



PHP's Critical Security Release and Your Joomla or WordPress Site

A critical PHP security release is due on 21 October 2026, fixing two CVSS 9.2 flaws. Whether your Joomla or WordPress site gets it is down to your host.

Phil E. Taylor | 20 October 2026

The PHP security team has posted [advance notice of a critical security release](#), due on Wednesday 21 October 2026 at 14:00 UTC. It fixes two vulnerabilities, both rated CVSS v4.0 9.2. PHP is holding back the details, the affected versions and the fixed versions until the release itself is out.

For anyone running Joomla or WordPress, there is a catch. On almost every hosting account the owner does not apply PHP updates, the host does, and the host only does it for PHP branches that still receive fixes. So the useful question is not just “patch now”. It is “is my site on a PHP branch that gets this fix at all, and will my host actually apply it”. That is what this post answers.

TL;DR

- PHP releases a critical security fix on Wednesday 21 October 2026 at 14:00 UTC, for two vulnerabilities rated CVSS v4.0 9.2.
- No CVE IDs, affected versions or fixed versions are public yet. They are published with the release.
- PHP 8.2, 8.3, 8.4 and 8.5 all get the fix. PHP 8.1 and older get nothing, because they are end of life.
- You usually cannot apply it yourself. PHP is installed and updated by your host, and your control panel only offers what the host has installed.
- Across the live sites we monitor, 22.7% run PHP 8.1 or older. For those, no patched build is coming.
- Find the PHP branch of every site you look after today, then ask your host when the patched release goes on, or plan the version upgrade if there is no patched release to wait for.

What to do now

You cannot download this patch yourself, because PHP is set by your host. Check which PHP branch each of your sites runs on. If a site is on 8.2, 8.3, 8.4 or 8.5, the fix is coming, so ask your host when they will apply it. If a site is on 8.1 or older, no patched build will ever arrive, and the real fix is a version upgrade you should plan now.

What PHP Announced, and What It Held Back

The notice is short. Two critical vulnerabilities, both scored 9.2 on CVSS v4.0, with a coordinated release on 21 October at 14:00 UTC. PHP also reserves the right to release earlier if details of either vulnerability become public before then, or if evidence of active exploitation appears in the wild. Treat the date as a latest, not a guarantee.

Everything else is withheld on purpose. The CVE IDs, the affected versions and the fixed versions all arrive with the release, which is the normal way to stop attackers getting a head start from a pre-announcement. No one outside the PHP security team knows what the bugs are, and anyone claiming to is guessing.

What can be said is where the fix will appear. PHP 8.6 is still in release-candidate testing, so it is not a stable branch and is not where a production fix goes. The patched builds will be published as point releases on 8.2.x, 8.3.x, 8.4.x and 8.5.x.

Why a PHP Flaw Matters to Every Joomla and WordPress Site

PHP is the engine every Joomla and WordPress page runs through. Every request a site serves, from a logged-out visitor loading the home page to an administrator saving an article, is executed by the PHP interpreter on the server. A flaw in the interpreter therefore sits underneath all of the normal traffic a site already handles, below the CMS, its plugins and extensions, and any security layer that lives in application code.

How these two particular bugs are reached is unknown until the release, so this post makes no claims about that. The reason to prepare now is the rating: a pair of 9.2

vulnerabilities in the layer under every site you run is not something to start thinking about after the details are public and the exploit write-ups follow.

PHP belongs to your host, not your CMS

There is no PHP version setting inside WordPress or Joomla. The version your pages run on is chosen on the server, so the fix for a PHP flaw is applied by whoever runs that server. Your job is to know which of your sites are exposed and to make your host act.

Which PHP Versions Will Get the Fix?

PHP 8.2, 8.3, 8.4 and 8.5 will all receive the fix. PHP 8.1 and anything older will not. Critical security fixes go to both the actively supported branches and the security-only branches, which is why 8.2 and 8.3 are included even though their active support has ended. The [supported versions timetable](#) on php.net shows the exact dates for each branch, and the [end-of-life page](#) lists every branch that has fallen off it.

PHP 8.2 users should notice how close to the edge they are. Its security window closes on 31 December 2026, so it gets this fix but may not get the next one, and a site on 8.2 should already have a move to 8.3 or newer in the plan.

