PHP ships security fixes for every supported branch on the day 8.6 arrives

20 November 2026 · 5 min read · blogs.iictp.org/php-november-2026-security-releases-php-8-6

The PHP project released PHP 8.5.13, 8.4.28, 8.3.37 and 8.2.36 on 19 November 2026, describing each as a security release and encouraging all users of those branches to upgrade. The same day it released PHP 8.6.0, a new major version. A day earlier, the PHP security team had pre-announced the fixes and said the highest severity was critical.

TL;DR The short version

- PHP shipped security releases for every supported branch on 19 November 2026, the same day PHP 8.6.0 arrived.
- The security team rated the worst issues critical, though some need non-default configurations.
- Upgrade and restart PHP-FPM, prioritising hosts that run PHP-CGI, expose the FPM status page or take untrusted input.

Read online, listen to it, or change the text size: https://blogs.iictp.org/php-november-2026-security-releases-php-8-6

What was reported

- In its pre-announcement, the PHP security team said the issues rated critical "require either non-default configuration or uncommon setups", and that the releases address vulnerabilities in all supported PHP versions.
- The PHP 8.5.13 changelog lists use-after-free flaws in magic method backtraces (CVE-2026-129474) and in the timezone cache (CVE-2026-129496), each described as able to lead to remote code execution.
- The same changelog lists an out-of-bounds read and write in PHP-CGI during PATH_INFO correction (CVE-2026-129538) and a double free during DOM XML serialisation (CVE-2026-129501).
- For PHP-FPM, it lists an epoll use-after-free that can lead to local privilege escalation (CVE-2026-129291), request smuggling through an unread HTTP request body (CVE-2026-129289), and cross-site scripting on the status endpoint (CVE-2026-129292).
- LWN reported the releases on 19 November and noted that Linux vendors and projects should be releasing updated packages soon.
- PHP 8.6.0 adds features including partial function application, default values for readonly properties, a new Io\Poll API, a clamp() function, a \Time\Duration class and a SortDirection enum, according to the PHP project.

What a practitioner should do

- Upgrade to the security release for your branch, or to your distribution’s patched package, and restart PHP-FPM, Apache or whatever runs PHP so the new binary is in use.

- Prioritise hosts that run PHP-CGI, expose the PHP-FPM status page, or accept untrusted input that reaches the DOM or date extensions, since those match the components named in the changelog.
- Make sure the PHP-FPM status page is not reachable from the internet. Even after patching, it should be limited to monitoring systems.
- Check container base images and platform runtimes, not just servers you manage directly. They are rebuilt on their own schedules.
- Treat PHP 8.6.0 as a planned upgrade, not an emergency. Read the migration guide, run your tests and keep security updates on your current branch until you move.

The wider lesson

A predictable release cycle and an advance warning give teams time to prepare, but only if someone already knows where each runtime is installed and how to roll it out. The changelog, not the headline severity, tells you which of your systems are actually exposed.

> Facts in this post were read from the sources listed below on 20 November 2026; this is a developing story or product and details may have changed since.

Sources and further reading

1. PHP project. PHP 8.5.13, 8.4.28, 8.3.37 and 8.2.36 released; PHP 8.6.0 released; security release pre-announcement. Read 20 November 2026. php.net
2. PHP project. PHP 8 ChangeLog, Version 8.5.13. 19 November 2026. php.net/ChangeLog-8.php
3. LWN.net. Four PHP security releases including fixes for critical vulnerabilities. 19 November 2026. lwn.net/Articles/1108552/

Published by IICTP, an independent technical credential body, on 20 November 2026. The current version of this post is at https://blogs.iictp.org/php-november-2026-security-releases-php-8-6. More guides: blogs.iictp.org.