Does the server load the patched PHP? Eight checks.

The list sums up the method from the case. It does not replace the vendor's or the hosting provider's guidance, and it is not a guide to testing other people's systems.

> This is educational material, not instructions for your server: test every change in a test environment first, with a current backup, and make it at your own risk.

1. Before you change anything, take a database dump and verify it. Keep it outside the application directory.
2. Inventory every hostname the server answers to, not just the public address.
3. Do not judge the fix by the X-Powered-By banner or by the version number. Some distributions backport fixes without changing the number: Ubuntu 24.04 shows 8.3.6 before the patch and after it.
4. Compare the build date from php -v and from the Build Date field in phpinfo with the date of the fix in the distribution package's changelog.
5. Check the PHP module file the web server loads. The command line and the web server can use different builds.
6. Run phpinfo only on a page that is not publicly reachable, and delete it after the check.
7. Trust only checks that can come out either way. A check script must be able to return both “not patched” and “patched”, and “cannot tell” when the data cannot settle it.
8. After every restart from the provider's panel and every image update, check the build again. Some restarts recreate the container.

php.net recommends setting session.upload_progress.enabled = 0 until the next regular PHP release, also after the 21 October update. The setting closes one attack path; only the update removes the vulnerability.



See the whole incident in the free narrated lab (in your browser, no sign-up):

cyberszkola.pl/php2shell

Sources

1. PHP security advisory GHSA-w8hw-w9fx-j79w — CVE-2026-109618, RCE via OOM corruption https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w
2. PHP security advisory GHSA-6wmf-4rv5-p3rp — CVE-2026-109619, RCE via stale global state https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp
3. php.net — advance notice of 20 October 2026 https://www.php.net/archive/2026.php#2026-10-20-1
4. php.net — informational advisory: session upload progress (23 October 2026, CVE-2026-115560) https://www.php.net/archive/2026.php#2026-10-23-1
5. CERT-EU Security Advisory 2026-018 — Critical Vulnerabilities in PHP (v1.2) https://cert.europa.eu/publications/security-advisories/2026-018
6. Ubuntu Security — CVE-2026-109618 (package table, USN-8948-1/2) https://ubuntu.com/security/CVE-2026-109618
7. Launchpad — php8.3 8.3.6-0ubuntu0.24.04.13 (changelog: SECURITY UPDATE, CVE-2026-109618/109619) https://launchpad.net/ubuntu/+source/php8.3/8.3.6-0ubuntu0.24.04.13
8. Tenable — php2shell FAQ (updated 28 October 2026) https://www.tenable.com/blog/php2shell-cve-2026-109618-cve-2026-109619-frequently-asked-questions-about-critical-php-remote
9. Datadog Security Labs — PHP2Shell: what the logs and processes show (updated 23 October 2026) https://securitylabs.datadoghq.com/articles/php2shell-critical-vulnerabilities-in-php/
10. Varonis — PHP2Shell: the log pattern to hunt for https://www.varonis.com/blog/php2shell
11. NCSC-NL — third-party software that embeds PHP (inventory aid, referenced by CERT-EU) https://github.com/NCSC-NL/php2shell
12. CISA — Known Exploited Vulnerabilities Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog
13. OWASP WSTG-CONF-01: Test Network Infrastructure Configuration https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/01-Test_Network_Infrastructure_Configuration
14. OWASP WSTG-INFO-02: Fingerprint Web Server https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server
15. OWASP WSTG-INFO-08: Fingerprint Web Application Framework https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework