Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

PHP Flaw Shows How AI 'Changing The Game' In Cyber Realm

By **Allison Grande**

Law360 (November 6, 2026, 8:38 PM EST) -- Artificial intelligence's role in uncovering a critical flaw in the PHP programming language that underpins a majority of the world's websites underscores its growing power to identify and help address cybersecurity vulnerabilities — and signals that such AI-driven discoveries may only just be beginning.

Security researchers announced last month that, with the help of advanced AI systems, they had discovered PHP2Shell — a pair of computer vulnerabilities contained in the scripting language that powers around 70% of all websites, including online services, stores and booking platforms.

The threat of hackers exploiting these flaws to remotely run unauthorized software on compromised web servers set off a rush among companies and governments around the globe to patch systems to limit these risks.

The discovery also brought to the forefront the rising influence of AI in cyberspace.

While it's been widely reported that hackers are using AI-powered tools to automate, scale and accelerate their attacks, researchers are also increasingly turning to these capabilities to find flaws such as PHP2Shell, which has been active for more than a decade but until now has eluded researchers due to its complexity.

"This incident gives us a glimpse into how cybersecurity is changing in real time and how AI is really changing the game," said Dan Altieri, a partner on the privacy and data security team at Harter Secrest & Emery LLP. "AI is being used for both good and bad, but in both cases, it can really do in no time whatsoever what would take human beings decades to do, if they could ever do it at all."

Given how much "faster and cheaper" AI makes catching and taking advantage of both new and existing vulnerabilities, the technology is likely to remain a key tool for those on both sides of the cyber arms race for the foreseeable future, said Austin Berglas, managing director and head of cyber operations at global investigations firm Nardello & Co.

"PHP2Shell is far from a one-off and more like a preview," said Berglas, who formerly served as head of the FBI's New York cyber branch.

Cybersecurity experts, including Berglas, have likened the PHP flaw to the **2014 disclosure** of the Heartbleed vulnerability that compromised the encryption technology relied on by roughly two-thirds of

all websites, and the revelation in late 2021 of a vulnerability in Apache Log4j, a popular Java-based logging library used across millions of enterprise applications and web servers worldwide, Berglas noted.

However, the involvement of AI tools to uncover the PHP flaw sets the latest event apart by significantly shortening the time needed to unearth vulnerabilities that were previously difficult for both security researchers and bad actors to identify, experts say.

"The PHP incident proves that AI will drastically accelerate the timeline between the discovery of these zero-day vulnerabilities and their weaponization, giving the defenders only a short window to act to protect their systems," said Matthew F. Ferraro, a partner in the privacy and cybersecurity group at Crowell & Moring LLP.

Ferraro agreed that the central role that AI played in the PHP incident is likely to be "a harbinger of what's to come," especially as these models continue to become more capable and autonomous.

Regulation and Enforcement Ahead

The attention that the discovery of the PHP flaw is drawing to AI's capabilities is likely to "amp up" efforts to regulate the emerging technology in both the U.S. and abroad, Ferraro said.

"Generally speaking, regulation is moving toward being more aggressive to try to mitigate alleged AI harms, including those related to children or vulnerable communities and concerns involving cybersecurity risks posed by these models," he said. "There appears to be a growing concern in the U.S. around the potential downsides of AI, and that gives fertile ground to politicians, regulators and litigants for taking action that gives them a say in how these products are both developed and deployed."

Amid growing reports of autonomous AI agents from major labs such as OpenAI and Anthropic having gone "rogue" and bypassing safety guardrails to breach private and governmental entities, policymakers have moved to place checks on AI's cyber capabilities and risks. These initiatives include an executive order issued by President Donald Trump earlier this year to encourage AI developers to give the government access to models up to 30 days before their planned release to test for and identify cybersecurity vulnerabilities.

Congress has also put forth several bills and initiatives focused on how AI is used to detect, track and manage cyber vulnerabilities, including a bipartisan proposal floated in June to require the federal government to establish a voluntary reporting program for AI developers to disclose, track and remediate AI-related flaws.

This work is projected to continue in the next Congress. After Democrats regained control of the U.S. Senate and U.S. House of Representatives in Tuesday's midterm elections, Rep. Ted Lieu, D-Calif., who serves as vice-chair of the House Democratic Caucus and co-chair of the House Democratic Commission on AI, criticized the current leadership's "conscious decision" to "let the AI industry run wild."

