

Critical PHP flaws CVE-2026-109618 and CVE-2026-109619: prepare for the patch



PHP.net has announced a critical update. SANS ISC raised its InfoCon level to yellow, citing PHP's wide use, an expected CVSS score of 9.4 and early proof-of-concept exploits circulating before the patch.

- PHP.net announced a critical update, to be released on the day of the SANS ISC diary.
- The flaws are tracked as CVE-2026-109618 and CVE-2026-109619.
- The expected severity is CVSS 9.4.
- Early proof-of-concept exploits are reportedly available before the patch.
- SANS ISC moved InfoCon to yellow because of PHP's widespread use.

What has been announced

PHP.net has said it will publish a critical update. SANS Internet Storm Center, which tracks internet-wide threat levels, responded by changing its InfoCon level to yellow. The two vulnerabilities are identified as CVE-2026-109618 and CVE-2026-109619.

Why it matters

SANS ISC gave three reasons for the change: PHP is very widely used, the flaw is expected to be severe at CVSS 9.4, and early proof-of-concept exploits are available before the patch itself. That last point narrows the time between disclosure and possible attacks. The source does not describe the technical nature of the flaws, the affected versions or any observed exploitation, so those details should be confirmed from the official PHP release notes once published.

What to do next

Institutions that run PHP-based websites, portals or internal applications should use the time before the patch to establish where PHP is deployed, who owns each system, and how quickly an update can be tested and applied. Internet-facing systems deserve priority. Keep monitoring the official PHP announcement and apply the update through your normal change process, with an emergency path for critical fixes.

What to do now

1. Inventory all systems and applications that run PHP, starting with internet-facing ones.
2. Assign an owner to each PHP system and confirm a test and deployment window for the update.
3. Follow the official PHP.net announcement and release notes for affected versions and fixed releases.
4. Apply the update through an emergency change process as soon as it is available and tested.
5. Increase monitoring of web server and application logs on PHP systems until patched.