LAW360

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

Global Webpage Flaw Unlikely To Spur Big Insurance Losses

By **Abraham Gross**

Law360 (October 29, 2026, 8:02 PM EDT) -- The recent revelation that a majority of the world's websites contain a vulnerability that can expose them to considerable risk has resulted in significant disruption and fears that, in all likelihood, the insurance industry will largely shrug off, attorneys said.

On Oct. 20, researchers announced that with the help of advanced AI systems, they had discovered PHP2Shell — a pair of computer vulnerabilities with a scripting language used as the basis for up to 70% of websites.

The vulnerabilities, if exploited, could allow hackers to gain remote access to a website host and run unauthorized software, stealing information, compromising users or creating further backdoors.

While cybersecurity experts say the exposure was substantial and a harbinger of future AI-assisted attacks exposing otherwise obscure faults across systems, insurance counsel told Law360 that the disruption was unlikely to result in a significant number of claims — at least for now.

As with the discovery of a defect in a mass-manufactured lock, it is unclear whether and when anyone had entered once-secure doors and what, if anything, they had taken or left behind.

Amazon Threat Intelligence announced last week that it had isolated an attempted exploit of PHP2Shell on Oct. 17, marking the outer boundary of when security experts should begin investigating potential compromises.

The announcement also advised that the PHP vulnerabilities demonstrated that, with the help of AI-assisted analysis, "more actors can act within hours or even minutes once technical details of a vulnerability are disclosed."

Laurie Kamaiko of Saul Ewing LLP, who represents insurers, said that under most cyberinsurance policies, the discovery of a significant vulnerability would not by itself constitute an insurable event absent a showing that the vulnerability has been exploited.

"There being a vulnerability alone is not necessarily going to be a triggering event," Kamaiko said. "What you want to be looking at is: Has there been a bad actor that is taking advantage of it and entering your computer system and doing something?"

That will likely leave policyholders shouldering the costs associated with patching PHP2Shell and website

downtime.

The burden for patching a website can vary greatly depending on the size and capabilities of the organization and the current state of its affected systems, according to Amy Mushahwar, chair of Lowenstein Sandler's data privacy, security safety and risk management practice.

"Most companies that have good web architecture have high availability architecture, where they can take down a segment of sites, patch that segment, and then take down another subset of a segment of sites and patch it, so that you have a rolling patch window so you don't have an outage," she told Law360.

Not all companies may have the ability to take down their servers immediately, Mushahwar said, adding that taking inventory of where PHP exists within an enterprise and patching an actively operating system is a time-consuming process.

Moreover, as of Thursday, not all the older versions of PHP that contain the two vulnerabilities have patches available, meaning that organizations using those legacy versions may have to first update to a later version before patching.

"Usually there's lots of different versions of software within your large enterprise, and if you've got the budget and handling to standardize, that's excellent," she said. "But most companies, on top of having large enterprises, are also constantly acquiring companies, so there's a bit of enterprise variation in most organizations."

While cyberinsurance policies may offer only limited relief for the immediate costs of patching PHP2Shell, carrier-side attorney Judith Selby of TittmannWeix said policyholders may also be exposed by their dependence on vendors and third parties and can look to their contractual obligations for support.

"It highlights the importance of your technology agreements and your indemnities and insurance provisions, waivers — all kinds of things like that, dealing with risk transfer — because that could be another source of recovery," she said.

If a policyholder finds that a hacker breached its systems before a patch, it has to be aware of any representations it may have made to its insurers about how it manages patches to avoid claims of misrepresentations, according to policyholder attorney Emily Garrison of Morgan Lewis & Bockius LLP.

"Even if an organization has an unpatched vulnerability, an insurer can't necessarily rely on that fact to deny coverage for an unrelated incident — the insurer may need to establish the connection between the failure to patch and the resulting loss," she added.

Another issue policyholders will likely face is when to provide notice to insurers of a potential covered incident.

Insurance experts who spoke to Law360 concurred that discovering a vulnerability would not meet the threshold for notifying insurers under most policies, but it was less clear when a potential breach crossed that line.

"We all have people attempting to break into our system: The issue is whether they have," said Kamaiko. "And if they have succeeded, what damage has that caused?"

Andrea DeField, head of Hunton Andrews Kurth LLP's cyberinsurance practice, said that since cyber insurers often look to policyholders that have a formalized incident response plan, activating that plan in response to a suspected intrusion is a good indicator for when to provide notice.

"If you internally believe this has now risen to the level of being an incident sufficient to trigger your internal reporting and plan and processes, it's probably a good time to give notice under your cyber policy," she told Law360.

DeField noted that companies with cyberinsurance are more likely to have more robust cybersecurity than those without coverage, both because they are aware enough of their risks and because insurers encourage a certain level of cybersecurity and protocols.

As for how the PHP event will shape the relationship between cyber insurers and policyholders, Selby said that it would not likely lead to restricted coverage terms, given the sheer number of competitors in the cyberinsurance space.

"When you're dealing with a soft market on any line of insurance, that's a tough time to start tightening up coverage, because people say, 'I'll go down the street to your competitor and get their policy,'" she added.

Cybersecurity experts, including Mushahwar, have said PHP2Shell illustrates the ways that AI can be used by both hackers and cybersecurity experts to discover vulnerabilities much faster than they otherwise would have.

DeField said that the insurance industry may already be seeing the impact of AI-assisted attacks by the growing volume of cyber claims.

Still, she told Law360 that policyholders are likely on a better security footing following a raft of ransomware attacks that peaked in 2021. The experience drove many companies to improve their security controls and create more backups, leading to less downtime and fewer large business interruption claims, according to DeField.

"I think there's obviously going to be a lag as we see controls step up to handle all these new types of exploits, but we are certainly seeing significant hardening and improvement amongst policyholders that is helping drive down many of those costs," she said.

--Editing by Bruce Goldman and Amy Rowe.

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