

Alert Bulletin

Bulletin N.: 117

Publication Date: 21/10/2026

Subject: Alert 2026-117 Two critical vulnerabilities in PHP

Traffic Light Protocol (TLP): White

Update: 10/21/2026 11:30 AM CDMX

Affected product(s):

UPDATE: the PHP team has now released the update <https://www.php.net/downloads.php?source=Y>

PHP Branch	Affected Status	Fixed Version
PHP 8.5.x	Pending official confirmation of the affected range	Pending publication
PHP 8.4.x	Pending official confirmation of the affected range	Pending publication
PHP 8.3.x	Pending official confirmation of the affected range	Pending publication
PHP 8.2.x	Pending official confirmation of the affected range	Pending publication
PHP 8.1 and earlier	Scope pending confirmation; branches outside official PHP support	No fix announced; also verify vendor support

The affected status comes from PHP's preventive advisory; the support situation of older branches is listed in their list of unsupported versions

Description

The PHP security team announced an emergency update to fix two critical vulnerabilities, identified by researchers as CVE-2026-109618 and CVE-2026-109619, related to remote code execution. PHP assigned both a CVSS v4.0 score of 9.2 and scheduled publication for October 21, 2026 at 14:00 UTC —11:00, UTC-3—, although it could be brought forward in case of disclosure of details or evidence of exploitation.

At the time of consultation, the official advisory did not yet specify the affected versions, exploitation requirements, or fixed versions. You are urged to prepare for urgent deployment and maintain vigilance

over official channels.

Both vulnerabilities allow remote code execution (RCE), and a research team has reportedly reproduced CVE-2026-109618. Some of the information was leaked before the planned disclosure, but the manufacturer keeps complete technical details pending.

Both vulnerabilities are detailed below:

Identifier	Reported Impact	Officially Announced Score	Pending Information
CVE-2026-109618	Remote code execution; The flaw is reported to have been reproduced.	CVSS v4.0: 9.2	Technical cause, affected configurations, requirements, and fixed versions.
CVE-2026-109619	Remote code execution reported by researchers.	CVSS v4.0: 9.2	Technical cause, affected configurations, requirements, and fixed versions.

The main **risk** is that the publication of patches or a functional proof of concept (POC) will rapidly reduce the barrier to developing and automating exploitation attempts: attackers could analyze the changes, adapt tools, and perform mass scans against PHP services exposed to the Internet. Given the remote code execution potential of CVE-2026-109618 and CVE-2026-109619, a delay in remediation could facilitate the compromise of servers, the theft of information, or the installation of backdoors.

Although not all exploitation requirements are yet known, and it cannot be assured that any installation is vulnerable, a short response window should be anticipated and the immediate update of affected systems prepared, without waiting to observe attacks within your organization.

Temporary Mitigation

The recommendation shared by the well-known researcher Kostas^[1] consists of disabling upload progress tracking using the following directive in the php.ini file (if you are on PHP 8.2):

```
session.upload_progress.enabled = Off
```

This should be presented as a provisional exposure reduction measure, not as a validated solution for both CVEs. The publication itself expresses doubts about its coverage; PHP has not yet confirmed in its official advisory that this setting blocks both vulnerabilities.

Implementation Considerations

- Apply the change in the configuration used by the corresponding web service, not only in the PHP configuration for the command line.
- Reload or restart the service running PHP, depending on the architecture: PHP-FPM or Apache when using PHP as a module. Both should not be restarted indiscriminately.

- Verify the effective value through a restricted diagnostic mechanism and remove it upon completion; do not publish `phpinfo()` pages accessible from the Internet.
- Test file upload functions. The directive controls progress tracking, not the general enablement of uploads; progress bars that depend on this feature may stop working.

PHP documentation identifies this option as enabled by default and of type `INI_PERDIR`; the measure should not be attempted via an `ini_set()` within the application code.

The distinction in the capture between versions before and after PHP 8.2 also does not constitute an official impact matrix, nor does it guarantee that older versions will receive a fix.

Solution

The vendor has published security patches to mitigate the issue; you can find them at the following link:

<https://www.php.net/downloads.php?source=Y>

If you use a hosting provider as a web service provider, such as Hostinger and others, they usually perform PHP core updates automatically. Please contact the corresponding support team and validate the version.

Additional information:

- PHP — official announcement of the emergency update:
<https://www.php.net/index.php#2026-10-20-1php>
- BleepingComputer — notice and researcher statements:
<https://www.bleepingcomputer.com/news/security/php-warns-admins-of-two-critical-flaws-emergency-patches-coming-tomorrow/bleepingcomputer>
- watchTowr — tracking of CVE-2026-109618 and CVE-2026-109619:
<https://watchtowr.com/intelligence/php-cve-2026-109618-faq/watchtowr>
- PHP — documentation of `session.upload_progress.enabled`:
<https://www.php.net/manual/en/session.configuration.php#ini.session.upload-progress.enabled>
- <https://www.php.net/downloads.php?source=Y>

[1] <https://x.com/Kostastsale/status/2112774685792571463>