PHP branch	Status on 20 October 2026	Gets this fix?
8.5	Active support	Yes
8.4	Active support	Yes
8.3	Security fixes only	Yes
8.2	Security fixes only, ends 31 December 2026	Yes
8.1	End of life since 31 December 2025	No
8.0 and older	End of life	No

One thing trips people up here. Being on the right branch is only half of it; the other half is the patch level within that branch, and a site on 8.4 that the host has not updated for a year can be further behind than a site on 8.3 that was patched last week. The full explanation of [branches versus patch levels, and why the higher PHP number can be the more out-of-date one](#), is in its own post.

What Our Monitoring Shows About PHP Right Now

The figures below come from live Joomla and WordPress sites under active management, measured on 20 October 2026: agencies run their clients' production sites through mySites.guru, so this is what real hosting looks like today, not a public survey of people who chose to answer.

PHP versions on the Joomla and WordPress sites we monitor

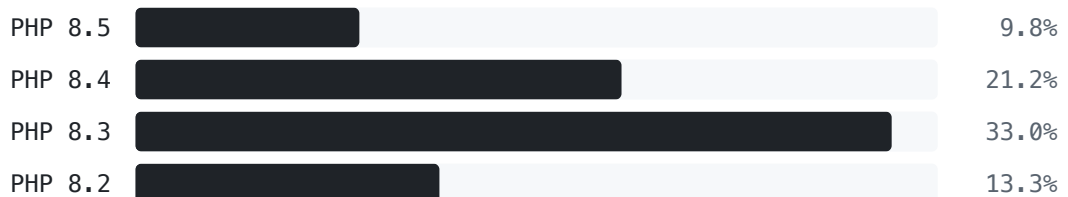
Every live site by the PHP branch it runs, grouped by whether that branch will get this release. Measured 20 October 2026.

All sites

Joomla sites

WordPress sites

On a supported branch, so this fix reaches them: 77.3%



End of life, so no patched build is coming: 22.7%



PHP versions detected on the live Joomla and WordPress sites mySites.guru monitors, measured 20 October 2026. These are production sites under active management, because agencies run their clients' sites through mySites.guru, so it reflects what real sites run rather than a public survey. Bars share one scale across all three tabs.

Read the chart from the top. 77.3% of the sites we monitor are on a branch between 8.2 and 8.5, so they will get this fix once their host applies the patched release. Those owners have one job, which is to make sure the host does it.

The other 22.7% are on PHP 8.1 or older, which is end of life and gets nothing no matter what the host does. Within that group, 16.6% of all sites are still on PHP 7 or older, running an interpreter that upstream stopped fixing years ago. The split by CMS is not even.

23.9%

of the Joomla sites we monitor run PHP 8.1 or older

end of life, so no patched build is coming

18.0%

of the WordPress sites we monitor run PHP 8.1 or older

WordPress still runs on PHP that upstream abandoned years ago

Detected on live Joomla and WordPress sites under active management, 20 October 2026. Joomla sites skew older than WordPress.

Why Do So Many WordPress Sites Run End-of-Life PHP?

Because WordPress lets them. The [official WordPress requirements](#) recommend PHP 8.3 or greater, but the current WordPress line still marks PHP 7.4 as compatible, and 7.4 has been end of life since November 2022. Recent WordPress versions kept compatibility all the way back to PHP 7.2, which reached end of life in November 2020. The [Core PHP compatibility matrix](#) shows this release by release.

WordPress does this on purpose, so that an update never fails because of the PHP underneath it. The side effect is that nothing ever forces a WordPress site off an abandoned interpreter: the CMS keeps updating, the plugins keep updating, and PHP stays wherever the host left it years ago.

Joomla takes a firmer line. Joomla 5 requires PHP 8.1 as a minimum and recommends 8.3, and [Joomla 6 requires PHP 8.3 and recommends 8.4](#), with the full list in the [Joomla technical requirements](#). The [WordPress 7 requirements](#) make an interesting comparison. A firmer floor pulls sites forward when they upgrade, but it cuts the other

way too: an old Joomla site that cannot move to a newer major version is pinned to whatever PHP its version supports, which is part of why the Joomla figure above is the higher one.

