



Riasztás a WordPress Core-t érintő sérülékenységről

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézete riasztást ad ki a széles körben használt WordPress tartalomkezelő rendszer (Core) aktívan kihasznált sérülékenysége miatt. A CISA 2026. szeptember 25-én vette fel a KEV-katalógusába. A hiba hitelesítés nélkül kihasználható, és bizonyos feltételek teljesülése esetén távoli kódfuttatáshoz vezethet.

A [CVE-2026-87902](#) azonosítón nyomon követett, magas súlyosságú sérülékenység önmagában helyi fájl beágyazását (Local File Inclusion) teszi lehetővé. Ez távoli kódfuttatássá (RCE) akkor válik, ha a szerverkörnyezet és az aktív téma is teljesít bizonyos előfeltételeket. Az alábbi feltételeknek együtt kell fennállniuk:

1; A téma tartalmaz page- előtagú főkönyvtárat. Az aktív témában kell lennie egy olyan legfelső szintű könyvtárnak, amelynek neve page- előtaggal kezdődik, például page-templates. Ez a legacy Twenty Twelve és Twenty Fourteen témákra igaz, valamint egyes népszerű külső témákra, például a Neve, Hestia és Sydney. A támadási útvonalnak egy valódi page- könyvtárral kell kezdődnie, és csak onnan léphet ki a témakönyvtárból.

2; A szerveren létezik egy olvasható célfájl. A beágyazott .php fájlak olvashatónak kell lennie a webszerver fiókja számára. A támadók a PEAR pearcmd.php fájlját használják erre, ha a PHP-ban a register_argc_argv értéke On. Ilyenkor a query string \$argv formában kerül a beágyazott scripthez, így a +config-show és a +config-create parancsként értelmeződik. A hivatalos Docker php image érintett. Az alapértelmezett cPanel-konfiguráció is érintett, ha 8.5 előtti PHP fut.

Érintett rendszerek

A WordPress Core 4.7.0 és 7.1.1 közötti kiadásai sérülékenyek. A javított verziót ágankénti backport adja:





Ág	Sérülékeny verziók	Javított verzió
7.1	7.1.0 - 7.1.1	7.1.2
7.0	7.0.0 - 7.0.5	7.0.6
6.9	6.9.0 - 6.9.8	6.9.9
6.8	6.8.0 - 6.8.9	6.8.10
6.7	6.7.0 - 6.7.8	6.7.9
6.6	6.6.0 - 6.6.8	6.6.9
6.5	6.5.0 - 6.5.11	6.5.12
6.4	6.4.0 - 6.4.11	6.4.12
6.3	6.3.0 - 6.3.11	6.3.12
6.2	6.2.0 - 6.2.12	6.2.13
6.1	6.1.0 - 6.1.13	6.1.14
6.0	6.0.0 - 6.0.15	6.0.16
5.9	5.9.0 - 5.9.17	5.9.18
5.8	5.8.0 - 5.8.16	5.8.17
5.7	5.7.0 - 5.7.18	5.7.19
5.6	5.6.0 - 5.6.20	5.6.21
5.5	5.5.0 - 5.5.21	5.5.22
5.4	5.4.0 - 5.4.22	5.4.23
5.3	5.3.0 - 5.3.24	5.3.25
5.2	5.2.0 - 5.2.27	5.2.28
5.1	5.1.0 - 5.1.25	5.1.26
5.0	5.0.0 - 5.0.28	5.0.29
4.9	4.9.0 - 4.9.32	4.9.33
4.8	4.8.0 - 4.8.31	4.8.32
4.7	4.7.0 - 4.7.36	4.7.37

Javítás

Frissíteni kell az adott ágon elérhető javított kiadásra.

Kockázatcsökkentés





- Ellenőrizni kell, hogy az aktív téma tartalmaz-e page- előtagú főkönyvtárat, és hogy a PHP-ban be van-e kapcsolva a register_argc_argv. A register_argc_argv kikapcsolása nem szünteti meg a beágyazást, de megszakítja a pearcmd láncot. Így információszivárgás marad, kód futtatás nem.
- Ideiglenes védelemként a pagename paraméterben tiltani kell a path traversal szekvenciákat. Egy valódi oldalnév ilyen nem tartalmaz, ezért a normál forgalmat nem zavarja.

Kompromittálódás ellenőrzése

A hozzáférési naplókban a következő jelek utalnak kihasználásra:

- A pagename paraméterben %2e%2e vagy %252e%252e szerepel, akár a query stringben, akár a POST törzsben.
- A pagename értéke templates%2f vagy más page- könyvtárnévvel kezdődik.
- A pagename és a page_id együtt jelenik meg a gyökérkönyvtárban vagy az /index.php-n. Ez ritka a normál forgalomban.
- Bármely kérés tartalmazza a pearcmd, +config-show vagy +config-create stringet.
- Egy normál oldal URL-jére OPML vagy RSS tartalmú, 200-as válasz érkezik. Ez azt jelzi, hogy az első fázisú próba sikeres volt.
- A gazdagépen ellenőrizni kell a /tmp és a /var/tmp könyvtárat váratlan .php fájlokra. Megfigyelt fájlnevek: wp-pear-rce-flag.php, poc87902.php, luci_<random>.php, zeta_<random>.php. Ilyen fájl jelenléte azt jelzi, hogy a támadás sikeres volt, és a gazdagépet kompromittálni kell tekinteni. A javítás előtt kitett rendszereknél a korábbi naplókat is át kell nézni.

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

