



FREE CHECKLIST · CYBER A.I. PROS · OCTOBER 21, 2026

PHP Emergency Update Checklist

For website owners whose site runs on PHP (that includes most WordPress and many other CMS sites). About 15 minutes, plus a message to your hosting provider.

What happened: on October 21, 2026 the PHP project released fixes for two **critical** security flaws (CVE-2026-109618 and CVE-2026-109619, each rated 9.2 out of 10). PHP says they can let an attacker run code on a web server **without logging in**, and that every PHP installation serving web requests is in scope. Cloudflare says it has already seen attack traffic aimed at these flaws. We haven't verified a count of compromised sites.

The fixed PHP versions (from php.net):

8.5.12

8.4.27

8.3.36

8.2.35

Important: a lower-looking version number is **not** automatically unsafe, and a matching one isn't automatic proof. Linux vendors and hosts often **backport** fixes into older version numbers (Ubuntu does this, for example). Only your host's or vendor's advisory or build information proves your PHP is fixed. PHP 8.1 and older get no updates from the PHP project; ask your vendor, or plan a move to a supported version.

Do these now

- ☐ **Find every site and app you run on PHP.**
Websites, shops, booking or membership pages, admin tools. Don't forget old or "test" sites that are still online.
- ☐ **Ask your hosting provider directly**
(use the message on the next page). Ask about **both** CVEs and the PHP that actually **serves your website**.
- ☐ **Write down the evidence**
in the table on the next page: the PHP version and vendor build, the advisory your host points to, and when it was applied.
- ☐ **If you manage your own server,**
install your operating system or vendor's supported PHP security update and restart PHP and your web server the way the vendor says, so the old code stops running.
- ☐ **Check your site still works:**
open the home page, log in to the admin area, test a contact form or checkout. Note the time you checked.

☐ **Keep watching for a few days.**

Look for unexpected new admin users, changed files, strange redirects or a surprise jump in errors. Ask your host to tell you about anything unusual they see.

Not enough on its own: updating WordPress, a theme or plugins does **not** fix these PHP flaws. Checking the command-line PHP version can also mislead, because the PHP that serves web pages can be a different build. A firewall service helps, but Cloudflare itself says to patch PHP anyway.

Copy-and-paste message for your hosting provider

Hi, I'm checking my site **[your website address]** after the PHP security fixes released on October 21, 2026 for **CVE-2026-109618** and **CVE-2026-109619**.

1. Is the PHP that serves my website patched for **both** CVEs? Which PHP version and build is it running now?
2. If you use backported packages, which vendor advisory covers my server (for example a USN or RHSA number)?
3. When was the update applied, and were the PHP workers restarted afterward?
4. If it isn't patched yet, when will it be, and what are you doing to protect my site until then?
5. Have you seen anything unusual on my account that I should know about?

Thanks!

Your evidence record

Website / app	
Hosting provider	
Web PHP version and vendor build (from your host)	
Advisory that covers it (php.net, vendor or host notice)	
Both CVEs fixed? (CVE-2026-109618 and CVE-2026-109619)	☐ Yes ☐ No ☐ Waiting for an answer
Date and time the update was applied	
PHP workers / web server restarted?	☐ Yes ☐ No ☐ Don't know
Site checked after the update (time, what you tested)	
Anything unusual noticed?	

If you can't get it fixed today

PHP says **updating is the only safe choice**; its temporary settings only reduce some risk. The EU's cyber agencies (ENISA and partners) and the UK's NCSC say to put internet-facing systems first, and if a system can't be fixed or protected, to consider taking it offline or isolating it until it can. Ask your host or developer which applies to you. Don't paste commands from social media into your server.

Official sources

- **[PHP security advisory \(October 21, 2026\)](https://www.php.net/archive/2026.php#2026-10-21-5)**
<https://www.php.net/archive/2026.php#2026-10-21-5>
- **[GitHub advisory CVE-2026-109618 \(GHSA-w8hw-w9fx-j79w\)](https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w)**
<https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w>
- **[GitHub advisory CVE-2026-109619 \(GHSA-6wmf-4rv5-p3rp\)](https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp)**
<https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp>
- **[ENISA and EU partners: joint statement](https://www.enisa.europa.eu/news/joint-statement-on-critical-php-vulnerabilities)**
<https://www.enisa.europa.eu/news/joint-statement-on-critical-php-vulnerabilities>
- **[UK NCSC: critical security issue affecting PHP](https://www.ncsc.gov.uk/news/critical-security-issue-affecting-php)**
<https://www.ncsc.gov.uk/news/critical-security-issue-affecting-php>
- **[Example vendor backport: Ubuntu USN-8948-1](https://ubuntu.com/security/notices/USN-8948-1)**
<https://ubuntu.com/security/notices/USN-8948-1>
- **[Cloudflare: protections and observed attack traffic](https://blog.cloudflare.com/php-vulnerabilities-waf-protection)**
<https://blog.cloudflare.com/php-vulnerabilities-waf-protection>
- **[Researchers' page \(Wiz\): php2shell.com](https://php2shell.com/)**
<https://php2shell.com/>

Checked against the sources above on October 21, 2026, 21:08 UTC (5:08 PM EDT). Security news moves fast: always follow your host's and vendor's latest advice. This checklist is general information, not a security audit of your site.

Watch the video and get more free resources: cyberaipropros.com/news · PHP logo by Colin Viebrock, CC BY-SA 4.0.

© 2026 Cyber A.I. Pros. Free to share, unchanged, with credit.