



POWERED BY COFFEE

SURVIVAL GUIDE

PHP





Contents

- ➔ What is PHP?
- ➔ Why is it important to update your website to PHP 8?
- ➔ Why now?
- ➔ What are the breaking changes?
- ➔ The 3 Hacks to PHP Updates Can Prevent
- ➔ Overview
- ➔ Contact Us

What is PHP?

PHP is an open source scripting language that powers **all** WordPress websites. Thanks to its suitability for web development and ability to generate HTML, it's one of the **most used scripting languages**.

Since the open source language emerged, the team behind the coding game changer have been committed to listening and responding to feedback, leading to the rapid supply of additional features, concepts and developer productivity tools. In short, they're committed to making running websites easier and safer for all. Whilst there was a little bit of lag between PHP 5.6 and 7, the team are racing through to 8 with bigger and better, but also more breaking changes than ever before.



What is PHP?

PHP, however, is constantly evolving and its updates aren't as quick and easy to install as the latest LinkedIn app update. Whilst every WordPress website runs on PHP, it's up to the developers or technical team to ensure any potential bugs or broken code is dealt with as a result of the update. **Why?** Because websites that are using older, and thus no longer supported versions of PHP, are at risk of security breaches and can affect the integration of plugins.

1

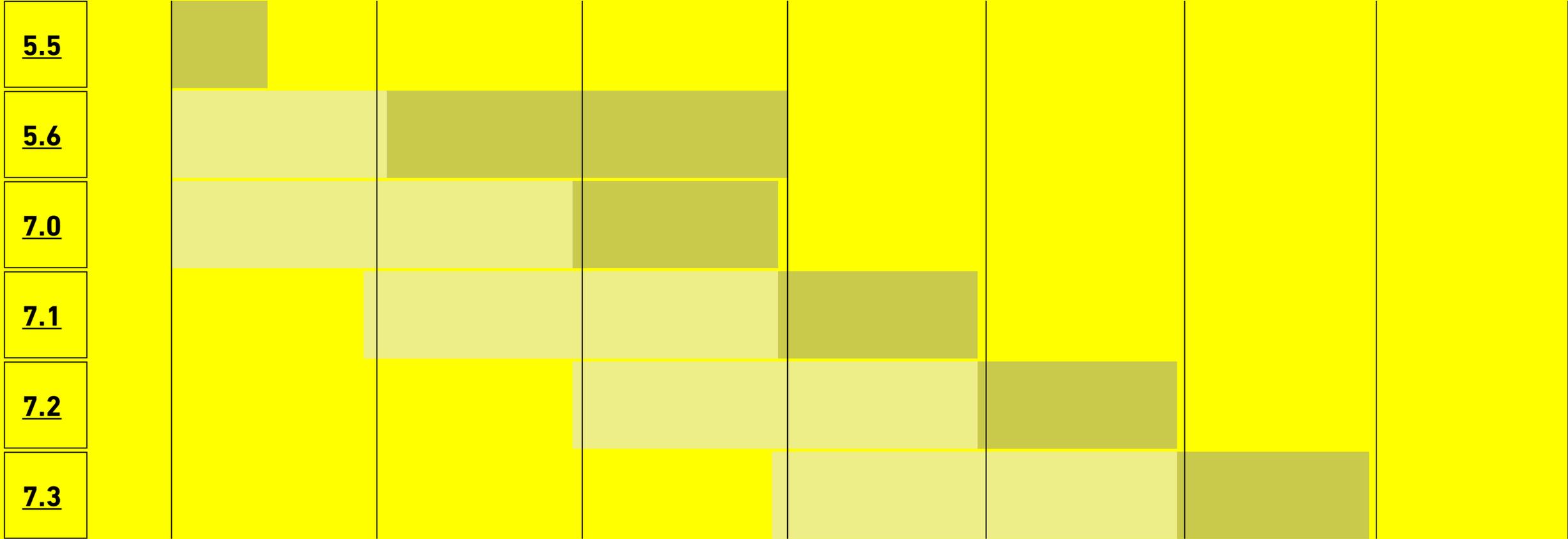
Branch	Since Initial Release		Active Support Until		Security Support Until	
<u>7.1</u>	1 Dec 2016	2 Yrs, 1Month	1 Dec 2018	1 Month	1 Dec 2019	in 10 Months
<u>7.2</u>	30 Nov 2017	1 Yr, 1Month	30 Nov 2019	in 10 Months	30 Nov 2020	in 1 Yr, 10 Months
<u>7.3</u>	6 Dec 2018	29 Days	6 Dec 2020	in 1 Yr, 11 Months	6 Dec 2021	in 2 Yrs, 11 Months



Active Support

Security Support

¹ Jan 2016 Jan 2017 Jan 2018 Jan 2019 Jan 2020 Jan 2021 Jan 2022 Jan 2023



PHP is used by
78.9%
of all websites.⁷

PHP 8 is
expected to be

45.39%

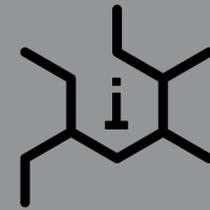
faster than PHP 7.4.⁸



Why is it important to update your website to **PHP 8**?



