

> HÁTTÉRANYAG SZAKMABELIEKNEK

Brotli-hiba (Node2Shell/HTTP2Shell): soron kívüli javítások a .NET-ben, a Node.js-ben, a PHP-ban és a Python-csomagokban

Egy tömörítő, amiről nem tudtad, hogy használsz

Esemény: 2026. október 21. (soron kívüli javítások: október 21-26.)

Lezárva: 2026. október 27. (kutatási változat: v1)

AI-csapattal készült, átnézte: Péter

Összefoglaló

A Google Brotli tömörítőkönyvtárának dekóderében határon túli írási hiba (CVE-2026-111497, „Node2Shell/HTTP2Shell”) van, amely egy speciális tömörített adatfolyammal összeomlást, memóriaszivárgást és bizonyos esetekben kódfuttatást okozhat. Mivel sok szoftver saját példányt épít be a könyvtárból, egy hét alatt soron kívüli javítás jelent meg a Node.js-hez, a .NET-hez, a PHP Windows-csomagjaihoz, a Python-csomagokhoz, a Bunhoz, az Envoyhoz és az Istióhoz. Vadonbeli kihasználásról 2026. október 23-ig nem tudni, de nyilvános PoC és kutatói demonstráció létezik. A legfontosabb teendő: leltár arról, hol van Brotli a környezetben, majd frissítés, konténer-újraépítés és újraindítás, mert a rendszerkönyvtár frissítése a beépített példányokat nem javítja.

KULCSMEGÁLLAPÍTÁSOK

- A hiba a Brotli C-dekóderben van (1.0.3–1.2.0), javítva az 1.0.10, 1.1.1 és 1.2.1 kiadásban (2026. október 21.).
- A rendszer Brotli-frissítése nem javítja a saját példányt beépítő alkalmazásokat (Node.js, .NET egyes változatai, PHP Windows-csomagok): ezeket külön kell frissíteni és újraindítani.
- Két irányból érkezhetsz rossz adat: befelé (tömörített kérésörzs) és kifelé (idegen szerverről letöltött válasz) – utóbbit a WAF nem látja, és az Accept-Encoding módosítása sem véd.
- A súlyosság vitatott (CVSS 8,1–9,2): kódfuttatást csak nehezen, nem megbízhatóan demonstráltak, a valószínűbb hatás a szolgáltatásmegtagadás.
- Magyar érintettség és hazai hatósági figyelmeztetés a kutatás idején nem ismert.

Mi történt

A Google nyílt forrású **Brotli** tömörítőkönyvtárának dekóderében (a kibontást végző részben) határon túli írási hiba (out-of-bounds write) van: **CVE-2026-111497**. Egy speciálisan összeállított Brotli-adatfolyam a kibontás közben a dekóder egy belső pufferén túlra írhat. Ennek következménye lehet összeomlás, memóriaszivárgás, és bizonyos körülmények között távoli kód futtatás. A hibát a sajtó és a kutatók több néven emlegetik: **Node2Shell** (mert először a Node.js-nél jelent meg), **HTTP2Shell** (mert kiderült, hogy minden HTTP-t használó ökoszisztémát érint) és tréfásan **Broccoli2Shell**. ([SecurityWeek](#); [Red Hat](#); [Aikido](#)) – **megerősített**

A Brotli az a tömörítés, amelyet a böngészők és a szerverek a weben a gzip mellett/helyett használnak (Content-Encoding: br). Sok szoftver saját példányt épít be belőle, ezért a hiba nem egy termék, hanem egy **beépített alkatrész** hibája: ahol a szoftver megbízhatatlan forrásból érkező Brotli-adatot bont ki, ott elérhető lehet.

