

THE ALS GROUP

Managing Risk to Influence Successful Outcomes

PHP2Shell: Would Your Cyber Insurance Cover a Website Shutdown?

Key Takeaways

- PHP2Shell is a pair of critical flaws in PHP, the language behind roughly 70% of websites, and organizations worldwide took sites offline to patch.
- The patch is IT's job, but the fallout (lost revenue, notifications, contract disputes and a claim that may or may not get paid) lands on leadership.
- Check five things this week: business interruption wording, patching conditions, vendor contracts, your cyber application and notice requirements.

"Hope is not a strategy."

On October 21, 2026, the U.S. National Security Agency and Europe's cybersecurity agency told businesses to act immediately on two critical flaws in PHP, the programming language behind roughly 70% of the world's websites, including WordPress and Drupal. Within a day, government sites across Europe, a major Japanese airline, a railway operator and Japan's largest bank had pulled pages offline while they patched. Even Wikipedia took systems down as a precaution.

The flaws, now called "PHP2Shell," had been sitting in the code for more than a decade. What changed? Researchers used AI to turn them into a working attack. According to Wiz, one of the security firms involved, a single researcher did in a week what used to take a top team months.

If your company has a website, a client portal, an online payment page, or a vendor that runs any of those for you, this is your issue too. And it isn't only an IT issue. It's a risk management issue.

Why a Software Bug Belongs on the CFO's Desk

Most people assume a cyber event is the IT department's problem. They are only partially correct. The patch is IT's job. The fallout (lost revenue, customer notifications, contract disputes and a claim that may or may not get paid) lands on leadership.

Simply put, PHP2Shell could let an attacker take over a website and read memory holding passwords and other sensitive data. That's a potential data breach, a business interruption and a liability claim, all from code you never wrote.

Five Questions to Ask This Week

Business Interruption: Would your cyber policy pay for lost income from a shutdown you chose, before anyone actually attacked you? Organizations around the world took their own sites offline to patch. Many policies tie business interruption coverage to an actual "security failure," and a voluntary or precautionary shutdown may fall outside that wording. Find out now, not after.

New Jersey
175 Main St
Woodbridge, NJ 07095
+1.732.395.4250

Florida
1800 NW Corporate Blvd Ste 202
Boca Raton, FL 33431
+1.561.437.0024

info@thealsgroup.com
thealsgroup.com



Patching Conditions: Does your policy penalize you for being slow to patch? Some cyber policies exclude or reduce coverage for losses caused by known vulnerabilities that weren't patched within a set window. The clock started when the PHP fix was released, so know exactly how much time your policy gives you.

Your Vendors: Who is responsible if your web developer or host falls behind? If an outside provider runs your site, their delay is your exposure. Check your contracts for patching responsibilities, response times, who pays if their system is the open door, and whether they carry cyber and technology errors and omissions ("Tech E&O") coverage that protects you.

Your Application: Does your last cyber application still match reality? Cyber applications ask how you manage software updates. If your answers don't match how things actually work, that gap can turn into a coverage dispute.

Notice: Do you know who to call, and when? Most cyber policies require prompt notice of a potential incident, and many require you to use the carrier's approved vendors. Check your policy before you hire outside help.

The Bigger Lesson: AI Changes the Clock

Wiz called this an "AI inflection point." We agree, and the takeaway for business owners is simple: the time between a flaw being found and a flaw being used is shrinking fast. Risks that sat quietly for years can go live overnight. A cyber program reviewed once a year against yesterday's threats won't keep pace.

Question everything. Especially the forms.

How ALS Helps

We read the forms. When an event like PHP2Shell hits, we test your cyber policy against the real-world scenario: whether business interruption responds to a precautionary shutdown, what the patching and notice conditions require, and where the gaps are. We also review your technology and vendor contracts so the risk sits with the party that controls it. Because we don't sell insurance or take commissions, our only job is making sure your coverage responds when you need it.

There you have it: one bug, five questions and a good reason to look at your cyber program before the next headline.

Frequently Asked Questions

What is PHP2Shell? PHP2Shell is the name given to two critical flaws in PHP, the programming language that runs most of the web. Disclosed in October 2026, the flaws could let attackers run their own code on a website and read sensitive data like passwords. A patch is available, and government cybersecurity agencies urged immediate action.

My website runs on WordPress. Am I affected? WordPress is built on PHP, so it's worth confirming. Ask your web developer or hosting company, in writing, whether your site's PHP version has been updated with the fix and when. Keep that confirmation on file; it can matter later if there is ever a claim.

Does cyber insurance cover a voluntary website shutdown? It depends on the wording. Some policies only pay business interruption losses after an actual breach or "security failure," while others include coverage for precautionary or voluntary shutdowns. The difference can be significant, and it's a question best answered before you pull the plug.

Who is responsible if my web developer or host doesn't patch in time? That comes down to your contract. A well-written technology agreement spells out patching responsibilities, response times, indemnification and the vendor's own insurance. Many small and midsize businesses have none of that in writing, which leaves the risk with them by default.



How does The ALS Group help with cyber risk? We act as your "outsourced" risk manager. We review your cyber coverage, applications and vendor contracts together, so the pieces actually fit, and we hold brokers and carriers accountable for coverage that matches how your business really operates.

Not sure how your cyber policy would respond to a precautionary shutdown, an unpatched vulnerability or a vendor's mistake? Let us read it before a claim does. Contact our Managing Principal, Albert Sica, at asica@thealsgroup.com or at 561.437.0024 to set up a review of your cyber coverage.