

PHP2SHELL

Confirm. Patch. Verify.

Two critical PHP flaws were patched on October 21, 2026. Arrange the runtime update with your host; a WordPress or plugin update alone is not the PHP fix.

PHP 8.2	PHP 8.3	PHP 8.4	PHP 8.5
8.2.35	8.3.36	8.4.27	8.5.12

First fixed upstream releases. Older branches need a supported upgrade or vendor-verified backport. A version number is not proof of a clean site.

- ☐ **Identify**
List the site, PHP forms, old subdomains and any PHP applications.
- ☐ **Patch**
Ask for the fixed release or the exact vendor security-backport advisory.
- ☐ **Verify**
Confirm the patched web service is running and affected workers were replaced.
- ☐ **Limit exposure**
If patching cannot be verified, discuss temporary isolation with your host.
- ☐ **Review evidence**
Ask about logs, unexpected accounts and file changes. Escalate suspected compromise.
- ☐ **Recover and maintain**
Confirm protected backups, access/MFA, ongoing updates and working forms/bookings.

WAF rules can add protection, but the PHP project says an update is needed for a complete fix. If compromise is suspected, preserve evidence and involve your host or an incident-response specialist.

ASK YOUR HOST.

Keep the answer.

Hi, can you confirm the PHP runtime and handler actually serving my website and any PHP-based forms or subdomains? Have CVE-2026-109618 and CVE-2026-109619 (PHP2Shell) been fixed on each affected service? Please provide the running version or the vendor advisory/package showing a security backport, and confirm affected workers have been restarted or replaced as needed. If a fix is not yet available, what temporary isolation and monitoring do you recommend? Please also confirm our backup/restore position and whether you found any signs that require incident-response review. Thank you.

Website / service:

Running runtime + handler:

Fixed package / vendor advisory:

Patch and worker verification date:

Review / restore contact:

BEFORE A PHP-FREE REBUILD

Scope pages, forms, APIs, bookings and hosting. Removing PHP from one page path does not remove every attack surface. Ask who owns updates, access, backups and monitoring.

Want to discuss a custom-coded website? First call is 30 minutes, free, with Shane personally.
digitalreach.co/contact/

Primary sources: [PHP official releases](#); [CERT-EU 2026-018](#); [PHP Foundation disclosure history](#); [WordPress hardening](#); [OWASP attack surface analysis](#).