

PHP team warns of two critical flaws ahead of emergency patches



The PHP security team will release emergency updates on 21 October for two critical flaws rated 9.2 under CVSS v4.0. Details reportedly leaked early; no exploitation in the wild has been observed.

- PHP announced security updates for 21 October at 14:00 UTC, covering two vulnerabilities each rated 9.2 under CVSS v4.0.
- The team may release earlier if details become public or exploitation appears.
- watchTowr says the flaws, CVE-2026-109618 and CVE-2026-109619, are remote code execution issues believed to affect PHP 5, 6, 7 and 8.
- watchTowr reports no exploitation in the wild so far and says it reproduced CVE-2026-109618.
- Official details, affected versions and fixed releases have not yet been published.

The PHP security team has told administrators to prepare for emergency security updates on Wednesday, 21 October, at 14:00 UTC. The updates address two critical vulnerabilities, each rated 9.2 under CVSS v4.0. PHP underpins many websites, content management systems, e-commerce platforms and custom web services.

What is known

The PHP team has not yet shared technical details, the affected versions or the releases that will contain fixes. It says it will publish these when the updates ship, and it has reserved the right to release earlier if details become public or exploitation is seen in the wild.

Researchers at watchTowr told BleepingComputer that the flaws are tracked as CVE-2026-109618 and CVE-2026-109619 and are remote code execution issues, believed to affect PHP versions 5, 6, 7 and 8. They say information leaked ahead of a planned embargo, and that they have reproduced CVE-2026-109618. They have not observed exploitation in the wild.

Note that watchTowr described both flaws as CVSS 10.0 and cited a different disclosure date, whereas PHP's own advisory gives 9.2 under CVSS v4.0 and a 21 October release. The official advisory should be treated as authoritative; the researchers' version claims are unconfirmed.

What to do now

Because the details are not yet public, the practical step is preparation: know where PHP runs, who owns each system, and how quickly a patch can be tested and deployed once the release appears.

What to do now

1. Inventory all internet-facing and internal systems running PHP, including CMS, e-commerce and custom applications, with their PHP versions and owners.
2. Schedule an emergency change window and test environment for 21 October so the patch can be validated and deployed quickly.
3. Monitor the official PHP advisory and ANNOUNCE list, since the release may come earlier than planned.
4. Confirm WAF and logging coverage on PHP applications and watch for unusual requests or process activity until patched.
5. Identify end-of-life PHP versions in use and plan their upgrade or isolation, as fix coverage for older versions is not yet confirmed.