During a press conference Wednesday, Lieu vowed that the Democratic majority in the next term would hold hearings on AI and pass legislation to impose "reasonable guardrails" on the technology.

Given the typically slow pace of lawmakers, attorneys say that they're also expecting increased enforcement by regulators that already have authority under existing statutes, such as Section 5 of

the Federal Trade Commission Act and state breach notification laws, to go after companies that fail to adequately protect personal data or mislead the public about the safeguards they have in place.

"Particularly when it comes to a very well-publicized vulnerability like this, the risk is not that a company was running their website with vulnerable software," said Altieri of Harter Secrest. "The risk is not addressing that vulnerable software when the issue has become known."

A Duty to Patch

When it comes to the PHP vulnerability, the primary step that impacted entities will likely be expected to take is to apply the patches that have been released to fix the flaws, experts noted.

"Anybody who is running a website with this vulnerable software is now on notice that continuing to run it with that vulnerability and without implementing the necessary patches could result in fairly significant issues," Altieri said.

Regulations such as the FTC's Safeguards Rule, the New York Department of Financial Services' cybersecurity regulation and the European Union's Cyber Resilience Act require timely patching as a core component of maintaining an effective information security program, and timelines for these efforts are likely to further constrict following incidents such as the PHP flaw, Nardello & Co.'s Berglas said.

"Regulators and agencies will insist on much shorter patching cycles," Berglas said, adding that the three-day federal deadline for patching "high-risk" vulnerabilities that was recently set by the Cybersecurity and Infrastructure Security Agency "signals where expectations are heading."

Both the regulatory and operational consequences are likely to be significant for failing to patch the PHP flaws, which, if exploited, could allow hackers to gain remote access to a website host and engage in nefarious activities, such as stealing customer information, installing malware and creating backdoors.

The vulnerabilities were discovered by researchers using advanced AI models developed by OpenAI and Google during a recent audit of PHP's source code. The review was funded by OpenAI as part of its Patch the Planet initiative, which is designed to help open-source projects identify and fix critical flaws before hackers can weaponize them.

"It's not particularly easy to find vulnerabilities in code, which is complicated and massive," Crowell & Moring's Ferraro said. "The game changer here is that these AI models can find those needles in a haystack much more quickly and autonomously than was ever possible in the past."

Given that AI models can be used for both cyber defensive and offensive purposes, it's vital that companies take steps to prepare for and be ready to quickly respond to such threats, including segmenting and fortifying their systems so that vital information isn't all accessible in one place, and having in place a program to swiftly deploy necessary patches and other remedies, attorneys say.

Additionally, because the PHP flaws were disclosed before patches could be fully deployed, website operators that run PHP software should be checking to make sure not only that any security gaps have been closed, but also that hackers weren't able to get into their systems before the fixes were implemented, Altieri said.

"Because AI is being leveraged by the bad guys as well, that means that companies are on the clock much sooner than they were in the past and there's really no time to employ the ostrich tactic, which is sticking your head in the sand and putting off until tomorrow what you know about today," Altieri said.

The AI-assisted discovery of the PHP flaw will also likely enhance long-standing calls for companies and governments around the world to engage in information-sharing about potential cyberthreats and the best practices being used to combat vulnerabilities, according to experts.

"When one company becomes aware of a vulnerability like this that may affect others, the idea is that information sharing can drive massive remediations at scale, which may result in more pushes from regulators for help with information-sharing as time goes on," Altieri said.

The PHP incident also further intensifies the importance of implementing robust vendor management procedures, given that such a widespread flaw that impacts potentially millions of websites gives hackers a variety of potential entry points to exploit, experts say.

"Companies can devote as many resources as possible getting their side of the fence in order, but the reality is, if they're working with a vendor, they're only as good as the security of that vendor," Altieri said. "So if a vendor is getting access to a company's information or network, then that company needs to be sure the vendor is taking security as seriously as it does and that any necessary patches are being implemented."

--Editing by Nicole Bleier and Jay Jackson Jr.

All Content © 2003-2026, Portfolio Media, Inc.