

The five-minute PHP check

On 21 October, PHP fixed two critical holes. Both are rated 9.2 out of 10. An attacker doesn't need a login, and attacks have been seen since that day.

The two are CVE-2026-109618 and CVE-2026-109619.

PHP runs about 7 in 10 websites whose server language is known. Steps 1 to 5 need no code.

1 Does your site run PHP?

It does if it's built on WordPress. WordPress runs on PHP.

If you have a hosting panel like cPanel or Plesk, it shows a PHP version for your site.

Not sure? Ask your host. It's one question.

If you never picked a host because your site builder runs everything, ask that platform's support whether they've applied the 21 October PHP fixes. Once they confirm, you're done.

2 Find your PHP version

- **WordPress:** go to Tools, then Site Health, then the Info tab. Open the Server section. PHP is listed there.
- **cPanel:** go to Software, then MultiPHP Manager. It shows the PHP version each domain uses.
- **Plesk:** go to Websites & Domains. The version sits next to the PHP icon on your domain.

Write down the whole number, like 8.3.36. Not just 8.3.

3 Compare it to the fixed versions

IF YOUR VERSION STARTS WITH	YOU'RE FIXED AT
8.5	8.5.12 or higher
8.4	8.4.27 or higher
8.3	8.3.36 or higher
8.2	8.2.35 or higher
8.1, 8.0, 7 or lower	No official release. Ask your host about a backported fix, or move to a supported version.

One catch. Some Linux builds of PHP are fixed without changing the number. Ubuntu's fixed PHP for its 24.04 release still reads 8.3.6. So a lower number doesn't always mean you're exposed.

A panel that only says "8.3" can't tell you either way. Your host can.

4 What to do if you're not fixed

1. **Send your host the message below.** It asks the one question that settles it.
2. **Don't stop at updating WordPress.** Keep it and your plugins updated, but that doesn't fix this. The holes are in PHP itself, and the attack runs before WordPress does.
3. **If you were on an unfixed version on or after 20 October, change your logins.** Details leaked that day. New admin passwords first. In WordPress, go to Users, then Profile, and click "Log Out Everywhere Else". That way anyone already signed in as you is signed out.
4. **Ask your host to check for files they didn't put there,** and to change your database password.

MESSAGE FOR YOUR HOST

Hi, my site is (your web address).

Please confirm the PHP version it runs, and that it includes the 21 October 2026 security fixes for CVE-2026-109618 and CVE-2026-109619 (fixed in PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35, or your own patched build).

If it doesn't, when will it be updated?

If I'm on PHP 8.1 or older, do you provide a backported fix, or what do I need to do to move to a supported version?

Thanks.

5 How you know you're done

- A fixed version from the table shows in Site Health or your panel, or your host confirms in writing that your PHP includes the 21 October fixes.
- If you were exposed: new passwords, other sessions logged out, and your host has checked for strange files.

6 If you have a developer

- Run `php -v`, and on a Linux distribution check the package version against the vendor's notice. Ubuntu's is USN-8948-1.
- Restart every PHP worker after the update or any `php.ini` change, so the fixed build is the one running.
- If you can't update today, the PHP team lists stopgaps on php.net, like `session.upload_progress.enabled=0` in `php.ini`. They cut the risk but don't remove it. Only the update does.
- If the site was exposed, change database passwords, API keys and session tokens, and scan for webshells.

7 Share this with your agent

If an AI agent can reach your site or hosting account, paste it this. It tells the agent to check and report, and to change nothing without your yes.

PASTE THIS TO YOUR AGENT

Check my website (your web address) for the October 2026 PHP vulnerabilities CVE-2026-109618 and CVE-2026-109619. Read only. Don't change anything without asking me first.

1. Find out if the site runs PHP.
2. Find the exact PHP version: WordPress Tools > Site Health > Info > Server, the hosting panel, or `php -v` on the server plus the installed package version.
3. Compare it to the fixed versions: 8.5.12, 8.4.27, 8.3.36, 8.2.35. PHP 8.1 and older get no official release. A Linux distribution package can be fixed with an older version number, so check the vendor's security notice.
4. Tell me in plain English: fixed, exposed or unsure, and why.
5. If exposed or unsure, draft the message to my host and list the passwords I should change. Don't send or change anything until I say yes.

Source: php.net/archive/2026.php (21 October 2026 security advisory).

We run site audits for businesses at CYSTEMS. If you want one, reply to my DM.

— Champ Smith, CYSTEMS

Sources: php.net/archive/2026.php (20, 21 and 23 Oct 2026 advisories) · ubuntu.com/security/notices/USN-8948-1 · wordpress.org/about/requirements · wordpress.org Site Health and Your Profile docs · docs.cpanel.net MultiPHP Manager · docs.plesk.com PHP Settings · [watchTowr](https://watchtowr.com) PHP2Shell FAQ · [Sansec](https://sansec.com) · [Huntress](https://huntress.com) · [W3Techs](https://w3techs.com) (23 Oct 2026).