1 or older (no upstream fix), per Mallory via Check Point (Shodan banners, Oct 20)[12]

These counts use different methods and mostly rely on what servers advertise.[12] They show the scale of exposure, not confirmed vulnerable or compromised systems.

6. Business risk

- **Server takeover:** remote code execution gives an attacker the same control over the server as the web application, which can expose databases, credentials, customer data and connected systems.
- **Persistence:** attackers commonly plant web shells and backdoors that survive patching. Patching alone does not remove an attacker who is already in, which is why the NCSC advises checking exposed systems for signs of compromise, including backdoors, before or while patching.[3]
- **Third-party exposure:** the NCSC warns that vendor products bundling PHP may be affected.[3] Hosting providers and SaaS vendors that run PHP may also hold your data even if you don't run PHP yourself, so ask them.
- **Reporting obligations:** if data was accessed, breach-notification laws, regulators, contracts and cyber insurance policies may set short deadlines. Involve counsel early.

7. Recommended actions

Today

1. **Find every PHP system**, starting with internet-facing ones and not only old versions.[3]
2. **Update** to 8.5.13, 8.4.28, 8.3.37 or 8.2.36 (November 19), then **restart all PHP workers** so the fix takes effect. If you are still on the October 21 builds, they fix PHP2Shell but not the third flaw.[1] [9] [29]
3. **If you can't patch:** isolate the system from the internet or take it offline until it is fixed.[3] [4] Apply the PHP project's interim settings only as a stopgap.[1]
4. **Turn off session upload progress** (`session.upload_progress.enabled=0`) on any server not yet on the November 19 releases, which fix CVE-2026-115560.[17] [18] [29]
5. **Ask your hosting provider and vendors** (control panels, appliances, SaaS) whether they are patched.[3] [6]
6. **Palo Alto Networks customers:** install the PAN-OS or Panorama hotfix for your release and allow management access only from trusted internal addresses, including any data-plane interface with a management profile.[23] [26]
7. **Check Point customers:** install the Jumbo Hotfix take listed in sk1000362 for your version, then confirm `/tmp/dynamic_socket` shows `0660` permissions, as Check Point describes. Prioritize gateways with an internet-facing Mobile Access portal.[30] [31]

Within 72 hours

1. **Preserve evidence first:** keep logs, configuration snapshots and suspicious files before cleanup.[9]
2. **Run a forensic triage** on every system that was exposed before you patched. CISA requires this of federal agencies for these flaws because a patch does not show whether an attacker got in first.[5] [32]
3. **Hunt for compromise** on any system exposed before patching: web shells, unexpected scheduled tasks, new accounts tied to PHP processes.[3] [9]
4. **Restrict outbound traffic** from web servers and alert when a web server process starts a command shell.[12]
5. **On Check Point gateways that ran Mobile Access,** run the log checks in sk1000362 and look for the files Check Point Research lists. Check backups and snapshots before restoring from them, since Check Point says the backdoor can persist through them, and treat firewall logs on a suspect gateway as possibly altered.[30] [31]
6. **If a firewall's management interface was exposed,** rotate credentials it stores or uses, such as LDAP service and administrator accounts, and look for password spraying and new accounts in Active Directory.[26]
7. **If you find signs of compromise,** treat it as an incident: contain, engage incident

8. **Update Linux kernels** on PHP servers and appliances to versions that fix Fragnesia (CVE-2026-46300).[22] [27]
9. **Use a web application firewall as a short-term shield** where available; Cloudflare's rules cover all plans, including free. It does not replace patching.[7] [8]

response support, and check notification obligations.

Strategic

1. **Retire unsupported PHP** (8.1 and older) and schedule PHP 8.2 upgrades before its December 31, 2026 end of life.[1]
2. **Keep a live software inventory**, including components inside vendor products, so the next zero-day can be scoped in hours.
3. **Set patch deadlines** for critical internet-facing flaws, and track CISA's KEV catalog.[5]
4. **Rehearse the "can't patch" decision:** who can take a public website offline, and how fast.

