



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 fejlesztői 2026. október 21-én 14:00 UTC-kor (magyar idő szerint 16:00 órakor) tervezik közzétenni a két sérülékenységet javító biztonsági frissítéseket. A CVE-2026-109618 és CVE-2026-109619 azonosítójú sérülékenységek egyaránt kritikus, 9,2-es CVSS v4.0 súlyossági besorolást kaptak. Részletes technikai információk egyelőre nem állnak rendelkezésre, azonban az eddig megjelent információk alapján a sérülékenységek sikeres kihasználása lehetővé teheti a támadók számára, hogy hitelesítés nélkül, távolról tetszőleges kódot futtassanak az érintett szervereken.

Az NBSZ NKI nyomtatékosan javasolja, hogy az érintett szervezetek készüljenek fel a biztonsági frissítések haladéktalan telepítésére, és azokat a megjelenésüket követően a lehető legrövidebb időn belül alkalmazzák. Amennyiben a frissítés nem végezhető el azonnal, javasolt az internet felől elérhető érintett rendszerek külső hálózatoktól történő elkülönítése, vagy szükség esetén működésük ideiglenes felfüggesztése a sérülékenységek megszüntetéséig.

A sérülékenységek pontos technikai részletei, az érintett verziók köre és a rendelkezésre álló javítások várhatóan a biztonsági frissítések megjelenésével egy időben válnak ismertté. Az NBSZ NKI a rendelkezésre álló információk alapján folyamatosan frissíti a sérülékenységekkel kapcsolatos tájékoztatást, amely az alábbi hivatkozásokon lesz elérhető:

[CVE-2026-109618](#)

[CVE-2026-109619](#)

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

