# Amazon: PHP2Shell exploitation attempts began four days before PHP patches



Amazon Threat Intelligence says attempts to exploit the critical PHP2Shell flaws started on October 17, four days before PHP released patches on October 21. Organisations running PHP should patch now and not treat disclosure day as the start of risk.

- CVE-2026-109618 and CVE-2026-109619 are critical flaws that allow remote code execution on vulnerable systems.
- The PHP security team released patches on October 21 after details leaked and the release date was brought forward.
- Amazon saw the first exploitation attempts on October 17 against a honeypot, from an anonymised IP address; payloads varied, suggesting multiple actors.
- Amazon says the flaws are now broadly exploited, though it is unclear how many attacks succeed;

> Dataminr TRACE reports only scanning and non-working exploits, with no known compromises.
>
> - VirusTotal tracks more than 5.1 million exposed PHP hosts.

## What happened

Amazon Threat Intelligence reports that attackers began targeting the PHP2Shell vulnerabilities on Saturday, October 17, four days before the PHP security team shipped patches on October 21. The two flaws, CVE-2026-109618 and CVE-2026-109619, are rated critical and allow remote code execution.

The PHP team says its coordinated release was moved forward after details, including the CVE identifiers and mitigation advice shared with some critical infrastructure providers, leaked online. Some proof-of-concept exploits were published before the patches, but the team said none worked.

## What is known about exploitation

Amazon's honeypot was hit from an IP address linked to a commercial anonymisation network while the issue was still under embargo. It is unclear how the actor obtained the information. After disclosure, multiple proof-of-concept exploits were deployed from VPN addresses. AWS CISO CJ Moses said the flaws are now broadly exploited, that it is unclear how many attempts succeed, and that defenders should not assume the disclosure date is the earliest date of exploitation.

Dataminr's TRACE team offers a more measured view: activity so far is limited to scanning, fingerprinting and non-working exploits, with no known compromises, though working exploits are expected to emerge.

## Why it matters

PHP is widely used and underpins common content management systems such as WordPress, Drupal and Joomla. VirusTotal tracks over 5.1 million exposed PHP hosts. The PHP developers describe the official patches as the only permanent defence, and the UK NCSC advised updating PHP servers immediately or taking them offline until patched.

## What to do now

1. Inventory all internet-facing PHP servers and PHP-based CMS sites, including those run by third parties.
2. Apply the official PHP patches for CVE-2026-109618 and CVE-2026-109619 immediately; take unpatched servers offline if patching must wait.
3. Review web server and WAF logs from October 17 onward for scanning, unusual requests or signs of web shells.
4. Treat unpatched systems exposed since before October 21 as potentially targeted and escalate through your incident response process if indicators appear.
5. Ask hosting providers and web vendors to confirm their patch status in writing.