Does Your Host Actually Apply PHP Patches?

A PHP security release of this kind is a patch release inside a branch, for example 8.3.x to 8.3.y. It is binary-compatible and a drop-in replacement, so a host can roll it out across its servers with nothing changing for the site owner, and well-run hosts apply these within days of publication. The release that can break things is the major or minor jump, say 8.1 to 8.3, because that can affect themes, plugins and extensions and needs the owner to test first. Do not confuse the two: a host telling you “PHP updates can break sites” as a reason not to apply a point release is describing the wrong kind of update.

Telling whether your host lags is simple once you know where to look. The PHP selector in your hosting control panel only lists the versions the host has installed on that server. If the patched release is not offered there after it is published, there is nothing you can set, and the useful move is a support ticket asking when it is coming. Check the version the site reports while serving a request rather than trusting `php -v` on the command line, because the CLI binary and the one serving your pages are often different builds; the amber and green post linked above explains why.

What You Can Actually Do About It

PHP Version Should Be Latest Supported Series

mySites.guru checks every connected site for this automatically and flags it the moment it appears. It runs as part of the full audit on every connected site.

Check your site for free →

1. Find the PHP branch each site runs. Use the version the site reports while serving a request, which is what mySites.guru records for every connected site and checks against the list php.net publishes, refreshed hourly.
2. Supported branch, 8.2 to 8.5: ask the host when they will apply the patched release, and select it in the control panel as soon as it appears there.
3. End of life, 8.1 or older: no patched build is coming, so plan the version upgrade now. Check first whether the CMS or an extension pins the PHP version, because that upgrade moves before PHP can. A Joomla 3 site is the classic case, and [what to do with Joomla 3 sites still on an agency retainer](#) covers that conversation with the client.
4. Across many sites, do it from one list. Whether you [manage multiple Joomla sites](#) or [manage multiple WordPress sites](#), the PHP version is one column across all of them, and the CMS-side moves can be run as a [mass upgrade from one dashboard](#).

Once the release is published on 21 October, the affected and fixed versions will be known and the question becomes which of your sites are on them. Seeing every site's PHP version today, before that happens, is what turns the answer into a short job rather than an afternoon of logging into control panels. A [free audit](#) shows you that list in a few minutes.

Further Reading

- [Upcoming Critical PHP Security Release](#) - the PHP security team's advance notice, with the release date and severity.
- [PHP: Supported Versions](#) - the official timetable of which branches still receive fixes.

- PHP: Unsupported Branches - every PHP branch that has reached end of life, with the date it happened.
- WordPress Requirements - the official minimum and recommended PHP versions for WordPress.
- WordPress and PHP compatibility - the Core matrix of which PHP versions each WordPress release still supports.
- Joomla Technical Requirements - the current PHP minimums for Joomla.

To see which PHP version every one of your sites is running, and whether it is the current one, run a free audit. No credit card needed.

Frequently Asked Questions

What exactly did PHP announce, and when is the release?

On 20 October 2026 the PHP security team posted advance notice of a critical security release scheduled for Wednesday 21 October 2026 at 14:00 UTC. It fixes two vulnerabilities, both rated CVSS v4.0 9.2, and PHP may release earlier if details leak or active exploitation is seen.

Will my site get the fix?

Only if it runs on a supported PHP branch. PHP 8.2, 8.3, 8.4 and 8.5 will all receive patched point releases. PHP 8.1 and anything older is end of life and will not be fixed.

Can I apply the PHP fix myself, or is it my host's job?

On almost all Joomla and WordPress hosting it is the host's job. PHP is installed and updated on the server, and your control panel can only offer versions the host has installed. Your part is to check which branch each site runs and ask the host when the patched release will be applied.

What if my site is on PHP 8.1 or PHP 7.4?

No patched build is coming for those branches, whatever your host does. The only fix is a version upgrade to a supported branch, which is a minor or major jump that can break themes, plugins or extensions, so test it first and check whether your CMS or an extension pins the PHP version.

Does a PHP vulnerability mean my WordPress or Joomla site is exposed?

