

FOR IMMEDIATE RELEASE
October 21, 2026

Limehawk Urges Businesses to Patch PHP Servers After Two Critical Flaws

Two newly fixed bugs in PHP can let an attacker run code on a web server without logging in. Only patching fixes them.

KNOXVILLE, Tenn., Oct. 21, 2026. Limehawk, LLC, a Knoxville managed IT services provider, today urged businesses to find and patch every system running PHP after the PHP project fixed two critical vulnerabilities that can allow unauthenticated remote code execution.

The PHP team released fixed versions 8.5.12, 8.4.27, 8.3.36 and 8.2.35 on Oct. 21. The two flaws, CVE-2026-109618 and CVE-2026-109619, are both rated 9.2 under CVSS v4.0. CISA refers to them as "php2shell."

According to the PHP team, every PHP installation that serves web requests is at risk, including PHP-FPM, Apache with mod_php, php-cgi, FrankenPHP and LiteSpeed. The team rates Apache with mod_php as the highest risk, because a demonstrated exploit there lets one unauthenticated request trigger the attack before any application code runs. PHP-FPM and the other setups are on the affected list, but the advisory does not describe a full working exploit against them.

CISA said it had not observed exploitation as of the time of its alert.

What is wrong with PHP?

CVE-2026-109618 (GHSA-w8hw-w9fx-j79w) is in out-of-memory handling. Cleanup can treat half-built request data as valid. CVE-2026-109619 (GHSA-6wmf-4rv5-p3rp) lets internal state from one request outlive its freed memory, so a later request on the same worker may use it.

What should businesses do?

Limehawk recommends these steps:

- **Find everything running PHP.** That includes WordPress and Drupal sites, custom web apps, and the web admin pages on routers, firewalls and other appliances. CISA notes PHP is often built into other software.
- **Patch internet-facing systems first.** Update to PHP 8.5.12, 8.4.27, 8.3.36 or 8.2.35. Linux distributions and LTS vendors got the patches in advance, so check your vendor's packages. For appliances, watch for vendor updates.
- **Confirm the version and restart.** Run `php -v` to check the version, then restart PHP-FPM, Apache or whatever serves PHP so every worker loads the fixed build. The command-line PHP can differ from the one serving your site, so check both.

- **Take offline what you can't patch.** CISA says systems that can't be updated right away, or that run PHP 8.1 or older, should come offline until patched. A web application firewall may give some protection meanwhile.
- **Watch for signs of compromise.** CISA recommends looking for PHP worker processes launching shells or downloading tools.

What if a server can't be patched today?

Only an update fixes these vulnerabilities. The PHP team lists configuration changes that narrow specific attack paths but do not make a server safe:

- Set `memory_limit=-1` in a way applications can't override, such as `php_admin_value` in the FPM pool or Apache config.
- Set `post_max_size = 8M`, or 32M if the site needs file uploads. Keep `upload_max_filesize` below it.
- Set `session.upload_progress.enabled=0` in `php.ini` or the FPM pool (not `ini_set()` or `.user.ini`), then restart every worker.
- On PHP 8.5, set `fatal_error_backtraces=0` and restart every worker.

The full list is in the PHP advisory.

What about older PHP versions?

PHP 8.1 and older no longer get updates from the PHP project. Because of the severity, the PHP security team published minimal source backports for 7.4, 8.0 and 8.1, and some distributions and LTS vendors ship their own. The volunteer-run `rpms.remirepo.net` will not have updates on release day; the PHP team urges its users to switch to distribution packages or build from source. PHP 8.2 reaches end of life on Dec. 31, 2026.

Sources

1. PHP, "Security advisory: Critical remote code execution vulnerabilities, update now." Oct. 21, 2026.
<https://www.php.net/archive/2026.php#2026-10-21-5>
2. PHP, "PHP 8.2.35 Released!" Oct. 21, 2026.
<https://www.php.net/archive/2026.php#2026-10-21-1>
3. PHP, "Upcoming Critical PHP Security Release." Oct. 20, 2026.
<https://www.php.net/archive/2026.php#2026-10-20-1>
4. CISA, "Critical Vulnerabilities in PHP Require Immediate Patching." Oct. 21, 2026.
<https://www.cisa.gov/news-events/alerts/2026/10/21/critical-vulnerabilities-php-require-immediate-patching>

Media Contact

Corey Watson, Managing Member
Limehawk, LLC
press@limehawk.io
<https://limehawk.io>

###