SMBTeam

LAW FIRM WEBSITE SECURITY

PHP Security Playbook

Is your law firm's website at risk?

What the October 2026 PHP security emergency means for your law firm, and exactly what to do about it.

> **URGENT**
>
> Two critical vulnerabilities were disclosed on October 21, 2026.
>
> Both are rated 9.2 out of 10 in severity, near the highest possible score.
>
> **If your site runs on WordPress and isn't patched yet, an attacker could reach your contact forms, lead data, and client intake information without ever needing a password.**

This playbook explains what happened, what's at risk, and what to do right now.

What happened, in plain English 2

What a hacker could do to your firm's site 3

Is your site affected? How to check right now 4

Why your WordPress plugins can't save you 5

What to do right now, step by step 6

Quick security checklist 7

THE SITUATION

01 What happened, in plain English

A flaw in the engine that runs most of the internet

About 70% of all websites in the world, including most WordPress sites, run on a computer language called PHP. Visitors never see it. PHP is the engine running underneath your site, processing every form submission, handling every page load, and managing every interaction a potential client has with your firm online.

On October 21, 2026, the people who build PHP disclosed two critical security flaws that had been sitting in the software. Security researchers found the details leaked before an official fix was ready, so the PHP team had to rush out emergency patches for both vulnerabilities at the same time.

THE TWO VULNERABILITIES	WHAT THEY ALLOW AN ATTACKER TO DO
CVE-2026-109618 RCE via out-of-memory corruption	If PHP runs out of memory at the wrong moment, an attacker can exploit incomplete cleanup to run their own code on your web server, with no password.
CVE-2026-109619 RCE via stale global state	Leftover data from one request can be read and exploited by a later request, letting an attacker insert malicious code before your website loads.

WHAT RCE MEANS

RCE stands for Remote Code Execution.

An attacker can run their own software on your web server from anywhere in the world, without logging in and without a password.

In the worst case, they can do it before your website or any security plugin even knows they're there.

Both CVEs are rated 9.2 out of 10 in severity, which security experts classify as critical.

THE RISK

02 What a hacker could actually do to your firm's site

This isn't abstract. It's your client data, your leads, and your reputation.

If a hacker exploits either of these vulnerabilities on your site, the consequences go well beyond a defaced homepage. They'd be running code with the same privileges as your website's software, so they can reach everything your site can reach.

What an attacker can access if your site isn't patched

- Your database credentials, including full access to every record your site stores
- Your **wp-config.php** file, the master key to your entire WordPress installation
- Every lead form submission, contact form entry, and intake response collected on your site
- Your full database: case inquiry details, client names, phone numbers, and email addresses
- The ability to modify your site files, inject malware, or install a backdoor for later access

The attacker doesn't automatically gain control of your entire server or network. But they'd have everything they need to steal client data, hold your site for ransom, or silently harvest leads for weeks without you knowing.

9.2
OUT OF 10
SEVERITY

Both flaws are rated **CRITICAL**, near the top of the scale, and neither needs a password to exploit.

Your site is often the first place a potential client goes during one of the hardest moments of their life. They share personal information. They decide whether to trust you. A compromised site puts that trust, and that data, directly at risk.

THE CHECK

03 Is your site affected? How to check right now

The answer depends on your PHP version and your host.

Every WordPress site runs on PHP. The question is whether yours runs a version that already has the emergency patch. Here's which versions are safe and which aren't.

PHP VERSION	FIX AVAILABLE?	STATUS	ACTION REQUIRED
8.5	8.5.12	Fully patched	Update immediately
8.4	8.4.27	Fully patched	Update immediately
8.3	8.3.36	Fully patched	Update immediately
8.2	8.2.35	Patched (EOL Dec 2026)	Update, then plan an upgrade to 8.3+
8.1 / 8.0	Vendor builds only	No official release	Upgrade to 8.3 or 8.4 now
7.4 and older	Vendor builds only	End of life, high risk	Upgrade to 8.3 or 8.4 now

How to check which PHP version your site runs

- Log into your WordPress dashboard
- Go to **Tools > Site Health > Info > Server**
- Look for the PHP version listed there

> **IMPORTANT**
>
> If your hosting provider applied a backport patch, your version number may not match the fixed releases above. Your host may have pushed the fix to an older-looking version number.
>
> **When in doubt, ask your host: "Has my site been patched for CVE-2026-109618 and CVE-2026-109619?"**

THE CATCH

04 Why your WordPress plugins can't save you

Security plugins only load after WordPress, and this attack hits before that.

