



**SERVICIUL
TEHNOLOGIA INFORMAȚIEI
ȘI SECURITATE CIBERNETICĂ**

RAPORT TEHNIC DE SECURITATE

PHP2Shell

CVE-2026-109618 și CVE-2026-109619

Raport tehnic de securitate

Sumar

Instalațiile PHP care deserve cereri web necesită actualizare urgentă pentru două vulnerabilități critice, CVE-2026-109618 și CVE-2026-109619, cunoscute sub denumirea PHP2Shell. Acestea pot permite executarea de cod fără autentificare, divulgarea memoriei și indisponibilizarea serviciilor. Remedierea completă presupune actualizarea runtimeului și înlocuirea proceselor care execută codul vulnerabil.

Câmp	Evaluare
Produs afectat	Runtimeul PHP din servere web, platforme de găzduire, containere și produse care includ PHP.
Identificatori	CVE-2026-109618 / GHSA-w8hw-w9fx-j79w; CVE-2026-109619 / GHSA-6wmf-4rv5-p3rp.
Severitate	Critică pentru ambele CVE; CVSS v4.0 9,2, publicat de proiectul PHP.
Acces necesar	Acces de rețea la o cale web exploatabilă; căile demonstrate nu necesită cont sau interacțiune umană.
Situație operațională	Cloudflare a observat trafic de atac și adaptarea cererilor pentru evitarea protecțiilor WAF.
Versiuni remediate	Primele versiuni remediate: 8.2.35, 8.3.36, 8.4.27 și 8.5.12.
Acțiune prioritară	Actualizare, repornirea tuturor workerelor și verificarea retrospectivă a activelor expuse.

Concluzie executivă

Prioritatea maximă revine serviciilor publice bazate pe Apache cu mod_php, precum și oricărei instanțe cu erori de memorie, căderi de procese sau execuții neobișnuite. PHP-FPM și celelalte integrări web trebuie incluse în inventar. Un CMS actualizat sau o regulă WAF activă nu dovedește remedierea PHP.

1 Coruperea memoriei la epuizarea resurselor

CVE-2026-109618 | RCE via OOM corruption

Câmp tehnic	Evaluare
Condiția necesară pentru exploatare	Runtime PHP vulnerabil și o cerere capabilă să provoace epuizarea memoriei într-un moment în care datele interne sunt inițializate parțial. În mod_php, o cale demonstrată este accesibilă înainte de executarea aplicației.
Descriere succintă	La întreruperea unei operații din cauza lipsei memoriei, PHP poate păstra structuri incomplete. Curățarea cererii interpretează ulterior aceste structuri ca fiind valide și corupe memoria.
CVSS	9,2 Critic, CVSS v4.0, proiectul PHP.
Tipul vulnerabilității	Corupere de memorie și utilizarea datelor neinițializate; mecanism asociat CWE-824, CWE-755 și CWE-1419. Avizul include și CWE-416 și CWE-1325.
Mod de exploatare	De la distanță, prin cereri HTTP special construite. Nu necesită autentificare sau interacțiunea utilizatorului pe căile demonstrate; fiabilitatea depinde de build, extensii și configurație.
Cauza	Ieșirea nonlocală prin longjmp() la OOM poate întrerupe inițializarea fără finalizarea stării interne. Într-un caz analizat, contorul unui HashTable este avansat înaintea inițializării complete a elementului Bucket.
Metode de exploatare	Presiune de memorie prin parsarea formularelor și a încărcărilor multipart, amplificarea structurilor interne sau alocări influențate de datele cererii. Un corp HTTP mic pe rețea poate genera o utilizare mult mai mare a memoriei.
Versiuni afectate	PHP 8.2 < 8.2.35; 8.3 < 8.3.36; 8.4 < 8.4.27; 8.5 < 8.5.12. Ramurile istorice necesită evaluare și migrare sau un backport confirmat de furnizor.
Versiuni remediate	PHP 8.2.35, 8.3.36, 8.4.27, 8.5.12 ori o versiune ulterioară dintr-o ramură suportată care include corecția.
Consecințe	Executare de cod în contextul contului workerului web, căderea procesului și compromiterea datelor accesibile acestuia. Obținerea privilegiilor root nu rezultă automat din această vulnerabilitate.
Detectare și monitorizare	Corelarea cererilor anormale cu OOM, SIGSEGV, reporniri de workeri, răspunsuri neobișnuite și activitate de procese sau fișiere. Un mesaj de memorie epuizată izolat este nespecific; se verifică istoricul HTTP și telemetria gazdei. Recomandare de analiză: secțiunile 4–6.

