Riasztás a PHP futtatókörnyezet kritikus sérülékenységeiről

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ NKI) riasztást ad ki a PHP futtatókörnyezetet érintő két kritikus sérülékenységgel kapcsolatban, tekintettel azok súlyosságára, várható kihasználására, valamint az érintett technológia széles körű elterjedtségére.

A PHP projekt 2026. október 21-én közzétette a CVE-2026-109618 és CVE-2026-109619 azonosítójú sérülékenységeket javító biztonsági frissítéseket. Mindkét sérülékenység kritikus, 9,2-es CVSS v4.0 súlyossági besorolást kapott.

A sérülékenységek kihasználása hitelesítés nélkül, távolról történhet, ezért minden, webes kérések kiszolgálására használt PHP telepítés érintettnek tekinthető. A mod_php használatával működő telepítések esetében a kockázat különösen magas, mert egy hitelesítés nélküli http kérés már az alkalmazáskód végrehajtása előtt kiválthatja a támadási útvonalat.

CVE-2026-109618 - RCE memóriahiány okozta adatsérülés révén

A PHP memóriahiány (OOM) esetén megszakíthatja a végrehajtást, miközben a kéréshez tartozó belső adatok még csak részben inicializáltak. A kérés lezárása során a PHP ezután érvényes adatként kezelheti az érvénytelen állapotú memóriaterületet, ami távoli kódfuttatáshoz vezethet.

CVE-2026-109619 - RCE elavult globális állapot miatt

Egy kéréshez tartozó belső állapot a mögöttes memória felszabadítása után is fennmaradhat. Ugyanazon worker által később kezelt kérés ezt az elavult állapotot felhasználhatja, még mielőtt a normál kérésinicializálás visszaállítaná azt. A hiba use-after-free típusú memóriahasználatot eredményezhet, amely célzott heap-elrendezéssel távoli kódfuttatáshoz vezethet.

A PHP projekt a következő verziókban tette közzé a javítást:

- PHP 8.5.12,

+36-1-336-4833 csirt@nki.gov.hu

- PHP 8.4.27,
- PHP 8.3.36,
- PHP 8.2.35.

A PHP 8.1 és korábbi verziók már nem részesülnek a PHP projekt által kiadott frissítésekben. Egyes disztribúciók és LTS-szolgáltatók visszaporolt (backported) javításokat biztosíthatnak, ezek elérhetőségéről az érintett szállítónál kell tájékozódni. A PHP biztonsági csapata a forrásból telepítők számára minimális visszaporolt javításokat biztosított a PHP 7.4, 8.0 és 8.1 verziókhoz is.

Az NBSZ NKI nyomatékosan javasolja, hogy az érintett szervezetek haladéktalanul frissítsenek a fenti javított PHP-verziók egyikére.

Amennyiben a frissítés nem végezhető el azonnal, az alábbi intézkedések csökkenthetik a kitettséget, azonban nem nyújtanak teljes körű védelmet, ezért nem helyettesíthetik a frissítést.

CVE-2026-109618 mérséklése

- A memory_limit=-1 érték beállítása javasolt, lehetőség szerint olyan módon, hogy az alkalmazások ne tudják felülírni, például php_admin_value használatával az FPM poolban vagy az Apache konfigurációjában. Ellenőrizendő, hogy semmilyen pool-, könyvtár- vagy alkalmazásszintű beállítás nem állít vissza véges memóriakorlátot.
- A post_max_size értékének csökkentése javasolt. Fájlfeltöltést nem igénylő alkalmazások esetén a post_max_size = 8M, fájlfeltöltést igénylő rendszereknél a post_max_size = 32M érték alkalmazása javasolt. Az upload_max_filesize értéke a post_max_size alatt maradjon.
- A dekódolt kérésméret, a bemeneti mezők száma, a multipart részek száma, a fejlécek száma és a beágyazási mélység korlátozása javasolt a webszerver vagy proxy szintjén. A korlátoknak a használható Content-Length fejléc nélküli kéréseket is le kell fedniük.
- Konténer- vagy cgroup-alapú erőforráskorlát alkalmazása javasolt rendelkezésre állási határként, lehetőség szerint úgy, hogy csak az érintett

worker álljon le. Az RLIMIT_AS vagy RLIMIT_DATA használata nem javasolt, mert ezek maguk is kiválthatják a sérülékeny memóriafoglalási hibát.

CVE-2026-109619 mérséklése

- A session.upload_progress.enabled=0 beállítás alkalmazása, majd az összes worker újraindítása javasolt. A beállítást a kérések feldolgozása előtt érvényes php.ini, FPM pool vagy szerverkonfigurációban kell elvégezni. Az ini_set() és az FPM .user.ini nem megfelelő megoldás.
- PHP 8.5 esetén a fatal_error_backtraces=0 beállítás alkalmazása, majd az összes worker újraindítása javasolt. Ez csak a megerősített végzetes hiba backtrace útvonalát blokkolja.
- Az inicializálás előtt diagnosztikai üzenetet generáló, kérésenként alkalmazott érvénytelen vagy elavult beállítások eltávolítása javasolt. A diagnosztikai üzenetek elrejtése error_reporting, display_errors vagy @ használatával nem nyújt védelmet.
- A támadó által elérhető végzetes hibák és végrehajtási időtúllépések javítása szükséges, beleértve a callbackek, fájlfeltöltési vagy importálási folyamatok, valamint a takarítási műveletek hibáit.

