

[Process Control Extensions](#)
[Other Basic Extensions](#)
[Other Services](#)
[Search Engine Extensions](#)
[Server Specific Extensions](#)
[Session Extensions](#)
[Text Processing](#)
[Variable and Type Related Extensions](#)
[Web Services](#)
[Windows Only Extensions](#)
[XML Manipulation](#)
[GUI Extensions](#)

Keyboard Shortcuts
?
This help
j
Next menu item
k
Previous menu item
g P
Previous man page
g n
Next man page
G
Scroll to bottom
g g
Scroll to top
g h
Goto homepage
g s
Goto search
(current page)
/
Focus search box

News Archive - 2026

Here are the most important news items we have published in 2026 on PHP.net.

21 Oct 2026

[Security advisory: Critical remote code execution vulnerabilities, update now](#)

PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35 fix two critical vulnerabilities that can allow unauthenticated remote code execution. All PHP users are strongly encouraged to update immediately.

Who is at risk: all PHP installations serving web requests, including PHP-FPM, Apache with mod_php, php-cgi, FrankenPHP and LiteSpeed. We consider the risk highest for mod_php, with a demonstrated exploit where an unauthenticated request can trigger the attack before any application code runs.

The vulnerabilities:

- **RCE via OOM corruption**, CVE-2026-109618 ([GHSA-w8hw-w9fx-j79w](#)): out-of-memory handling can interrupt PHP while internal request data is only partially initialized. Request cleanup may then treat the invalid data as valid.
- **RCE via stale global state**, CVE-2026-109619 ([GHSA-6wmf-4rv5-p3rp](#)): request-owned internal state can survive after its backing memory has been freed. A later request handled by the same worker may use that stale state before normal initialization resets it.

How to update:

- Update to PHP 8.5.12, 8.4.27, 8.3.36 or 8.2.35. Source downloads are on our [downloads page](#). Windows source and binaries are [on the same page](#).
- Linux distributions and LTS vendors received the patches in advance, so check your vendor for updated packages.
- **PHP 8.1 and older** no longer receive updates from the PHP project. Some distributions and LTS vendors provide backported fixes, so contact your vendor for details, or upgrade to a supported version.
- If you rely on the volunteer-maintained rpms, remirepo.net, we urge you to switch to distribution packages or build from source, so you can immediately apply updates. The repo will not have updates today.
- Given the severity of these vulnerabilities, the PHP security team provided minimal source-backports for [PHP 7.4](#), [PHP 8.0](#), and [PHP 8.1](#) to help people building from source or without access to an LTS vendor.

If you cannot update immediately: while only an update is a complete solution, the following measures reduce exposure to specific attack paths but do not make an installation safe.

RCE via OOM corruption (CVE-2026-109618):

- Set `memory_limit=-1`, preferably in a way applications can't override, such as `php_admin_value` in the FPM pool or Apache configuration, and check that no pool, directory or application setting puts a finite limit back. This removes the controllable PHP memory limit failure, but an underlying allocation failure can still reach the vulnerable path.
- Set a low `post_max_size`. For applications that don't require file uploads, set `post_max_size = 8M`. If file uploads are necessary, set `post_max_size = 32M`. Keep `upload_max_filesize` below `post_max_size`. Consider enforcing limits at the web server or proxy level for decoded request size, input field count, multipart part count, header count, and nesting depth. These limits must also cover requests without a usable `Content-Length`.
- Use a container or cgroup limit as an availability boundary, preferably with a policy that kills only the affected worker. Do not substitute `RLIMIT_AS` or `RLIMIT_DATA`, as these can cause the vulnerable allocation failure.

RCE via stale global state (CVE-2026-109619):

- Set `session.upload_progress.enabled=0` and restart every worker. Use `php.ini`, an FPM pool or server configuration that applies before request parsing. Do not rely on `ini_set()` or `FPM.user.ini`. This blocks the confirmed session paths but not other variants.
- On PHP 8.5, set `fatal_error_backtraces=0` and restart every worker. This blocks the confirmed fatal backtrace path only.
- Remove invalid or deprecated settings applied per request that emit diagnostics before initialization. Hiding diagnostics with `error_reporting`, `display_errors` or `@` does not help.

