



HiveForce Labs

THREAT ADVISORY



VULNERABILITY REPORT

**Back-to-Back PHP Warnings Continue
With an Unpatched Code Execution Flaw**

Date of Publication

October 23, 2026

Admiralty Code

A1

TA Number

TA2026313

Summary

First Seen: October 23, 2026

Affected Products: PHP (The PHP Group)

Impact: PHP published a short informational advisory on October 23, 2026, about CVE-2026-115560, a newly assigned issue tied to the session upload progress feature that could, under an unusual configuration, let an attacker run code on a web server. The warning landed two days after PHP shipped emergency fixes for the critical PHP2Shell flaws CVE-2026-109618 and CVE-2026-109619, and this issue carries its own CVE and is not fixed by those releases, though any shared root cause with CVE-2026-109619 remains unconfirmed. PHP is not issuing an emergency release and recommends setting `session.upload_progress.enabled=0` until the fix ships in the next regular bugfix release. The configuration required for exploitation is uncommon enough that most deployments are unlikely to be exposed. No threat actor or malware has been linked to this CVE, and no exploitation has been reported.

CVE

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2026-115560	PHP Remote Code Execution Vulnerability	The PHP Group PHP			

Vulnerability Details

#1

CVE-2026-115560 is a potential remote code execution issue in PHP, disclosed by the PHP project in an informational advisory rather than a full security advisory. PHP has not yet published a technical write-up, a CWE classification, a CVSS score, or the list of affected and fixed versions, and has said it will publish the complete advisory alongside the next release.

#2

The exposure is tied to session upload progress, a feature that is enabled by default and lets an application track how far a file upload has got. PHP describes the problem as arising from an unusual combination of configuration and application behaviour rather than from the feature alone. An application must set `session.serialize_handler` to `php_binary` or `php_serialize` in its configuration, then change that setting to `php` at runtime through `ini_set()`, and make that change before it calls `session_start()`.

#3

Session upload progress must also still be enabled. Where all of those conditions hold, PHP says an unlikely remote code execution vector exists. A default PHP installation does not meet that bar on its own; session upload progress is on by default, but the runtime change to the serialize handler can only come from the application itself, which is why PHP calls the combination unlikely in practice.

#4

PHP has not explained the underlying mechanism in detail, and it has not said whether this issue shares a root cause with CVE-2026-109619, the stale global state flaw patched on October 21. What is documented is the mitigation overlap: `session.upload_progress.enabled=0` was already listed as a mitigation for [CVE-2026-109619](#), so organisations that applied it then are already covered and need to take no further action. Because the attack path depends on the application changing a session setting at runtime, the practical attack surface is far smaller than the installed base of PHP, and an application that keeps a single serialize handler throughout its lifecycle is not reachable through this path. PHP judged the setup uncommon enough to handle the fix in its regular release cycle rather than as an out-of-band emergency, a notable contrast to its handling of the two PHP2Shell flaws two days earlier.

#5

Risk evaluation is limited by what the vendor has released. No CVSS vector or base score has been published for CVE-2026-115560, no affected version range has been confirmed, and no fixed release has been named, so severity should be treated as unrated for now. There is also no evidence of exploitation: public reporting records no attacks against CVE-2026-115560, and the exploitation activity observed since October 17 targets CVE-2026-109618 and CVE-2026-109619 instead.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-115560	PHP (affected versions not disclosed by vendor)	cpe:2.3:a:php:php:*:*:*:*:*:*:*	-

Recommendations



Turn Off Session Upload Progress: Set `session.upload_progress.enabled=0` and restart every worker. Apply it through `php.ini`, an FPM pool, or a server configuration that takes effect before request parsing; do not rely on `ini_set()` or an FPM `.user.ini`, since those apply too late. If you already set this during the October 21 PHP2Shell response and left it in place, you are covered, and nothing further is needed. On side effects: this only switches off upload progress tracking, not file uploads themselves, so ordinary uploads keep working as before.



Check How Your Applications Handle the Serialize Handler: Search your codebase for calls to `ini_set()` that change `session.serialize_handler`, especially any that run before `session_start()`. If your application never changes the handler at runtime, you are not exposed through this path and can keep session upload progress enabled if you depend on it. This check is the fastest way to tell whether this advisory actually applies to you.



Confirm You Are on the October 21 Security Releases: PHP 8.5.12, 8.4.27, 8.3.36, and 8.2.35 fix the two critical PHP2Shell vulnerabilities, CVE-2026-109618 and CVE-2026-109619. They do not fix CVE-2026-115560, but they close two confirmed unauthenticated code execution holes that are already being attacked. If you are on PHP 8.1 or older, the PHP project no longer ships updates for you; contact your distribution or LTS vendor, or plan an upgrade to a supported branch.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	<u>T1190</u> : Exploit Public-Facing Application	
Execution	<u>T1059</u> : Command and Scripting Interpreter	

Patch Details

The vendor will patch the CVE in the upcoming releases.

References

<https://www.php.net/archive/2026.php#2026-10-23-1>

<https://www.hivepro.com/threat-advisory/php2shell-your-application-code-is-clean-but-the-engine-underneath-it-isnt>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of HivePro.

REPORT GENERATED ON

October 23, 2026 • 12:00 PM

© 2026 All Rights are Reserved by HivePro



More at www.hivepro.com