A frissítés elvégzéséig javasolt az internet felől elérhető, érintett PHP alapú rendszerek hálózati elkülönítése, illetve a kockázatértékelés alapján szükség esetén ideiglenes leállítása.

WAF-alapú védelem

Az AWS és a Cloudflare egyaránt közzétett WAF-alapú mérséklési lehetőségeket a PHP2Shell sérülékenységekhez. Az AWS WAF javaslata szerint a PHP_SESSION_UPLOAD_PROGRESS mezőt tartalmazó POST-kérések blokkolása, fájlfeltöltést nem igénylő alkalmazásoknál a multipart/form-data kérések tiltása, a kéréstest méretének korlátozása, valamint az ismétlődő POST-kérések sebességkorlátozása csökkentheti a kitettséget a javítás telepítéséig. A Cloudflare Managed Ruleset és Managed Free Ruleset keretében több, anomális

végrehajtásra figyelő szabályt telepített, amelyek alapértelmezés szerint elérhetők a WAF-felhasználók számára; a vállalat emellett teljes HTTP-tranzakcióelemzést alkalmaz a kérés- és válaszjelek együttes értékelésével a téves riasztások csökkentése érdekében. Mindkét szolgáltató kiemeli, hogy a WAF-szabályok csak kiegészítő védelmet nyújtanak, a sérülékenység teljes megszüntetéséhez a PHP javított verziójára történő frissítés szükséges.

Szabályok

A Lorikeet Security a következő detektálási és fenyegetettségvadászati szabályokat tette közzé a sérülékenységekhez kapcsolódóan.

Linux rendszereken auditd szabály javasolható a webkiszolgálói fiókokból (euid=33) indított shellfolyamatok, valamint a /tmp és /dev/shm könyvtárakba történő írás figyelésére:

```
# Monitor execution of shells from web server user accounts
-a always,exit -F arch=b64 -S execve -F euid=33 -k web_shell_exec
-a always,exit -F arch=b32 -S execve -F euid=33 -k web_shell_exec
# Monitor writes to writable web directories and temp locations
-w /tmp -p wa -k web_tmp_write
-w /dev/shm -p wa -k web_shm_write
```

Konténeres és Kubernetes-környezetekhez Falco-szabály érhető el, amely kritikus riasztást generál, ha PHP-FPM vagy Apache worker folyamatból shell indul.

```
- rule: PHP Worker Spawned Shell
  desc: Detects an interactive shell spawned by a PHP-FPM or Apache worker
  condition: >
    spawned_process and
    proc.name in (bash, sh, dash, zsh, ksh) and
    proc.pname in (php-fpm, apache2, httpd, php)
  output: >
    "Critical: Shell spawned by PHP runtime (user=%user.name
command=%proc.cmdline parent=%proc.pname container_id=%container.id)"
```

priority: CRITICAL
tags: [security, php, rce, mitre_execution]

A Suricata és a Snort IDS a CVE-2026-109618 kihasználására utaló, a Zend Engine OOM-korlátjait célzó multipart POST kérések azonosítására készült szabálya:

alert http $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (

msg:"ATTACK-RESPONSES PHP Zend Engine OOM Heap Grooming Attempt (CVE-2026-109618)";
flow:to_server,established;
content:"POST"; http_method;
content:"multipart/form-data"; http_header;
pcre:"/Content-Length\x3a\s(?:1[0-9]{8,}|[2-9][0-9]{7,})/Hi";*
threshold:type both, track by_src, count 5, seconds 60;
classtype:web-application-attack;
sid:2026109618; rev:1;
)

A webszerver naplóiban az alábbi jelenségek utalhatnak kihasználási kísérletre vagy sikeres támadásra:

- ismétlődő HTTP 500 válaszok nulla vagy egy bájtos választesttel,
- PHP-FPM hibanaplóban SIGSEGV vagy SIGABRT miatti child process leállás,
- a www-data, apache vagy nobody fiókokból induló, nem szabványos TCP-portokra irányuló kimenő kapcsolatok,
- a /var/log/php-fpm.log módosítása, illetve crash dumpok megjelenése.

A nyilvános proof-of-concept eszközökhöz köthető vizsgálatok a Mozilla/5.0 (php2shell-poc) és a php2shell-verify/1.0 User-Agent értékekkel azonosíthatók a hozzáférési naplókban. Ezek a kérések a webszerver rétegén blokkolhatók, mielőtt a PHP futtatókörnyezet meghívásra kerülne.

Végponti szinten gyanús jel, ha webkiszolgálói vagy PHP-futtatókörnyezeti folyamatból shell, parancsértelmező vagy hálózati segédprogram indul. Linux, Docker és Kubernetes környezetben a php-fpm, apache2, httpd, php-cgi és

frankenphp folyamatokból induló sh, bash, dash, zsh, python, perl, curl, wget, nc vagy socat, míg Windows Server és IIS környezetben a w3wp.exe, php-cgi.exe vagy httpd.exe folyamatokból induló cmd.exe, powershell.exe, pwsh.exe, certutil.exe vagy bitsadmin.exe folyamat tekinthető kritikus riasztásnak.

A legfrissebb információkért kérjük ügyfeleinket, hogy folyamatosan kövessék a Nemzeti Kiberbiztonsági Intézet weboldalát.

+36-1-336-4833 csirt@nki.gov.hu