

PHP2Shell: the PHP security flaw every website owner needs to check

Two critical PHP flaws let attackers take over web servers with no login. Updating WordPress won't fix it. Here's how to check your PHP version and what to ask your host.

If your website runs on WordPress, WooCommerce, Joomla, Drupal, Magento or anything else built with PHP, this one matters. The fix sits on your web server, not in your website, so you probably need your host to act.

What happened

On 21 October 2026 the PHP project released urgent updates for two critical flaws in PHP itself, CVE-2026-109618 and CVE-2026-109619, both rated 9.2 out of 10. The flaws have been nicknamed PHP2Shell.

In plain words: someone with no login can send requests to a website and, in the right conditions, run their own code on the server behind it. From there they could reach your files and your database, install malware or take the site down.

Researchers at the security firms Calif and Wiz found the flaws with the help of advanced AI tools. Calif was working through OpenAI's Patch the Planet programme, which gives researchers those tools to find and fix flaws. The bugs had gone unnoticed for more than a decade. Details leaked on social media on 20 October, so the fix came out earlier than planned.

Governments and security agencies moved fast. The UK's National Cyber Security Centre (NCSC) told organisations to update, and to consider taking systems offline if they can't. Finland temporarily shut down its government's public web services, Dutch government sites went offline, and the Wikimedia Foundation took some systems down as a precaution. Cloudflare's chief technology officer said it was already seeing early attacks.

Who is affected

PHP is the language that runs a large share of the web. You are likely affected if your site uses:

- WordPress, including WooCommerce shops
- Joomla or Drupal
- Magento
- any custom site or web app written in PHP
- some control panels and other products that use PHP in the background

The PHP project says every PHP installation serving web pages is at risk, including PHP-FPM, Apache with mod_php, php-cgi, FrankenPHP and LiteSpeed. It rates the risk highest for Apache with mod_php, where an attack has been shown to work before the website's own code even runs. The NCSC says all versions may be affected, so don't assume an older or newer version is safe.

What to ask your host

Copy this, fill in your web address and your name, and send it to your host's support team.

Subject: PHP2Shell (CVE-2026-109618 and CVE-2026-109619) on my website

Hi,

Please can you confirm the following for my website [your web address]:

1. Which PHP version is my site running right now?
2. Has PHP been updated to 8.2.35, 8.3.36, 8.4.27, 8.5.12 or later, or had the PHP2Shell fixes applied? If not, when will it be?
3. If my site is on PHP 8.1 or older, what is the plan to move it to a supported version?
4. Have you checked my hosting account for any signs of compromise since the flaws were made public?

Thanks,

[your name]

Why updating WordPress alone doesn't fix it

WordPress, Joomla and the rest are programs that run on top of PHP. This flaw is in PHP, the layer underneath. You can have WordPress fully updated, every plugin current, and still be exposed.

The fix is a PHP update on the server. On most shared or managed hosting, only your host can do that. If you run your own server, it is your job (or your developer's).

How to check your PHP version

- WordPress: go to Tools, then Site Health, then the Info tab, and open the Server section. It shows the PHP version.
- Hosting control panel: most panels, such as cPanel or Plesk, show the PHP version in a PHP settings or PHP version section.
- Ask your host or developer: if you can't find it, the email above does the job.

One catch: some hosts and Linux distributions fix older versions without changing the main version number (called backporting). So the number alone may not tell the whole story. Ask your host to confirm in writing that the PHP2Shell fixes are applied.

The fixed versions

Your server should be on one of these, or later:

- PHP 8.5.12
- PHP 8.4.27
- PHP 8.3.36
- PHP 8.2.35

PHP 8.1 and older no longer get updates from the PHP project. It has published small source patches for PHP 7.4, 8.0 and 8.1 for people who build PHP themselves, and some hosts and vendors supply their own fixed versions, but the safest step is to move to a supported version. PHP 8.2 also reaches end of life on 31 December 2026, so plan to move off it soon anyway.

What to do if you can't patch yet

Ask your host or developer to apply the PHP project's temporary mitigations. These are server settings that block some known attack routes. The PHP project is clear that they reduce the risk but do not make a site safe.

If that isn't possible, or will take too long, the NCSC says to consider taking the site offline until it is fixed. A short "back soon" page served from somewhere else is better than a hacked site.

Before and after updating, check for signs someone got in: unfamiliar admin accounts, new or changed files you don't recognise, odd redirects or spam pages. Updating stops new

attacks but does not remove anything already planted.

Keep an eye out for updates from vendors whose products bundle PHP, such as control panels and other hosting software.

Common questions

My site is on WordPress and it's fully updated. Am I safe?

Not from this. WordPress updates don't change PHP. You need to know your server's PHP version and whether your host has patched it.

I'm on shared hosting. Do I need to do anything?

Your host should be updating PHP, but don't assume. Send the email above and get it confirmed.

My site is on PHP 7.4 or 8.0. What now?

There is no new official release for those versions. Ask your host whether they have applied a fix, either the PHP project's source patch or their own, and plan a move to a supported version. Check your site and plugins work on the newer version first.

Is my website down because of this?

Possibly. Some organisations have taken sites offline as a precaution, and applying the fix can mean a short restart. Ask your host.

How was this found?

Researchers found the flaws with AI tools after they had sat unnoticed for more than a decade. Tools like these make flaws quicker to find for everyone, attackers included, which is why patching quickly matters more than ever.

Want us to check it for you?

If you're not sure which PHP version your site runs, or whether your host has patched it, we can check it for you and tell you in plain words what needs doing. [Book a short call with Pete](#), or email your web address to enquiries@corsolutions.co.uk.

Sources

[PHP security advisory, 21 October 2026](#)

[NCSC: Critical security issue affecting PHP](#)

[BBC News, 21 October 2026](#)

[NHS England Digital alert: Critical Vulnerabilities in PHP \(PHP2Shell\)](#)

Tags: #PHP2Shell #PHP #WordPress #Website Security #Web Hosting #NCSC

COR Intelligence, a trading name of COR Solutions Services Ltd (Co. 15027891). Read online:
<https://blog.corsolutions.co.uk/articles/php2shell-php-security-flaw-website-owners>