PHP2Shell flaws confirmed exploited in the wild: patch PHP and review exposure



Two critical PHP remote code execution flaws, tracked as PHP2Shell, have been exploited successfully in the wild, according to a honeypot capture. PHP patches have been available since 21 October.

- CVE-2026-109618 and CVE-2026-109619 are critical RCE flaws, collectively called PHP2Shell.
- A honeypot recorded confirmed code execution against Apache mod_php running PHP 8.4.26.
- The researcher stressed this was a favourable single-worker setup and does not measure reliability elsewhere.
- The PHP security team released patches on 21 October.
- A separate unpatched RCE, CVE-2026-115560, has a mitigation: set session.upload_progress.enabled=0.

What happened

Two critical remote code execution vulnerabilities in PHP, CVE-2026-109618 and CVE-2026-109619 and together known as **PHP2Shell**, have now been exploited successfully in the wild. The activity was captured by Adel Karimi of Perplexity through honeypots, which recorded confirmed code execution against an Apache mod_php installation running PHP 8.4.26. Marcus Hutchins of Expel confirmed the findings.

Karimi noted the evidence comes from a deliberately favourable single-worker mod_php profile. It does not show how reliable the exploit would be on other worker counts, PHP builds or applications.

Background

The PHP security team patched the flaws on 21 October. Details and some proof-of-concept exploits leaked before the patches, though the team said none worked. Several security firms and Amazon Threat Intelligence saw attempts before disclosure, all described as unsuccessful until this confirmation. CISA published a SIGMA detection rule for exploitation attempts, but had not yet listed the flaws as exploited when the source was written.

Separately, the PHP team shared mitigation for another RCE, CVE-2026-115560, which has no patch and is exploitable only with an unusual mix of configuration and application code. Admins are advised to set session.upload_progress.enabled=0 until a fix arrives.

Why it matters

PHP runs on roughly 70% of websites, and VirusTotal estimates more than 5.1 million PHP hosts are exposed online. Institutions should treat internet-facing PHP applications as a priority for patching and review.

What to do now

1. Inventory internet-facing PHP applications and hosts, including Apache mod_php deployments, and record their PHP versions.
2. Apply the PHP security updates released on 21 October through emergency change control, starting with exposed systems.
3. Where CVE-2026-115560 may apply, set session.upload_progress.enabled=0 until a patch is published.
4. Deploy the CISA SIGMA rule in your SIEM and review web and process logs since mid-October for suspicious activity.
5. Escalate any confirmed compromise under your incident response plan and notify NCA and SAMA as your obligations require.