Czy serwer ładuje poprawione PHP? Osiem sprawdzeń.

Lista streszcza metodę z przypadku. Nie zastępuje zaleceń producenta ani dostawcy hostingu i nie jest instrukcją testowania cudzych systemów.

> To materiał edukacyjny, a nie instrukcja dla Twojego serwera: każdą zmianę najpierw sprawdź w środowisku testowym, z aktualną kopią zapasową, i wprowadzaj ją na własną odpowiedzialność.

1. Zanim cokolwiek zmienisz, wykonaj i zweryfikuj zrzut bazy. Przechowuj go poza katalogiem aplikacji.
2. Uwzględnij w inwentaryzacji każdą nazwę hosta, pod którą odpowiada serwer, nie tylko adres publiczny.
3. Nie oceniaj poprawki po banerze X-Powered-By ani po numerze wersji. Niektóre dystrybucje dodają poprawki bez zmiany numeru: Ubuntu 24.04 pokazuje 8.3.6 przed łatką i po niej.
4. Porównaj datę kompilacji z php -v i z pola Build Date w phpinfo z datą poprawki w changelogu pakietu dystrybucji.
5. Sprawdź plik modułu PHP, który ładuje serwer WWW. Wiersz poleceń i serwer WWW mogą używać innych kompilacji.
6. phpinfo uruchamiaj tylko na stronie niedostępnej publicznie i usuń ją po sprawdzeniu.
7. Sprawdzenie, które daje ten sam wynik niezależnie od stanu serwera, niczego nie dowodzi. Skrypt sprawdzający musi umieć zwrócić „bez poprawki” i „z poprawką”, a gdy dane nie pozwalają rozstrzygnąć, „nie da się stwierdzić”.
8. Po każdym restarcie z panelu dostawcy i po każdej aktualizacji obrazu sprawdź kompilację ponownie. Niektóre restarty tworzą kontener od nowa.

php.net zaleca ustawienie session.upload_progress.enabled = 0 do następnego regularnego wydania PHP, także po aktualizacji z 21 października. Zamyka ono jedną ścieżkę ataku; dopiero aktualizacja usuwa podatność.

Zobacz cały incydent w bezpłatnym laboratorium z lektorem (w przeglądarce, bez zapisu):

cyberszkola.pl/php2shell

Źródła

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