

Abrams PHP2Shell Owner Checklist

Free guide from Abrams Grp LLP — Abrams Patch Assist

Version: 2026-10-23 · **Seller:** Abrams Grp LLP (OC437246) · VAT GB400170172

Contact: info@abramsgrp.com · +44 115 777 0127

Page: <https://abramsgrp.com/business-services/php-patch/>

This checklist helps organisation owners and website operators verify exposure to **PHP2Shell** (CVE-2026-109618 and CVE-2026-109619) and record evidence of patching. It is **not** a penetration test, **not** incident response, and **not** Cyber Essentials certification for your organisation.

Authoritative references: CISA alert of 21 October 2026; PHP security release of 21 October 2026; fixed builds listed by the PHP project.

1. What PHP2Shell is (plain English)

On 21 October 2026 the PHP project released emergency fixes for two critical flaws in the **PHP runtime** that serves web requests. Both are scored **CVSS 9.2**. Unauthenticated attackers may be able to run code on a vulnerable server or disclose memory from the PHP worker.

These flaws are in **PHP itself**, not in WordPress plugins or themes. Updating plugins alone does **not** fix PHP2Shell.

Fixed upstream builds (confirm your host's exact package):

PHP branch	Fixed release
8.5	8.5.12 or later
8.4	8.4.27 or later
8.3	8.3.36 or later
8.2	8.2.35 or later

PHP **8.1 and earlier** are end-of-life for this fix stream from the PHP project. Plan a supported upgrade, a vendor backport, or take internet-facing PHP offline until remediated (per CISA).

2. Inventory worksheet

List every place PHP may run. Prioritise anything reachable from the public internet.

#	Host-name / URL	Role (prod / staging / tool)	Who manages PHP?	man-ages PHP?	PHP version shown	Workers restarted?	Notes
1							
2							
3							
4							
5							

Also tick:

- ☐ Production website(s)
- ☐ Staging / UAT / “old redesign” copies
- ☐ Forgotten subdomains
- ☐ Containers / Docker images used in deploy
- ☐ Hosting control panels that embed PHP
- ☐ Vendor appliances or admin tools that run PHP

3. Host email template (copy and send)

Use this when a host or agency manages PHP for you.

Subject: Confirm PHP2Shell (CVE-2026-109618 / CVE-2026-109619) fix on [YOUR DOMAIN]

Hello,

Please confirm for the PHP runtime that serves live traffic for [YOUR DOMAIN]:

1. Whether that runtime includes the fixes for CVE-2026-109618 and CVE-2026-109619
(or a vendor build with those fixes backported), and the exact version string.
2. Whether PHP workers / FPM pools / the web PHP process were restarted after the update.
3. If not yet complete, the expected completion time.
4. If we are on PHP 8.1 or older, which supported version you recommend.

A reply that “WordPress is up to date” does not answer this question – we need the PHP runtime status.

Thank you,
[YOUR NAME]
[ORGANISATION]

Record the reply date and the version string they give.

4. After the patch — verify

1. Confirm the **running** PHP version (not only a package install message). In WordPress: **Tools** → **Site Health** → **Info** → **Server**.
2. Restart evidence: ask the host, or restart PHP-FPM / the pool yourself if you manage the server.
3. Smoke-test what makes money or trust:
 - ☐ Homepage / key landing pages load
 - ☐ Login works
 - ☐ Contact / forms submit
 - ☐ If WooCommerce: product → cart → checkout (use payment sandbox where possible)
 - ☐ Scheduled jobs / cron still run
4. Write down: previous version, new version, date/time, who verified.

Interim mitigations (WAF rules, php.ini tweaks published by vendors) may reduce risk but **do not replace** a fixed runtime.

5. When to stop DIY and book Abrams Patch Assist

Book paid help when any of these apply:

- You manage a **VPS or dedicated** server and are unsure how to patch and verify safely.
- You have **multiple sites** or unclear staging copies.
- The host's answer is vague or contradicts Site Health.
- You need a written inventory and patch plan for directors or insurers (**Exposure Check**).
- You want Abrams to apply or coordinate the patch under **time-boxed, revocable access** (**Patch & Verify**).

Packages (GBP, include UK VAT 20%)

Package	Price	Scope
Exposure Check	£349	1 site — inventory + written plan
Patch & Verify	£899	1 site — patch/coordinate + verify + revoke access
Multi-site Patch	£1,999	Up to 5 sites, same legal entity
Runtime Watch	£249 / month	Up to 3 sites — version watch + priority window

Portal: <https://access.abramsgroup.com/patch>

Or email: info@abramsgroup.com · Phone: +44 115 777 0127

Abrams Patch Assist does **not** sell incident response, forensics, managed vulnerability management platforms, or cyber-insurance readiness as this product line.

6. After-patch signals that need a separate conversation

If you see unexpected administrator accounts, unknown PHP files under uploads, unexplained redirects, or content you did not publish, treat that as a **possible compromise** question — separate from “are we on a fixed PHP build?”. Do not rely on this free checklist for forensics. Contact Abrams for a separately scoped discussion, or your specialist incident provider.

Footer

© Abrams Grp LLP · Enterprise House, David Lane, Basford, Nottingham NG6 0JU, United Kingdom.

This guide may be shared internally. Do not rebrand as a certification. Evidence for security marks (for example Cyber Essentials) must come from the relevant scheme — not from completing this checklist alone.