Described by Yoast as the **“most breaking PHP releases in the history of PHP”**, version 8 poses stricter typing language than ever before as well as a whole host of a shopping list of changes included in the update, meaning developers have their work cut out.



Up next: why your business needs to update to PHP 8

The biggest and most impactful change is the **stricter type language**. Whilst PHP 8 will try to recover the type, it is throwing more errors than it's fixing. This means that, alongside your update, you'll need to go under the hood of your website and fix these **manually**.

That's right, to ensure a **smooth transition**, going through your applications and manually resolving the errors will be an essential and worthwhile process.

1 Stricter Typing Language



2

Avoid the rush

Yes, PHP 7.4 will continue to receive active support from the PHP community. However, as we've seen with previous versions, support will eventually be withdrawn. This means, if you wait too long to update your PHP, your developers will be making amends without support from PHP themselves.

While this might not sound so bad, it's the equivalent of a mechanic replacing a gasket in a pitch-black garage. Whilst they may know their way around your website and code, shining a light on a solution to a problem is always easier than doing it in the dark...



We don't need to tell you that, to keep your website safe, you need to ensure your WordPress website and PHP is up to date. But the sooner you update your website, the sooner your developers will be accustomed to the breaking changes PHP 8 delivers.

Your very own in-house experts will be on-hand for minor tweaks, better able to deal with new integrations, and able to complete other requests faster.

3 Get ahead of the code



PHP 8: New & Improved Features



Despite the chore of ensuring your website will be code-ready to run PHP 8, the new update comes with a host of new features and improvements that will make your website and your developer's jobs easier.

Even faster than PHP 7 thanks to the new JIT compiler

The highly anticipated just in time compiler boasts improved performance. But what is it *exactly*? According to Stitchio, **"JIT" is a technique that will compile parts of the code at runtime, so that the compiled version can be used instead."**

Rather than repeating the translation of the PHP code, JIT allows your site to run the code on a repetitive basis, creating a faster and smoother experience for your website users.

Improved Developer Productivity from new Language Features

The long-awaited update packs a powerful productivity punch thanks to its language features. PHP 8's update includes less repetition from constructor, static return type and object creations, and even improved error handling and standardisation between errors and exceptions. Once their head is around it, your developer team will be able to work smarter.

New Static Return Type

Return type is one of the most used types. Previously, only self was allowed to provide a valid return. However, static now benefits from this developer favourite thanks to PHP 8.

Strict Typing

PHP 8 will prevent entire classes of bugs and errors through its advanced strict typing feature. While it's considered a breaking change, once they get used to it, your developers will offer a sigh of relief knowing they no longer have to tell the code the difference between, "false", false, 0, "" or null.



44% of hacking was caused by outdated WordPress sites.

The FBI has reported that cybercrime cost businesses **\$3.5 billion** in 2019.⁹

Cyber attacks cost UK businesses **£34 billion.**¹⁰



Why now?

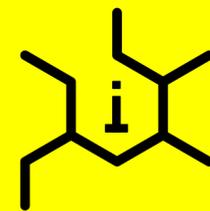
So, PHP 8 may have been released, but PHP 7 is still available. So you may find yourself wondering why it's worth updating your WordPress website and why *right now*? The PHP 7 legacy will continue to exist, just like the versions of PHP before it, however, if previous updates are anything to go by, it's unlikely that updates for security and bug fixes will be delivered in 2022.

You might be thinking that this gives you plenty of time to update your website's script. However, depending on how many breaking changes affect your website, and whether you'll have the time and resources to do it next year, you may find yourself rushing to fix your code. Or worse, you leave yourself open to hacks, hostages, and malicious code.



What are the breaking changes?

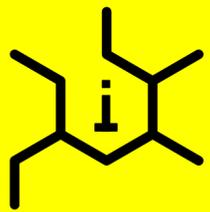
This is one of PHP's biggest updates in recent years. Therefore, there will be breaking changes. Now, if you've been staying up to date with PHP versions (7 or its deprecations), they won't be so groundbreaking. However, if you've been running your website on PHP 5.6 or older, the breaking changes will have a more dramatic impact.



