



| Flash |

AI-Discovered PHP Vulnerability

F-2026-10-22a

Classification: TLP:CLEAR

Criticality: HIGH

Intelligence Requirements: Vulnerability, Artificial Intelligence,

October 22, 2026

Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 7:00 AM (EDT) on October 22, 2026**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

| Flash | AI-Discovered PHP Vulnerability

| Key Findings

- On October 21, 2026, the PHP Foundation released emergency patches for two critical PHP core vulnerabilities, CVE-2026-109618 and CVE-2026-109619 (“PHP2Shell”), and allows unauthenticated remote code execution (RCE).
- Multiple parties reportedly independently discovered the flaws in August 2026 using frontier artificial intelligence (AI) models, which reportedly also reduced the effort required to build working exploits.
- ZeroFox has observed reporting of early exploitation attempts of both CVEs, urgent patching warnings from U.S. and European government agencies, and several government websites taken offline as a precaution.
- ZeroFox assesses that organizations running end-of-life PHP versions face the highest exposure risk, as no official patch is available for those versions at the time of writing.
- ZeroFox assesses with moderate confidence that exploitation of unpatched and end-of-life PHP deployments will almost certainly continue and expand in the coming weeks, and that this event will very likely accelerate AI-assisted vulnerability discovery and exploitation.

| Overview

On October 21, 2026, the PHP Foundation released emergency patches for two critical vulnerabilities in the PHP core engine, CVE-2026-109618 and CVE-2026-109619 (“PHP2Shell”), which allow unauthenticated RCE on unpatched servers.¹ The flaws were reportedly discovered with the assistance of frontier AI models, which also enabled the rapid development of working exploits.² ZeroFox assesses with moderate confidence that exploitation of unpatched systems will almost certainly continue and expand over the coming weeks.

| Details

PHP is an open-source, server-side scripting language first created in 1994 and maintained by the PHP Foundation.³ It is used by roughly 70 percent of websites—including the WordPress content management system, which reportedly powers around 40 percent of all websites.⁴ The two flaws are described as RCE through out-of-memory corruption (CVE-2026-109618) and RCE through stale global state (CVE-2026-109619), and both can be exploited without logging in.⁵

An AI red-teaming firm identified the first issue on August 1 using OpenAI’s GPT-5.6 Sol, and OpenAI’s own analysis then found additional elements of the flaw.⁶ A second cybersecurity firm reportedly found the vulnerabilities independently in August, after which the parties formed a coordinated disclosure effort with the PHP Foundation.⁷ OpenAI’s president stated that the root cause had been present for 14 years and that a limited version was identified in 2024 but was not considered significant at the time.⁸

¹ [hXXps://www.helpnetsecurity\[.\]com/2026/10/21/php2shell-php-vulnerabilities-patched-cve-2026-109618-cve-2026-109619/](https://www.helpnetsecurity.com/2026/10/21/php2shell-php-vulnerabilities-patched-cve-2026-109618-cve-2026-109619/)

² [hXXps://fortune\[.\]com/2026/10/21/ai-tools-discovered-the-php-vulnerability-that-could-take-down-70-of-the-internet-now-the-race-is-on-to-patch-it-before-ai-powered-hackers-attack/](https://fortune.com/2026/10/21/ai-tools-discovered-the-php-vulnerability-that-could-take-down-70-of-the-internet-now-the-race-is-on-to-patch-it-before-ai-powered-hackers-attack/)

³ [hXXps://thephp\[.\]foundation/](https://thephp[.]foundation/)

⁴ [hXXps://fortune\[.\]com/2026/10/21/ai-tools-discovered-the-php-vulnerability-that-could-take-down-70-of-the-internet-now-the-race-is-on-to-patch-it-before-ai-powered-hackers-attack/](https://fortune.com/2026/10/21/ai-tools-discovered-the-php-vulnerability-that-could-take-down-70-of-the-internet-now-the-race-is-on-to-patch-it-before-ai-powered-hackers-attack/)

⁵ [hXXps://github\[.\]com/serversideup/docker-php/discussions/721](https://github.com/serversideup/docker-php/discussions/721)

⁶ [hXXps://fortune\[.\]com/2026/10/21/ai-tools-discovered-the-php-vulnerability-that-could-take-down-70-of-the-internet-now-the-race-is-on-to-patch-it-before-ai-powered-hackers-attack/](https://fortune.com/2026/10/21/ai-tools-discovered-the-php-vulnerability-that-could-take-down-70-of-the-internet-now-the-race-is-on-to-patch-it-before-ai-powered-hackers-attack/)

⁷ *Ibid.*

⁸ [hXXps://mashable\[.\]com/tech/openai-takes-credit-for-finding-php-flaws](https://mashable.com/tech/openai-takes-credit-for-finding-php-flaws)

Details reportedly surfaced publicly before the planned patch release, and PHP issued fixes in versions 8.5.12, 8.4.27, 8.3.36, and 8.2.35.⁹ PHP 8.1 and earlier are end-of-life and have no official fixed release.¹⁰

Impact

ZeroFox has observed reporting of early exploitation attempts against unpatched systems from a major web infrastructure provider; however, the extent of exploitation is currently unclear. Successful exploitation would provide an attacker with an entry point into the hosting network and potential access to sensitive data. ZeroFox assesses that organizations running end-of-life PHP versions face the highest exposure risk, as no official patch is available for those versions at the time of writing.

