Critical PHP vulnerabilities (21st Oct, 2026): What you need to do

Critical Security Updates · https://www.aeserver.com/support/critical-php-vulnerabilities-cve-2026-109618-109619/

On 21 October 2026, the PHP project released fixes for two critical vulnerabilities, CVE-2026-109618 and CVE-2026-109619 (both rated CVSS 9.2), which can allow unauthenticated remote code execution. The fixed versions are PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35, and security researchers report that attackers are already trying to exploit them. The flaws are in PHP itself, the language that WordPress and many other websites run on, so they affect sites and servers wherever they are hosted.

Official advisory Read the PHP project's advisory on php.net: Critical remote code execution vulnerabilities, update now.

Shared hosting

If your website is on AEserver shared hosting, including our WordPress Hosting plans, you do not need to do anything. We had already applied protective measures on our servers before the PHP patches were released, and the patched PHP packages have also been installed on the server hosting your website.

Please note that your website may still show the same PHP version number as before. Our operating system (CloudLinux) delivers the security fix as a patched build of the same version, rather than changing the version number. The fix for both vulnerabilities is included in the installed build.

Cloud and dedicated servers

PHP's advisory says every installation that serves web requests is at risk, whichever PHP handler it uses. If you manage your own cloud or dedicated server, we recommend that you:

1. **Check which PHP version** your server and applications are running.

2. **Install the fixed PHP release now** from your operating system or control panel vendor, then restart your PHP handler if needed so the update takes effect. Many vendors, including CloudLinux and the major Linux distributions, deliver the fix as a patched build of the same version, so check your vendor's security notice rather than relying on the version number alone.
3. **If you run PHP 8.1 or older, plan an upgrade** to a supported version (8.3 or 8.4 recommended). The PHP project no longer releases updates for these versions, although some operating system vendors provide backported fixes. PHP 8.2 received this fix in 8.2.35, but its security support ends on 31 December 2026, so include it in your upgrade plan as well.
4. **If you use containers, rebuild your images** from the updated PHP base image and redeploy your containers.

If you cannot update straight away The PHP advisory lists temporary mitigations, but warns that they do not make a server safe. Updating is the only complete fix.
If your server runs cPanel You can check and change the PHP version for each domain in cPanel. See How to Change the PHP Version via CloudLinux Selector in cPanel or How to Set the PHP Version per Domain in cPanel.

What happens next

We will keep this article updated if further details are confirmed. If you need help checking your PHP version or planning the update, please contact our support team.

Our UAE-based support team is available 24/7

- Open a ticket from your client area
- Start a live chat on aeserver.com