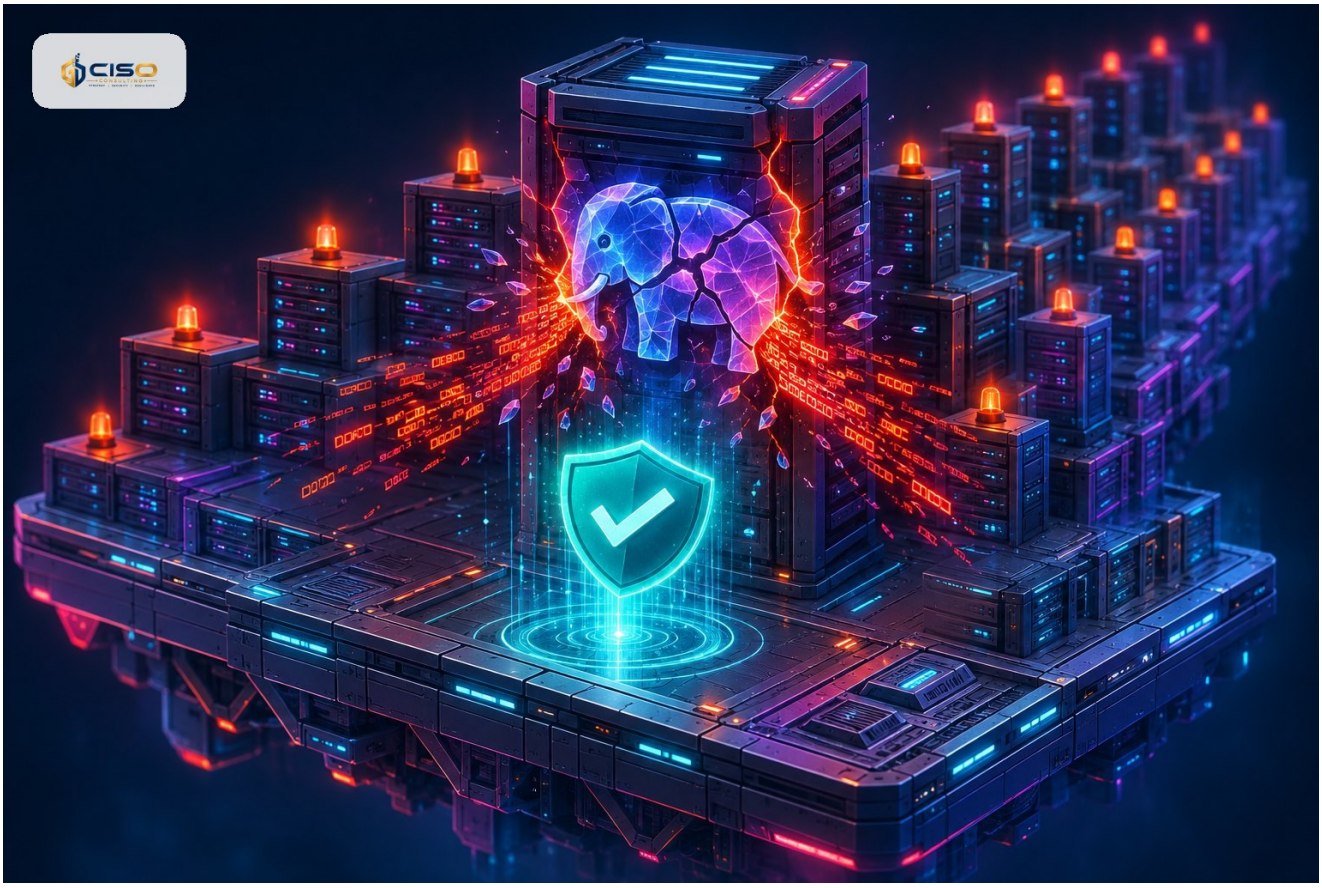
Critical PHP flaws under active exploitation: patch to fixed versions now



PHP issued an emergency update for two critical flaws that allow remote code execution. Exploitation is already reported, and every PHP version from the past decade is affected by at least one flaw.

- CVE-2026-109618 and CVE-2026-109619 let an attacker run code of their choosing on a vulnerable server.
- Fixes are in PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35; affected servers run PHP 5.4 or later.
- Cloudflare reports some exploitation and deployed web application firewall rules at 3:02 am UTC.
- Wiz expects mass exploitation to install web shells, and compares the scale of the problem to Log4Shell.
- Censys counted about 2.58 million internet-facing hosts and 54.9 million web properties running

> PHP.

PHP has released an emergency security update addressing two critical vulnerabilities, tracked as CVE-2026-109618 and CVE-2026-109619. Either can allow an attacker to execute code of their choosing on a vulnerable server. Experts cited in the report say working exploits exist and that exploitation in the wild has begun.

What is affected

PHP underpins many publishing platforms, including Drupal, Magento, Joomla and WordPress. The flaws affect web servers running PHP 5.4 or later, and Wiz states that every PHP version released in the past decade is affected by at least one of them. Fixes are included in PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35.

Reuters reported that some government websites in Europe and elsewhere went offline after disclosure. Cloudflare said it detected some exploitation and put web application firewall rules in place at 3:02 am UTC. Censys identified about 2.58 million internet-facing hosts and 54.9 million web properties running PHP.

Why it matters

Wiz researchers expect mass exploitation aimed at installing **web shells**, which give attackers remote control of a site. They also note that PHP is embedded so deeply in applications that organizations may struggle to patch for some time, drawing a comparison with Log4Shell in 2021. Vendors are shipping updates; Ubuntu, for example, has released updated PHP packages, and the SANS Internet Storm Center is tracking other platforms.

The story is still developing, so teams should check vendor advisories regularly. A web application firewall rule can reduce exposure but is not a substitute for updating PHP itself.

What to do now

1. Inventory all internet-facing and internal servers running PHP, including those behind CMS platforms such as Drupal, Magento, Joomla and WordPress.
2. Upgrade to PHP 8.5.12, 8.4.27, 8.3.36 or 8.2.35, or apply the vendor-supplied patched package for your operating system.
3. Ask hosting providers and web agencies to confirm in writing their patch status for systems hosting your sites.
4. Enable or verify web application firewall rules against these CVEs as a temporary layer while patching.
5. Hunt for web shells and unexpected files or processes on PHP servers, and escalate any finding through your incident response process.
6. Plan to upgrade any server on an end-of-life PHP branch, since fixes are only listed for the four versions

above.