Interpretarea vectorului: atac prin rețea, complexitate ridicată și condiții suplimentare prezente; fără privilegii prealabile și fără interacțiune. Impactul ridicat privește confidențialitatea, integritatea și disponibilitatea sistemului vulnerabil.

2 Reutilizarea stării interne între cereri

CVE-2026-109619 | RCE via stale global state

Câmp tehnic	Evaluare
Condiția necesară pentru exploatare	O operație lasă stare aferentă unei cereri într-o zonă globală a workerului; memoria cererii este eliberată fără resetarea acelei stări. Același worker procesează o cerere ulterioară care utilizează referința veche înaintea reinițializării normale.
Descriere succintă	Referințe interne pot supraviețui duratei de viață a memoriei către care indică. Accesarea ulterioară produce use-after-free și poate permite divulgarea memoriei sau executarea de cod.
CVSS	9,2 Critic, CVSS v4.0, proiectul PHP.
Tipul vulnerabilității	Use-after-free între cereri și gestionarea incorectă a condițiilor excepționale. Avizul asociază CWE-416, CWE-755, CWE-824, CWE-1325 și CWE-1419.
Mod de exploatare	Cereri HTTP succesive procesate de un worker persistent; căile publicate pot fi accesibile fără cont. Condițiile concrete diferă în funcție de versiune, SAPI, extensii și aplicație.
Cauza	O eroare fatală poate împiedica resetarea stării; un diagnostic poate, de asemenea, recrea stare după curățarea normală. Inițializarea unei cereri ulterioare poate utiliza acea stare înainte să o înlocuiască.
Metode de exploatare	Publicarea și consumarea stării vechi prin căi precum backtrace la eroare fatală în PHP 8.5, session upload progress sau procesarea timpurie a configurației. Nu este necesar ca toate aceste condiții să fie prezente simultan.
Versiuni afectate	PHP 8.2 < 8.2.35; 8.3 < 8.3.36; 8.4 < 8.4.27; 8.5 < 8.5.12. Ramurile istorice necesită evaluare și migrare sau un backport confirmat de furnizor.
Versiuni remediate	PHP 8.2.35, 8.3.36, 8.4.27, 8.5.12 ori o versiune ulterioară dintr-o ramură suportată care include corecția.
Consecințe	Citirea memoriei workerului, expunerea parolelor, tokenurilor și cheilor API, căderi de procese sau RCE cu drepturile serviciului. Divulgarea memoriei poate apărea fără lansarea unui shell.
Detectare și monitorizare	Se corelează erorile fatale și timeouturile cu cereri ulterioare către același worker, căderi sau răspunsuri anormale. Se urmăresc diagnosticele la inițializare, uploadurile și telemetria gazdei. Datele de PID sau request ID îmbunătățesc corelarea; lipsa lor limitează atribuirea locală.

PHP2Shell grupează mai multe căi de atac. Nu presupune că fiecare exploatare combină obligatoriu ambele CVE sau că dezactivarea unei singure funcționalități elimină toate variantele.

3 Produse afectate și impact operațional

Versiuni vulnerabile și primele versiuni remediate

Ramură PHP	Versiuni vulnerabile	Primul prag remediat
8.2	8.2.0–8.2.34	8.2.35
8.3	8.3.0–8.3.35	8.3.36
8.4	8.4.0–8.4.26	8.4.27
8.5	8.5.0–8.5.11	8.5.12
5.4–8.1	Ramuri istorice: cel puțin o cale este raportată; aplicabilitatea diferă între versiuni.	Migrare la o ramură suportată sau pachet cu backport verificat.

Pragurile de mai sus se referă la versiunile upstream. Furnizorii pot integra corecțiile în pachete cu un număr de versiune upstream mai vechi; dovada o constituie avizul și revizia exactă a pachetului. Pentru PHP 7.4, 8.0 și 8.1, proiectul a publicat backporturi minimale de cod sursă pentru situații speciale; acestea nu restabilesc suportul general al ramurilor.