8. What to watch for

- New or modified `.php` files in web roots, upload or cache folders.[9] [12]
- Web server or PHP processes (for example `php-fpm`, `httpd`, `apache2`) starting command shells or unexpected programs.[12]
- Unexpected scheduled tasks, new user accounts, or outbound connections from web servers.[9] [12]
- Unexpected outbound SSH from firewalls, appliances or web-facing servers, and web server or PHP processes calling `su` or spawning root shells. Rescana notes the reported Fragnesia tampering (of `/etc/pam.d/su`) happens in memory, so disk-based file-integrity checks may miss it.[26] [27]

- On Check Point gateways: commands in `/var/log/dynamicCli.log` that lack the normal Clish wrapper; `zz*.tpl` files in the Mobile Access templates folder; `slot_CPconfigdaemon` or `/lib/libcpfwcommon.so`; connections involving `130.94.19[.]204` or `130.94.19[.]168`. On VMware ESXi hosts: SSH logins by `vpxuser` from a gateway and files named `DREAM_ANNEXATION.txt`.[30] [31]
- Unusual file-upload style requests (multipart/form-data) to pages that never accept uploads. Check Point rates the early research on this pattern as low confidence, so treat it as a lead, not proof.[12]

9. Questions for leadership

1. Do we know every place PHP runs, including hosting providers and vendor products?
2. Are all internet-facing PHP systems patched or isolated today, and who confirmed it?
3. For systems exposed before patching, have we checked for signs of compromise?
4. Which of our vendors and service providers have confirmed they are patched?
5. Are any firewall or appliance management interfaces reachable from the internet, and are their kernels patched for Fragnesia?
6. Do we run Check Point gateways with Mobile Access, and are they on the fixed Jumbo Hotfix?
7. Are all PHP servers on the November 19 releases, which also fix the third flaw?

Appendix A. Source map

Every citation, traced to its publisher. Sources were opened and checked on October 21, 2026, new or updated ones on October 25 and 26, 2026, new ones for v1.3 on November 17, 2026, and new ones for v1.4 on November 19, 2026, each round followed by an independent fact-check, except where noted.

#	WHAT IT SUPPORTS	SOURCE	TYPE	LINK
1	Advance notice (Oct 20, which gives the CVSS v4.0 9.2 rating); security advisory and releases (Oct 21); flaw descriptions; affected installations; mod_php risk; fixed versions; interim settings "do not make an installation safe"; 8.1 and older unsupported; 8.2 end of life	The PHP Group, php.net news archive	Vendor (official)	php.net

#	WHAT IT SUPPORTS	SOURCE	TYPE	LINK
2	CISA alert "Critical Vulnerabilities in PHP Require Immediate Patching," October 21, 2026 (title and date; the page could not be loaded from our environment)	Cybersecurity and Infrastructure Security Agency (CISA)	U.S. government	cisa.gov
3	Alert of Oct 21: update, temporary mitigations, consider taking systems offline; inventory and prioritize internet-facing systems; vendor products bundling PHP; check for backdoors	U.K. National Cyber Security Centre (NCSC)	U.K. government	ncsc.gov.uk
4	Security Advisory 2026-018 (first released Oct 20, 2026): CVSS 9.2; patch immediately; consider isolating internet-facing applications from public networks	CERT-EU (Cybersecurity Service for the EU institutions)	EU	cert.europa.eu
5	KEV catalog version 2026.11.18, checked Nov 19 via CISA's official kev-data repository: CVE-2026-109618 and -109619 added Oct 26 (due Oct 29); CVE-2026-46300 added Oct 28 (due Oct 31) with a note that it chains with PHP2Shell; CVE-2026-123039 (Check Point) added Nov 13 (due Nov 16); all four marked "forensicTriage: Yes" under BOD 26-04; CVE-2026-115560 not listed; ransomware use "Unknown"; federal fix deadlines for listed entries	CISA Known Exploited Vulnerabilities catalog, via official kev-data repository	U.S. government	cisa.gov · data
6	Affected and fixed version table; fixed Linux and Windows builds; internal engine (sw-engine) fixed in 18.0.81 Update 4 and 18.0.80 Update 11 (article updated Oct 22)	Plesk support article	Vendor	support.plesk.com
7	Affected server types; source backports for 7.4, 8.0, 8.1; Cloudflare WAF rules on all plans	Help Net Security, Oct 21, 2026	Security news	helpnetsecurity.com
8	Researchers (Calif, Wiz, OpenAI); Cloudflare CTO on early attacks; Cloudflare WAF rules; VirusTotal exposure estimate	BleepingComputer	Security news	bleepingcomputer.com