- An initial industry analysis identified 22.6 million potentially vulnerable instances.¹¹
- The National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) Cyber Division urged affected organizations to update their current software, and the NSA advised taking systems offline where patching is not possible.¹²
- Agencies in the Netherlands and Finland reportedly took websites offline as a precaution, and the PHP Foundation described the flaws as among the most severe it has encountered.¹³

Outlook and Assessment

ZeroFox assesses with moderate confidence that mass exploitation of unpatched PHP servers will almost certainly continue through at least the coming weeks, driven by the pre-disclosure leak, the flaws' pre-authentication reach, and the large population of unpatched and end-of-life deployments. Initial activity is likely to consist of opportunistic scanning, web shell deployment, and credential theft, with initial access sales and follow-on ransomware activity likely to follow. ZeroFox assesses it is very likely that PHP2Shell will remain a long-tail exposure, as legacy systems that cannot be patched will

⁹ [hXXps://github\[.\]com/serversideup/docker-php/discussions/721](https://github.com/serversideup/docker-php/discussions/721)

¹⁰ [hXXps://laravel\[.\]com/forge/docs/knowledge-base/php-security-release-october-2026](https://laravel[.]com/forge/docs/knowledge-base/php-security-release-october-2026)

¹¹ [hXXps://fortune\[.\]com/2026/10/21/ai-tools-discovered-the-php-vulnerability-that-could-take-down-70-of-the-internet-now-the-race-is-on-to-patch-it-before-ai-powered-hackers-attack/](https://fortune[.]com/2026/10/21/ai-tools-discovered-the-php-vulnerability-that-could-take-down-70-of-the-internet-now-the-race-is-on-to-patch-it-before-ai-powered-hackers-attack/)

¹² [hXXps://www.cnn\[.\]com/2026/10/21/tech/php2shell-vulnerability-ai](https://www.cnn[.]com/2026/10/21/tech/php2shell-vulnerability-ai)

¹³ [hXXps://www.aljazeera\[.\]com/news/2026/10/22/world-leaders-warn-against-security-flaw-found-in-php-computer-programming](https://www.aljazeera[.]com/news/2026/10/22/world-leaders-warn-against-security-flaw-found-in-php-computer-programming)

persist for months, and further related disclosures are likely given the scrutiny now directed at the PHP codebase.

More broadly, ZeroFox assesses it is very likely that PHP2Shell will accelerate the use of AI by both defenders and threat actors to find and weaponize flaws in long-established codebases. The reported reduction in effort required to turn a complex memory-corruption flaw into a working exploit is likely to shorten the window between disclosure and exploitation, which will place pressure on coordinated disclosure norms and patch cycles. There is a roughly even chance that another widely deployed open-source component will be publicly linked to AI-assisted vulnerability discovery within the next six months.

| Recommendations

- **Patch immediately.** Update to PHP 8.5.12, 8.4.27, 8.3.36, or 8.2.35, and restart PHP services so the fixed code is loaded. Where PHP is supplied by an operating system or hosting vendor, confirm the vendor has shipped a patched package.
- **Inventory all PHP exposure.** Identify PHP in content management systems, container images, base images, and third-party applications, including instances that are not centrally managed. Rebuild and redeploy container images that bundle an affected version.
- **Isolate what cannot be patched.** Where patching is not immediately possible, remove the system from the internet or take it offline, in line with NSA guidance. Treat any vendor or web application firewall mitigations as interim controls only, as updating is the only complete fix.
- **Retire end-of-life versions.** PHP 8.1 and earlier reportedly have no official fixed release, and ZeroFox assesses these deployments carry the highest sustained risk. Prioritize migration to a supported version..
- **Hunt for prior compromise.** Review web server and application logs from at least October 20, when details reportedly surfaced ahead of the patch, for unusual multipart upload requests followed by memory errors or repeated HTTP 500

responses, unexplained PHP worker restarts, newly created web shells, unexpected administrator accounts, and unusual outbound connections.

- **Rotate secrets where exposure is suspected.** Because successful exploitation can expose sensitive data, rotate credentials, API keys, tokens, and session secrets on any internet-facing PHP server that was unpatched during the exposure window.
- **Shorten patch timelines for internet-facing core components.** ZeroFox assesses that AI-assisted exploit development will very likely reduce the time between disclosure and exploitation; organizations should plan for emergency patching of core runtimes within hours rather than days.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%