



Urgent – A Security Flaw Affecting Most Websites Needs Your Attention Today

A serious security problem was made public today that likely affects your company's website and any online services you operate. Please forward this to whomever manages your website or IT.

What Happened, in Plain Terms

Most of the world's websites, roughly seven out of 10, are built using a programming language called PHP. Think of it as the engine running under the hood of your website. It's largely invisible to you, but it's there.

Today, the organization that maintains PHP released an emergency fix for two newly discovered flaws in that engine. Security researchers rated the flaws to be about as severe as a flaw can be rated.

Here's Why These Flaws Matter:

An attacker needs no password and no account. They don't have to trick an employee or steal credentials. They can simply send a request to your website, and through that request, the attacker can take control.

They can take control of the server running your site – reading data, altering your site, or using it as a foothold into your network.

They can also read whatever is sitting in the server's memory, which often includes passwords, access keys, and digital certificates belonging to your business and your customers.

This is not a flaw in your website's design. Even a perfectly built, well-maintained site is affected, because the problem is with the underlying engine. Nothing your team did wrong caused this, and no amount of good coding on your end prevents it.

Attacks have already been observed. Government agencies across Europe took their websites offline as a precaution while waiting for the fix. This is an active threat, not a theoretical risk.

What To Do Now

- **Install the update today.** Your IT team or web host needs to update PHP immediately. The maintainers of PHP have been blunt: partial workarounds don't fully protect you. Updating is the only real fix.
- **Ask about older systems.** Some older versions of the software no longer receive official updates. If you're running one, you need a plan this week – not this quarter.
- **Change your passwords and keys.** Because attackers could have read sensitive information out of memory, assume anything stored on an exposed system may have been seen. Rotate passwords, access keys, and certificates.
- **Check your vendors.** Your own system may be fine while a vendor holding your data is exposed. Ask them in writing to confirm that they've applied the fix.
- **Call us if you see anything suspicious.** If there are signs of a breach, legal notification deadlines can start running quickly under state law, industry regulations, and your own contracts. Bringing in counsel early also helps protect the confidentiality of the investigation.

Why Is This Different From Every Other Software Bug? Artificial Intelligence (AI) Found This Flaw

This problem has been hiding in plain sight for more than a decade. Human security experts had looked at this part of the code before – one developer examined it as recently as 2024 – and concluded it was too difficult for an attacker to exploit. They moved on.

Earlier this year, AI tools found it. Two separate security teams, working independently, used advanced AI models to analyze the code and uncovered what

human reviewers had set aside for years.

For Business Leaders, There Are Four Practical Takeaways:

1. **Expect this to happen more often.** This is the second large-scale emergency patch in a few months driven by an AI discovery. Long-dormant flaws in trusted, mature software are now being surfaced at a pace we have never seen. Emergency patching is becoming routine, not exceptional.
2. **The time you have to react is shrinking.** The same tools that find flaws help attackers exploit them. Researchers now measure the gap between a flaw becoming public and attacks beginning in minutes, not weeks. If your IT policy allows 30 or 90 days to apply critical updates, that policy is out of date for any system facing the internet.
3. **The legal standard is moving.** Contracts and regulations routinely require “reasonable” or “industry standard” security. That bar rises as AI-assisted code review becomes cheap and common. Expect regulators, plaintiffs’ lawyers, insurers, and business partners to start asking a harder question after an incident: Why wasn’t this found?
4. **Your contracts need a second look.** Agreements with software vendors and cloud providers often contain patching deadlines, breach notice timelines, and liability terms written for a slower world. We’d encourage a review.
5. **Respond to a breach.** Data breaches happen and responding to them technically and legally needs to happen quickly. Reach out if you have (or think you may have) suffered a breach. But if it hasn’t happened yet, we encourage everyone to prepare now and hope your preparation isn’t needed instead of hoping a breach never happens.

How We Can Help

Our Privacy and Cybersecurity team can assist with breach notification analysis, incident response planning, vendor contract review, regulatory inquiries, and insurance claims. Please contact Gregory Ewing, Aaron Minster, or reach out to your regular contact at the firm.

This blog was drafted by [Greg Ewing](#) and [Aaron Minster](#), attorneys in the Spencer Fane Washington, D.C. and Minneapolis offices. For more information, visit

www.spencerfane.com.

Technical reference for IT:

CVE-2026-109618 and CVE-2026-109619, known as PHP2Shell.

Patched releases are PHP 8.5.12, 8.4.27, 8.3.36, and 8.2.35.

Click [here](#) to subscribe to Spencer Fane communications to ensure you receive timely updates like this directly in your inbox.