Particularități ale integrării cu serverul web

Integrare	Evaluare tehnică
Apache cu mod_php	Prioritate maximă. O cale RCE a fost demonstrată cu setări implicite, înainte de codul aplicației.
PHP-FPM	Inclus în domeniul afectat. Eșecul la startup elimină anumite căi, însă există căi legate de execuția aplicației; utilizarea FPM nu constituie remediere.
FrankenPHP, CGI, LiteSpeed	Se inventariază și se actualizează. Avertizarea PHP acoperă integrările web; gradul demonstrației unei anumite căi nu trebuie generalizat la toate configurațiile.
Containere și produse incluse	Se verifică runtimeul din imaginea efectiv pornită, nodurile și replicile. Actualizarea unei imagini fără redeploy nu înlocuiește procesele active.

Impact pentru serviciile instituției

Un atac reușit poate expune date procesate de portal, modifica pagini și fișiere sau întrerupe furnizarea serviciilor. Secretele disponibile în memoria PHP pot permite acces ulterior la baze de date ori servicii integrate. Extinderea către alte sisteme depinde de permisiuni, segmentare și identitățile disponibile procesului; nu reprezintă un efect automat demonstrat pentru fiecare instalare.

Evaluarea inventarului trebuie să includă site-uri secundare, staging, panouri de administrare și runtimeuri multiple pe aceeași gazdă. Prioritizarea după expunere și sensibilitatea datelor este o recomandare operațională a prezentului raport.

4 Detectare și monitorizare

Se colectează evenimentele de la WAF, reverse proxy, server web, PHP și sistemul de operare. Corelarea se face după gazdă, domeniu virtual, timp, PID și identificatorul cererii, unde sunt disponibile. Regulile de mai jos sunt recomandări de investigație, nu semnături care confirmă singure o anumită CVE.

Sursă de telemetrie	Ce se urmărește	Acțiuni de triere
WAF și proxy	Potriviri ale protecțiilor PHP2Shell, cereri repetate multipart și depășirea limitelor de inspecție.	Verificarea acțiunii efective, a rutei și a accesului direct la origin. Păstrarea identificatorului regulii și cererii.
PHP și server web	Allowed memory size exhausted, erori fatale, Maximum execution time exceeded, SIGSEGV și workeri terminați.	Compararea cu nivelul obișnuit; identificarea cererii și a procesului asociat. OOM poate avea și cauze legitime.
EDR și audit de procese	Procese web/PHP care lansează interpretoare ori utilitare neașteptate; conexiuni externe fără justificare.	Inspectarea arborelui de procese, contului, argumentelor și destinației. Escaladare când există execuție neautorizată.
Integritatea fișierelor	Fișiere PHP/phtml nou create sau modificate, configurații schimbate și artefacte în directoare temporare.	Compararea cu baseline-ul și schimbările aprobate. În Wazuh FIM se monitorizează crearea, modificarea și ștergerea.
Răspunsuri HTTP	Conținut binar sau date sensibile neașteptate într-un răspuns; diferențe de volum și erori corelate.	Verificare controlată, fără distribuirea datelor sensibile. Divulgarea memoriei poate să nu producă un proces nou.

Aplicare în instrumentele de monitorizare

În Wazuh se centralizează jurnalele și alertele FIM; în EDR se verifică procesele și conexiunile. Zabbix poate urmări memoria și repornirile serviciilor. Un scanner de vulnerabilități cu verificări actualizate poate corobora inventarul; închiderea constatării necesită și dovada pachetului remediat și a runtimeului activ. Aceste verificări nu înlocuiesc analiza incidentelor.

5 Verificări locale și analiză retrospectivă

Exemplele următoare sunt verificări locale pentru Linux. Se adaptează numele binarelor, serviciilor, jurnalelor și directorul web la sistemul inventariat. Ele nu trimit cereri de exploatare.

Identificarea versiunii și a proceselor

```
type -a php php-fpm php-fpm8.2 php-fpm8.3
php -v
php --ini
php -m
ps -eo pid,ppid,user,lstart,args --forest \
  | rg 'php-fpm|php-cgi|apache2|httpd|lsphp|frankenphp'
dpkg-query -W 'php*' 'libapache2-mod-php*' 2>/dev/null
rpm -qa | rg '^(^)-php([0-9-])$'
```

Erori și conexiuni care necesită verificare

```
rg -n -i \
  'Allowed memory size|out of memory|SIGSEGV|segmentation fault|Maximum execution time' \
  /var/log/php* /var/log/apache2 /var/log/nginx
journalctl --since '2026-10-20 00:00:00' --no-pager \
  | rg -i 'php|apache|httpd|oom|segfault|killed process'
ss -tpn
```

Data din exemplu este un punct de pornire pentru triere. Se examinează întreaga retenție relevantă și arhivele de jurnale, se aliniază fusurile orare și se corelează cererile cu erorile. Lipsa unui mesaj din aceste căutări nu exclude divulgarea memoriei sau exploatarea.