#	WHAT IT SUPPORTS	SOURCE	TYPE	LINK
9	In-the-wild exploitation of both CVEs, first observed Oct 21 (page updated Oct 22); session upload progress attack path; restart workers; preserve evidence; compromise checks; unsupported versions	watchTowr Labs	Security vendor	watchtowr.com
10	22.6 million exposed instances potentially vulnerable	Palo Alto Networks Unit 42 threat brief	Security vendor	unit42.paloaltonetworks.com
11	Background FAQ (updated Oct 23): early reports of a 10.0 score; Amazon's report of broad exploitation; neither CVE in KEV as of Oct 23; timeline;	Tenable	Security vendor	tenable.com
12	Leak timeline; PHP notice at 19:33 UTC; no in-the-wild exploitation at time of writing; ~884,000 hosts (Mallory); detection and network controls; low-confidence request pattern	Check Point Research blog (published before the patch)	Security vendor	blog.checkpoint.com
13	Exploitation incidents reported to Patchstack by hosting partners (07:34 UTC, Oct 21); affected PHP applications	Patchstack	Security vendor	patchstack.com
14	Pre-patch status from watchTowr and Huntress; later reports of exploitation attempts	SecurityWeek	Security news	securityweek.com
15	Precautionary takedowns by government bodies in six countries, summarizing Reuters and Dutch media reporting	Safeguard (summary of news reports)	Secondary summary	safeguard.sh
16	TLP:CLEAR definition; Traffic Light Protocol 2.0	FIRST	Standards body	first.org
17	CVE-2026-115560 (Oct 23): conditions, no patch yet, mitigation session.upload_progress.enabled=0, fix in next regular release, no exploitation reported	BleepingComputer, Oct 23, 2026	Security news	bleepingcomputer.com

#	WHAT IT SUPPORTS	SOURCE	TYPE	LINK
18	Alert AL26-026, Update 1 (Oct 23): CVE-2026-115560 not fixed by the Oct 21 updates; disable session upload progress	Canadian Centre for Cyber Security	Canadian government	cyber.gc.ca
19	Amazon's Oct 17 pre-disclosure probe and Oct 21 attempts by multiple actors; CrowdStrike on few traces	The Hacker News, Oct 22, 2026	Security news	thehackernews.com
21	Confirmed remote code execution on a honeypot (PHP 8.4.26, Apache mod_php) reported Oct 26; Expel researcher's confirmation; earlier Dataminr assessment; CISA detection rule but no KEV listing (as of Oct 26); CVE-2026-115560 still unpatched (as of Oct 26)	BleepingComputer, Oct 26, 2026	Security news	bleepingcomputer.com
22	CISA's Oct 28 KEV addition of Fragnesia (CVE-2026-46300) and its chaining note; PHP2Shell KEV listing; Fragnesia background (XFRM ESP-in-TCP, root, public proof of concept, kernels before May 13, 2026); Dream's 25-server campaign	BleepingComputer, Oct 29, 2026	Security news	bleepingcomputer.com
23	Palo Alto Networks' advisory as summarized (Palo Alto's own page could not be loaded from our environment): active exploitation of internet-exposed PAN-OS management interfaces; affected PAN-OS branches; 12.2.4-h1 fix; patches for all branches as of Oct 30; GlobalProtect portal, gateway and Clientless VPN not affected; restrict management access; Unit 42 verification	The Hacker News (Ravie Lakshmanan), Oct 29, 2026, updated with patch status as of Oct 30	Security news	thehackernews.com
24	Dream's findings: custom PHP2Shell exploit plus Fragnesia; 25 servers rooted in four countries; exploitation from Oct 23, government-affiliated firewalls rooted Oct 23 and 24 and an internal server reached by tunnel; PAN-OS 12.1 and 12.2 targeted; Unit 42 verification	The Register (Jessica Lyons), Oct 29, 2026	Security news	theregister.com

