



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 kód futtatáshoz 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 kód futtatáshoz vezethet.

A PHP projekt a következő verziókban tette közzé a javítást:

- PHP 8.5.12,





- 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 kitétséget, 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 kéreisméret, a bemeneti mezők száma, a multipart részek száma, a fejlécek száma és a beágyazási mélység korlátozása javasolt a webservert 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 memórafoglalási 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, kérezenként 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.

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