If you've got a security plugin like Wordfence, WP Cerber, or iThemes Security, you may assume it'll catch this. It won't. Here's why.

> **THE ATTACK CAN HAPPEN BEFORE WORDPRESS EVEN LOADS**
>
> The most dangerous attack path targets Apache with mod_php, one of the most common server setups for WordPress hosting.
>
> **The flaw can be triggered and exploited before WordPress launches, before your theme runs, and before any plugin starts.**
>
> **Your security plugin never gets a chance to see the request.**

A Web Application Firewall (WAF) at the network level may block some attack patterns. But security researchers have confirmed attackers are already changing their payloads to get around firewall rules. A firewall isn't a substitute for patching. The only real fix is an updated PHP build.

What definitely does NOT fix this

- Updating WordPress core
- Updating your plugins or themes
- Changing PHP settings inside WordPress (wp-config.php, .htaccess, plugins)
- Running a malware scan, which finds existing infections but doesn't prevent new ones

> **WHERE THE FIX LIVES**
>
> **The fix has to happen at the server level, not inside WordPress.**
>
> Your host is responsible for this. If you manage your own server or VPS, you need to update PHP yourself and restart your web server software.
>
> **Only an updated PHP build closes the hole.**

THE PLAN

05 What to do right now, step by step

A clear action plan for law firm owners

1 Find out who manages your website hosting.

If a web developer, IT contact, or agency manages your site, contact them today and ask: **"Has my PHP been updated to patch CVE-2026-109618 and CVE-2026-109619? Have PHP workers been restarted?"** Don't accept "we're looking into it." You need a confirmed yes or a timeline.

2 Check your PHP version in WordPress.

Go to Tools > Site Health > Info > Server and note the PHP version. Compare it to the patched versions in the table on page 4. If your version is below the fixed release and your host hasn't confirmed a backport, escalate immediately.

3 Make sure your site and database are backed up.

Before any PHP update or server change, confirm your host has a recent backup of your site files and database. If you're not sure, ask your host or check your hosting control panel. An off-server backup is best, not just one stored on the same server being patched.

4 If you're on PHP 7.4 or older, treat this as an emergency upgrade.

PHP 7.4, 8.0, and 8.1 have no official upstream fix. Vendors like WP Engine and some Linux distributions have released backport patches for managed hosting customers. If you're on unmanaged hosting, upgrade to PHP 8.2 or higher immediately. Test on a staging environment first, and contact your host if you're unsure how.

5 Confirm that PHP workers were restarted after patching.

Installing the patched PHP build isn't enough on its own. The old code stays in memory until PHP-FPM, Apache, or LiteSpeed is restarted. Ask your host to confirm workers were restarted after the patch was applied. A PHP update without a restart isn't a complete fix.

IF YOU'RE AN SMB TEAM CLIENT

You're already protected.

We checked every SMB Team client site on October 21, 2026, the day the vulnerabilities were disclosed. Every single one was already running PHP 8.2 or higher, so every site received the emergency fix. Our hosting partner WP Engine rolled the patch out across the Flywheel platform right away, and PHP workers were restarted automatically. You didn't have to do anything.

Your job is to run your law firm. Our job is to keep the technical foundation under your site secure while you do.

DO IT TODAY

06 Quick security checklist

- [ ] Confirm which PHP version your site runs (Tools > Site Health > Info > Server)
- [ ] Ask your host or web manager for written confirmation that CVE-2026-109618 and CVE-2026-109619 have been patched
- [ ] Ask whether PHP workers were restarted after the patch was applied
- [ ] If you're on PHP 7.4 or older, schedule an immediate upgrade to PHP 8.3 or 8.4
- [ ] Verify your site and database backups are current and stored off-server
- [ ] If you suspect your site was already compromised, contact your host before making any changes. Don't patch or scan first.

SMBTeam

Scale your law firm across leads, intake, operations, and finance

Learn more