#	WHAT IT SUPPORTS	SOURCE	TYPE	LINK
26	Palo Alto's Oct 28 confirmation; management web UI and XML API affected, pass-through traffic not affected; Panorama affected; data-plane management profiles; 12.2.4-h1; post-compromise activity (web shells, reverse SSH tunnels, LDAP password, Active Directory spraying); credential rotation and hunting guidance	Field Effect, Oct 30, 2026	Security vendor	fieldeffect.com
27	Fragnesia severity (CVSS 7.8), local-access requirement, May 13, 2026 disclosure with public proof of concept, distribution fixes from May 15; RHEL 6 and 7 not affected; KEV listing Oct 28; in-memory tampering and hunting guidance	Rescana (published after Oct 29, 2026)	Security vendor	rescana.com
28	PHP release tags checked Nov 17, 2026: latest final releases 8.5.12, 8.4.27, 8.3.36, 8.2.35 (Oct 21); later tags are release candidates only (8.5.13RC1 dated Nov 3, 8.4.28RC1 dated Nov 4, 8.6.0RC7 dated Nov 11)	The PHP Group, official php-src source repository (tags)	Vendor (official)	github.com
29	Release notes (NEWS) for PHP 8.5.13, 8.4.28, 8.3.37 and 8.2.36, dated Nov 19, 2026, checked Nov 19: CVE-2026-115560 ("Session serializer mismatch can lead to remote code execution") fixed in all four, with more than ten other security fixes, including others described as able to lead to remote code execution; PHP 8.6.0 (Nov 19) also lists the fix	The PHP Group, official php-src source repository (release tags and NEWS)	Vendor (official)	github.com

#	WHAT IT SUPPORTS	SOURCE	TYPE	LINK
30	"PHP2Shell Exploitation on Check Point Gateway" (Nov 12, 2026), read Nov 19: waves of Oct 30 and Nov 2; Mobile Access portals; CVE-2026-123039 to root; web shells; TSGA backdoor and TSProxy (backup and snapshot persistence, firewall-log tampering); SSH to ESXi as vpxuser; destroy_v6 wiper and DREAM_ANNEXATION.txt note; fix available about a week before the attacks; attribution assessment; indicators	Check Point Research	Vendor (official research)	research.checkpoint.com
31	sk1000362, "CVE-2026-123039 – Local privilege escalation to root in the DynamicCLI process" (created Nov 8, modified Nov 12, 2026), read Nov 19: active exploit against "a couple of dozen customers"; CVSS 7.8; affected and non-affected products and versions (R81 and R81.10 end of support); fixed Jumbo Hotfix takes; interim mitigation; log checks; 0660 socket permission check	Check Point Support Center	Vendor (official)	support.checkpoint.com
32	BOD 26-04, "Prioritizing Security Updates Based on Risk" (June 10, 2026), read Nov 19: "& forensic triage" means an agency must remediate within three days and "carry out a forensic triage of the asset to assess whether the system is compromised"; supersedes BOD 22-01 and BOD 19-02	Cybersecurity and Infrastructure Security Agency (CISA)	U.S. government	cisa.gov

This advisory summarizes public information for awareness and planning. It is not legal advice and does not replace guidance from your vendors or incident responders. Need help assessing exposure? Contact advisors@stratcyberadvisors.com.