Please see the following page for the core changes that will affect your WordPress site



Core changes



You can find a full list of breaking changes on [Github²](#), but the core changes that will affect your WordPress site are:

- 001.** Consistent type errors
- 002.** Reclassified engine warnings
- 003.** The @ operator no longer silences fatal errors
- 004.** Default error reporting level
- 005.** Default PDO error mode
- 006.** Concatenation precedence
- 007.** Stricter type checks for arithmetic and bitwise operators
- 008.** Namespaced names being a single token
- 009.** Saner numeric strings
- 010.** Saner string to number comparisons
- 011.** Reflection method signature changes
- 012.** Stable sorting
- 013.** Fatal error for incompatible method signatures



52%

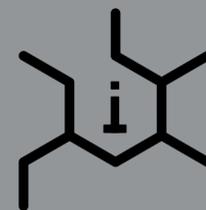
of WordPress vulnerabilities relate to WordPress plugins.¹¹



The **3** Hacks PHP Updates Can Prevent

According to Malcare.com, **“outdated themes and plugins are the leading cause behind hacked websites”**.³ But here’s the important takeaway from that point: all themes and plugins all run on PHP script which is what makes the security risk of not updating to PHP 8 so great.

As vulnerabilities come to the forefront, the PHP team issues updates to ensure that our websites and the data hosted within them are protected. However, the longer you leave it to update, the more exposed you are to security breaches and attacks.



Next Up: 3 of the most common preventable website security attacks



Similar to file inclusion exploits, SQL injections are designed to target your database and WordPress accounts. Abusing bugs in codes to perform actions that weren't intended, they attack data-driven applications, planting malicious SQL statements.

These types of attacks can result in a variety of detrimental security breaches. Most commonly, data is deleted, lost or stolen. However, in more severe circumstances, it can lead to websites being defaced, becoming unauthorised, or **“compromise individual machines or entire networks”**.⁴

Keeping your PHP updated means it's harder for hackers to find broken code which will allow them to complete the SQL injection in the first place.

1 SQL Injection



2

Sensitive Data Exposure

It's not just your WordPress website that you need to worry about. When web applications and APIs are not up to date, you're failing to properly protect any sensitive data. With cybercrime becoming more and more sophisticated every year, if you do not update your PHP, you leave your website wide open for a variety of attacks that you might not be able to come back from.

In today's data-obsessed world, where we're giving our information away on a near-daily basis, these types of scams can single-handedly bring your business to its knees by sending your customers fraudulent emails, scamming them of hundreds, or even thousands, of pounds.



According to OWASP, this is a commonly seen issue. The attack occurs as a **“result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information.”**

What that essentially means is that at any point, across your website, servers, code, and anywhere else in your stack, you’ve not kept your website up to date or ensured that there are no weaknesses in the code, you will be vulnerable to an attack. As part of your stack, PHP is one of the elements that can so easily compromise your security if it is not updated correctly.

3

Security Misconfigured



What does **PHP** have to do with this?

As explained by WordPress themselves, one of the two major benefits of keeping your PHP up to date is that it will make your website **“more secure”**.

PHP, like WordPress, is maintained by its community. Because PHP is so popular, it is a target for hackers – but the latest version will have the latest security features. Older versions of PHP do not have this, so updating is essential to keep your WordPress site secure.⁵

While WordPress gets a bad wrap for security, it is in fact not WordPress itself that’s causing the problem; it’s an out of date PHP script.



What's the **impact** on my WordPress website?



Within the dev community, everyone's asking whether WordPress is compatible with PHP 8 and, the consensus from industry leaders like Yoast is, well, *they're not sure*.⁶

Whilst the volume of breaking changes are raising some eyebrows within the development community, it's safe to say that there are some undeniably positive changes that will improve the performance of WordPress websites and make them, crucially, more secure.

Did you know that the Panama Papers Leak in 2016, which saw **2.6TB** of data, **11.5million** documents, and **4.8 million** emails leaked was due to a plugin that hadn't been updated?¹²



It's time to update

PHP 8 is a beast of an update. With the variety of break changes, the stricter typing language, and the impact on your website's security, we cannot stress this enough... ***Update to PHP 8 sooner rather than later!***

Whether you seek the help of a development agency, or you're doing it yourself, don't put it off too soon. The risks by far outweigh the benefits of investing time and money into a smooth transition to PHP 8.



We're WordPress & PHP experts

Want some help with your PHP 8
update? Or do you just want someone
to do all the hard work for you?



Reference URL Links

001. [Server Guy](#)

002. [GitHub](#)

003. [Malcare](#)

004. [E-Security Planet](#)

005. [WordPress](#)

006. [Yoast](#)

007. [Kinsta](#)

008. [Git Connected](#)

009. [CBR Online](#)

010. [Reliance CSN](#)

011. [Kinsta](#)

012. [Kinsta](#)