Fișiere modificate în zona web

```
find /var/www/html -xdev -type f \
  \( -name '*.php' -o -name '*.phtml' -o -name '.htaccess' \) \
  -newermt '2026-10-20 00:00:00' \
  -printf '%TY-%Tm-%Td %TH:%TM %u %m %p\n'
```

Rezultatele se compară cu manifestul aplicației, baseline-ul FIM și schimbările autorizate. Data modificării este orientativă și poate fi alterată. Fișierele suspecte se păstrează pentru analiză; o listă de fișiere recente nu reprezintă, singură, dovada unui webshell.

6 Indicatori de atac și mapare MITRE ATTACK

Indicatorii comportamentali de mai jos susțin trierea. Nivelul de încredere privește existența unei activități suspecte, nu atribuirea ei exclusivă PHP2Shell. Un URI, un mesaj OOM sau un cod de eroare HTTP izolat nu confirmă exploatarea.

Indicator observabil	Încredere	Interpretare și verificare
Eveniment WAF asociat PHP2Shell	Mediu	Semnal de tentativă ori potrivire cu regula. Verificarea acțiunii și a traficului către origin.
Rafală de cereri, OOM și căderi de workeri	Scăzut–mediu	Poate indica presiune de memorie controlată. Se exclud încărcarea legitimă și defectele aplicației.
Shell ori executabil neautorizat cu părinte PHP/web	Ridicat	Semnal de execuție suspectă. Se păstrează arborele, argumentele și evenimentele conexe.
Cod nou în zona web fără schimbare aprobată	Mediu–ridicat	Verificare de integritate și analiză de conținut; confirmarea funcției malițioase este necesară.
Date sensibile neașteptate în răspuns	Ridicat după validare	Posibilă divulgare de memorie; poate apărea fără RCE și fără fișiere malițioase pe disc.

Tehnici relevante pentru investigație

Maparea reprezintă o analiză a mecanismului și a etapelor posibile. Tehnicile de după accesul inițial se raportează ca observate numai când există dovezi locale.

ID	Tehnică	Aplicare în scenariul analizat
T1190	Exploit Public-Facing Application	Acces inițial prin exploatarea runtimeului PHP accesibil din rețea.
T1059.004	Command and Scripting Interpreter Unix Shell	Executarea de comenzi după obținerea RCE, dacă este confirmată în telemetrie.
T1505.003	Server Software Component Web Shell	Persistență posibilă printr-un script web, dacă atacatorul poate scrie fișiere.
T1105	Ingress Tool Transfer	Transfer de unelte sau payloaduri după acces, demonstrat prin evenimente de rețea și fișiere.

7 Remediere și reducerea expunerii

Acțiuni pentru remedierea completă

- Inventarierea tuturor runtimeurilor PHP și a responsabililor, inclusiv imaginile container, replicile, site-urile secundare și produsele care includ propriul PHP.
- Instalarea unei versiuni remediate din ramura utilizată sau a unui pachet pentru care furnizorul confirmă explicit corectarea ambelor CVE. Se verifică proveniența pachetului și compatibilitatea extensiilor.
- Repornirea serviciilor afectate și înlocuirea tuturor workerelor. În containere se reconstruiește imaginea și se face redeploy pe toate replicile. Se confirmă că nu mai rulează procese vechi.
- Verificarea funcțională a autentificării, formularelor, uploadurilor și operațiilor critice; validarea remedierii se efectuează conform secțiunii 8.

