

WHAT TO DO TODAY

"PHP2Shell": Two Critical PHP Flaws Let Attackers Take Over Web Servers

Patches were released Oct 21–22, 2026. Public proof-of-concept exploits already exist. Patch before attackers do.

SEVERITY

CRITICAL · CVSS 9.2

ATTACK

**Unauthenticated
RCE**

EXPLOITED IN WILD?

Attempts reported

FIX AVAILABLE?

Yes, update now

1 Do This Today

1 Inventory every PHP system.

Websites, WordPress/Laravel apps, intranets, appliances, containers and vendor products that bundle PHP. Run `php -v` or ask your IT/MSP and hosting providers.

2 Patch internet-facing systems first.

Update to **8.5.12**, **8.4.27**, **8.3.36** or **8.2.35**, then restart web server/PHP-FPM workers so the fix loads.

3 Can't patch yet? Isolate it.

Take the PHP system offline or off the public internet. A WAF gives only partial protection.

4 On PHP 8.1 or older?

No upstream fix. Ask your OS vendor for a backport or migrate to a supported version urgently.

5 Hunt for compromise.

Look for web-server/PHP processes launching shells, new files or accounts, and odd outbound connections. Missing log entries do not prove safety.

6 Call your vendors & hosts.

Ask: "Is our product patched for CVE-2026-109618 / -109619?" Get the answer in writing.

2 Who's Affected

PHP branch	Status
8.5 < 8.5.12	Vulnerable
8.4 < 8.4.27	Vulnerable
8.3 < 8.3.36	Vulnerable
8.2 < 8.2.35	Vulnerable
8.1 and older	No routine fixes
Fixed releases	8.5.12 · 8.4.27 · 8.3.36 · 8.2.35

Web setups at risk: Apache `mod_php` (highest risk), PHP-FPM, `php-cgi`, FrankenPHP, LiteSpeed.

Stopgaps only (not a fix):

```
session.upload_progress.enabled=0;
fatal_error_backtraces=0 (PHP 8.5); cap
post_max_size (e.g., 8M); block unneeded multipart
uploads. Restart workers after changing.
```

3 The Flaws

- **CVE-2026-109618:** memory corruption when PHP runs out of memory (crafted multipart requests).
- **CVE-2026-109619:** use-after-free from stale state reused between requests.
- Found by Wiz Research; reported to PHP Aug 24, 2026.

4 Tell Your Team

Employees: no action on your devices, but **report** any website outages, odd site behavior, or vendor notices to IT. Leaders: treat this as an **out-of-cycle emergency patch** and confirm completion by end of week.

5 Trusted Sources

[CISA Alert](#) · [Canadian Cyber Centre AL26-026](#) · [Rapid7 Analysis](#) · [Wiz Research](#) · [CERT-EU](#) · [Google Cloud](#) · [PHP Downloads & ChangeLog](#)