The two vulnerabilities are undisclosed until the release, so no one outside PHP knows how they are reached. What is known is that PHP is the engine every request to a Joomla or WordPress site runs through, and that both flaws are rated 9.2, which is reason enough to prepare before the details are public.

How do I tell which PHP version a site actually runs?

Use the version the site reports while serving a request, not what `php -v` prints on the command line, because the two often differ. mySites.guru shows that version for every connected site and flags it against the list php.net currently publishes, refreshed hourly.

Why does PHP 8.2 get the fix if it is in security-only support?

Critical security fixes go to both actively supported branches and security-only branches. PHP 8.2 is security-only until 31 December 2026, so it receives this one, but its window is closing and sites on it should be planning the move to 8.3 or newer.

AI MODIFIED

Written and edited by a human, with AI assistance. [Our approach to AI](#)

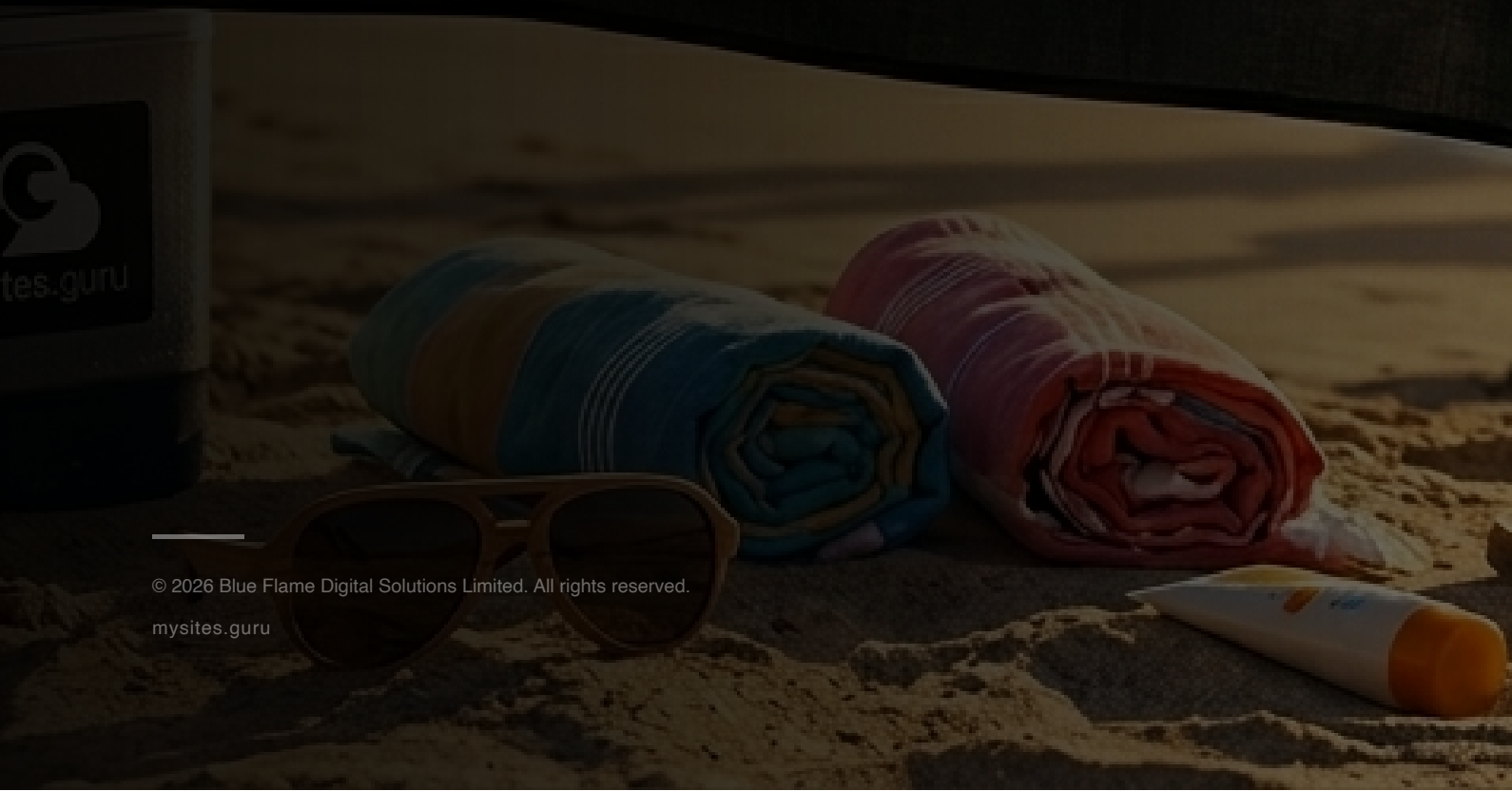
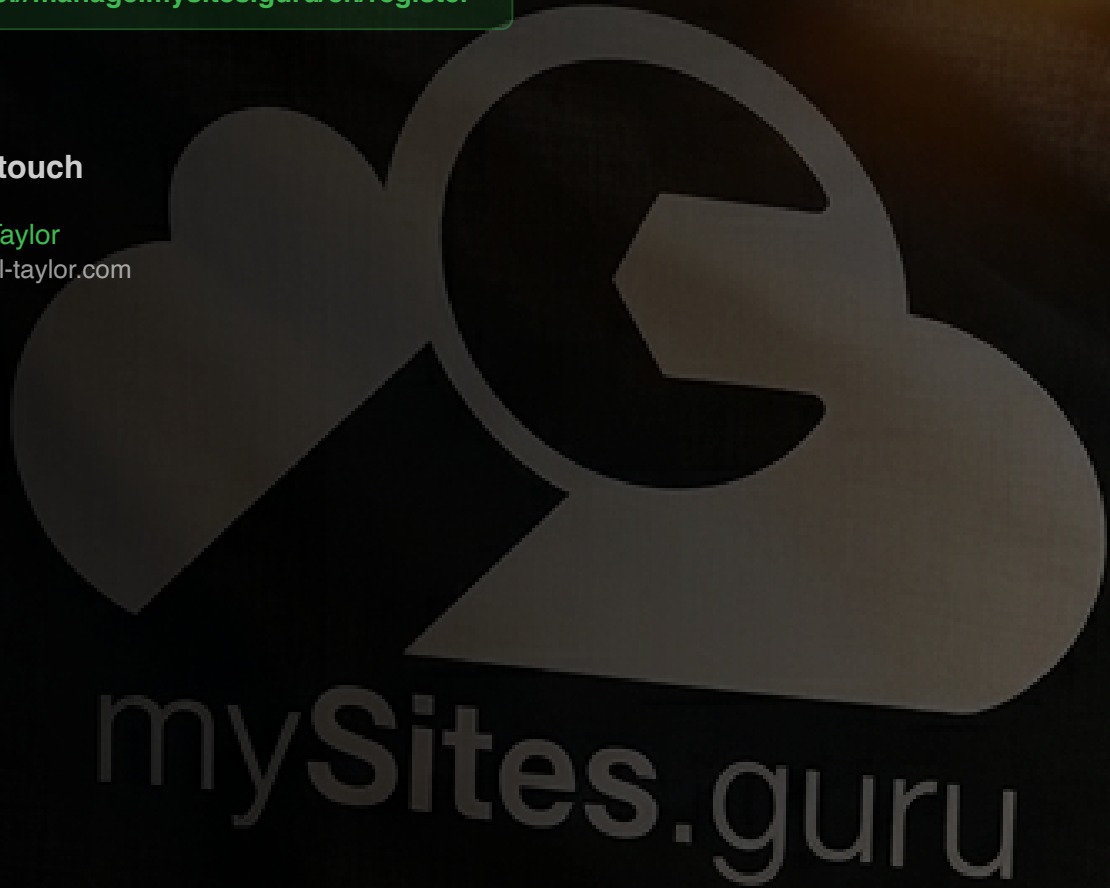
Get Your Free Site Audit

See how your WordPress and Joomla sites measure up.
No credit card required.

<https://manage.mysites.guru/en/register>

Get in touch

Phil E. Taylor
phil@phil-taylor.com



© 2026 Blue Flame Digital Solutions Limited. All rights reserved.

mysites.guru