Măsuri temporare când actualizarea întârzie

Aceste măsuri reduc anumite căi și au limite de acoperire. Pentru un serviciu public care nu poate fi actualizat prompt, se evaluează restricționarea accesului sau izolarea temporară până la remediere. [7]

Măsură	Aplicare și limită
Reducerea accesului	Restricționarea rutelor și a accesului la origin; menținerea WAF în blocare după verificarea impactului asupra traficului legitim. Nu corectează memoria runtimeului.
Limitarea cererilor	Limite pentru dimensiunea decodată, câmpuri, părți multipart și niveluri de imbricare, inclusiv cereri fără Content-Length utilizabil. <code>post_max_size</code> orientativ: 8M fără uploaduri sau 32M când sunt necesare; <code>upload_max_filesize</code> sub acest prag.
<code>memory_limit=-1</code>	Numai ca măsură temporară evaluată împreună cu o limită OS/cgroup și impactul asupra disponibilității. Înlătură o cale OOM controlabilă, dar nu toate eșecurile de alocare. Nu se înlocuiește cu <code>RLIMIT_AS</code> ori <code>RLIMIT_DATA</code> .
Progresul încărcării	<code>session.upload_progress.enabled=0</code> se aplică administrativ înainte de parsarea cererii, cu repornirea workerelor. Nu se bazează pe <code>ini_set()</code> sau pe <code>.user.ini</code> în FPM; acoperă căile de sesiune confirmate.
<code>fatal_error_backtraces=0</code>	Aplicabil PHP 8.5, cu repornire. Reduce calea backtrace confirmată, fără a elimina celelalte stări globale vulnerabile.
Erori și reutilizarea workerelor	Eliminarea diagnosticelor de configurație și a erorilor fatale accesibile. Reciclarea mai frecventă a workerelor poate avea cost de performanță; nu constituie remediere completă.

Ascunderea erorilor cu `display_errors`, `error_reporting` sau `@` nu elimină accesul la starea vulnerabilă. După actualizare se reevaluează măsurile temporare, în special limitele de memorie și efectul asupra serviciului. [2, 10]

8 Surse și referințe

Surse consultate la 22 octombrie 2026. Referințele numerice din text indică baza factuală; recomandările de corelare, prioritizare și acceptare sunt formulate pentru gestionarea vulnerabilităților.

[1] Cyber Security News · Cloudflare Detects Early Exploitation Attempts Targeting Two Leaked PHP Vulnerabilities

<https://cybersecuritynews.com/php-early-exploitation-attempts/>

[2] Proiectul PHP · Security advisory Critical remote code execution vulnerabilities update now

<https://www.php.net/archive/2026.php>

[3] Proiectul PHP · CVE-2026-109618 RCE via OOM corruption

<https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w>

[4] Proiectul PHP · CVE-2026-109619 RCE via stale global state

<https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp>

[5] The PHP Foundation · Security release din 21 octombrie 2026

<https://thephp.foundation/blog/2026/10/21/todays-php-security-release-and-how-were-strengthening-php-security/>

[6] Cloudflare · Cloudflare deploys protections against php2shell vulnerability

<https://blog.cloudflare.com/php-vulnerabilities-waf-protection/>

[7] CERT-EU · Security Advisory 2026-018 Critical Vulnerabilities in PHP

<https://cert.europa.eu/publications/security-advisories/2026-018/>

[8] Wiz Research · PHP2Shell cercetarea tehnică

<https://www.wiz.io/blog/php2shell-php-rce>

[9] Calif Research · A tale of two PHP remote vulnerabilities

<https://calif.io/php2shell/>

[10] PHP2Shell · Sinteza cercetărilor și recomandări de actualizare

<https://www.php2shell.com/>

[11] Google Cloud · Responding to core PHP vulnerabilities

<https://cloud.google.com/blog/products/identity-security/responding-to-core-php-vulnerabilities-cve-2026-109618-cve-2026-109619>

[12] Proiectul PHP · Anunțurile versiunilor remediate

https://www.php.net/releases/8_2_35.php | https://www.php.net/releases/8_3_36.php | https://www.php.net/releases/8_4_27.php | https://www.php.net/releases/8_5_12.php

[13] Manualul PHP · Opțiunile liniei de comandă

<https://www.php.net/manual/en/features.commandline.options.php>

[14] Documentația Wazuh · File integrity monitoring

<https://documentation.wazuh.com/current/user-manual/capabilities/file-integrity/index.html>

[15] MITRE ATTACK · Tehnicile utilizate pentru maparea analitică

<https://attack.mitre.org/techniques/T1190/> | <https://attack.mitre.org/techniques/T1059/004/> | <https://attack.mitre.org/techniques/T1505/003/> | <https://attack.mitre.org/techniques/T1105/>

[16] Manualul PHP · Directivele de configurare php.ini

<https://www.php.net/manual/en/ini.core.php>