- Fix attacker-reachable fatal errors and execution timeouts, including failures in callbacks, upload or import processing and cleanup.

The advisories linked above have the full technical details.

21 Oct 2026

PHP 8.5.12 Released!

The PHP development team announces the immediate availability of PHP 8.5.12. **This is a security release fixing two critical vulnerabilities (CVE-2026-109618, CVE-2026-109619) that can allow unauthenticated remote code execution. All PHP 8.5 users are strongly encouraged to update immediately.**

There are no complete mitigations, updating is the only safe choice. See the [security advisory](#) for details.

For source downloads of PHP 8.5.12 please visit our [downloads page](#). Windows source and binaries can also be found [there](#). The list of changes is recorded in the [ChangeLog](#).

21 Oct 2026

PHP 8.4.27 Released!

The PHP development team announces the immediate availability of PHP 8.4.27. **This is a security release fixing two critical vulnerabilities (CVE-2026-109618, CVE-2026-109619) that can allow unauthenticated remote code execution. All PHP 8.4 users are strongly encouraged to update immediately.**

There are no complete mitigations, updating is the only safe choice. See the [security advisory](#) for details.

For source downloads of PHP 8.4.27 please visit our [downloads page](#). Windows source and binaries can also be found [there](#). The list of changes is recorded in the [ChangeLog](#).

21 Oct 2026

PHP 8.3.36 Released!

The PHP development team announces the immediate availability of PHP 8.3.36. **This is a security release fixing two critical vulnerabilities (CVE-2026-109618, CVE-2026-109619) that can allow unauthenticated remote code execution. All PHP 8.3 users are strongly encouraged to update immediately.**

There are no complete mitigations, updating is the only safe choice. See the [security advisory](#) for details.

For source downloads of PHP 8.3.36 please visit our [downloads page](#). Windows source and binaries can also be found [there](#). The list of changes is recorded in the [ChangeLog](#).

21 Oct 2026

PHP 8.2.35 Released!

The PHP development team announces the immediate availability of PHP 8.2.35. **This is a security release fixing two critical vulnerabilities (CVE-2026-109618, CVE-2026-109619) that can allow unauthenticated remote code execution. All PHP 8.2 users are strongly encouraged to update immediately.**

There are no complete mitigations, updating is the only safe choice. See the [security advisory](#) for details.

PHP 8.2 reaches end of life on 31 December 2026 and will receive no further security fixes after that date. Please plan your upgrade to a supported version.

For source downloads of PHP 8.2.35 please visit our [downloads page](#). Windows source and binaries can also be found [there](#). The list of changes is recorded in the [ChangeLog](#).

20 Oct 2026

Upcoming Critical PHP Security Release

The PHP security team would like to give advance notice of an **upcoming security release**.

It is scheduled for Wednesday, 21 October 2026 at 14:00 UTC.

It addresses two critical vulnerabilities, both rated CVSS v4.0 9.2.

All PHP users are encouraged to prepare now so they can upgrade as soon as the release is available.

We reserve the right to release earlier should details of either vulnerability become public, or should evidence of active exploitation appear in the wild.

Full details, affected versions, and the fixed versions will be published with the release.

Thank you for helping us keep PHP secure.

08 Oct 2026

PHP 8.6.0 RC3 available for testing

The PHP team is pleased to announce the first release candidate of PHP 8.6.0, RC3. This continues the PHP 8.6 release cycle, whose rough outline is specified in the [PHP Wiki](#).

Source downloads of PHP 8.6.0 RC3 are available on the [download page](#).

Please carefully test this version and report any issues found in the [GitHub Issues](#).

Please DO NOT use this version in production, it is an early test version.

For more information on the new features and other changes, you can read the [NEWS](#) file, or the [UPGRADING](#) file for a complete list of upgrading notes. These files can also be found in the release archive.

The next release will be RC4, planned for 22 October 2026.

The signatures for the release can be found in the [manifest](#) or on the [pre-release builds page](#).