Érintett és javított Brotli-verziók: 1.0.3–1.2.0 érintett; javítva az **1.0.10, 1.1.1 és 1.2.1** kiadásban (2026. október 21.). ([SecurityWeek](#); [Wiz](#)) – **megerősített**

Felfedezés: a Node.js a hiba felfedezését az OpenAI Codex Security csapatának tagjainak tulajdonítja; a beszámolók szerint az OpenAI red teaming közben találta a hibát, és ő értesítette a Brotli fejlesztőit és a downstream projekteket. A gyökérokot javító változtatás már 2026 februárjában bekerült a Brotli forráskódjába, de akkor nem tudták, hogy biztonsági hiba, és nem jelent meg hozzá kiadás. ([SecurityWeek](#); [Broccoli2Shell tracker](#); [The Hacker News](#)) – **jelentett** (több forrás; az OpenAI saját közleményét nem vizsgáltuk)

Kihasználás: a vadonban zajló támadásról 2026. október 23-ig nem érkezett jelentés, és a CISA ismerten kihasznált sebezhetőségek katalógusában (KEV) sem szerepelt. Nyilvános koncepcióbizonyíték (PoC) és egy kutatói demonstráció létezik (lásd lent). ([Sysdig](#); [The Hacker News](#); [SecurityWeek](#)) – **megerősített** (állapot október 23-án)

Idővonal

Dátum	Esemény	Forrás
2026. február	A gyökérokot javító módosítás bekerül a Brotli forrásába, biztonsági jelölés és kiadás nélkül (jelentett)	SecurityWeek , The Hacker News
2026. október 14.	A Node.js előre bejelenti a biztonsági kiadást (érintett ágak, magas súlyosság)	Sysdig
2026. október 21.	Node.js-javítások: 22.23.4, 24.22.1, 26.12.1 (összesen 10 CVE a kiadásban); a Brotli 1.0.10 / 1.1.1 / 1.2.1 megjelenik	The Hacker News , Sysdig
2026. október 21.	Néhány órával a javítás után megjelenik az első nyilvános tároló a CVE-hez	Sysdig
2026. október 22.	A CVE és a GitHub-tanácsadás publikus; Python Brotli 1.2.1 a PyPI-on; az Imperva kód futtatást demonstrál egy Node.js-buildön	Broccoli2Shell tracker , The Hacker News
2026. október 23.	brotliffi 1.2.1.0; kiderül, hogy a hatás túlmeleg a Node.js-en (Bun, Envoy, Istio javítások); nincs KEV-bejegyzés	Aikido , Sysdig
2026. október 25. (vasárnap)	A Microsoft soron kívüli javítást ad ki: .NET 8/9/10, .NET 11 RC3, Visual Studio, PowerShell	BleepingComputer , SecurityWeek

Dátum	Esemény	Forrás
2026. október 26. körül	A PHP öt napon belül másodszor építi újra a Windows-csomagjait („-1” buildek, Brotli 1.2.1-gyel)	The Hacker News

Szereplők és háttér

- **Google / Brotli-projekt:** a könyvtár gazdája, kiadta a javított verziókat. A Google a CVE-rekordban CVSS 4.0 szerint **9,2 (kritikus)** pontszámot adott. ([The Hacker News](#); [Sysdig](#))
- **OpenAI Codex Security:** a Node.js szerint ők jelentették a hibát. Érdekes háttér: egy AI-alapú biztonsági csapat talált hibát egy széles körben használt C-könyvtárban. ([SecurityWeek](#); [Broccoli2Shell tracker](#))
- **Node.js-projekt:** elsőként adott ki javítást (október 21.), súlyosság: magas. ([The Hacker News](#))
- **Microsoft:** CVSS 3.1 szerint 8,1, jogosultságkiterjesztésként sorolta be, „Exploitation More Likely” értékeléssel; .NET-re és Visual Studióra kritikus, PowerShellre fontos besorolás. ([SecurityWeek](#))
- **PHP-projekt:** a Windows-csomagokba beépített Brotli miatt újraépítette a csomagokat, alig néhány nappal a PHP2Shell-javítások után. ([The Hacker News](#))
- **Python-ökoszisztéma:** a Brotli és a brotlicffi csomagok javultak; a népszerű HTTP-kliensek (urllib3, requests, httpx, aiohttp) automatikusan használják, ha telepítve vannak. ([Aikido](#); [Broccoli2Shell tracker](#))
- **Kutatók és biztonsági cégek:** Imperva (kihasználhatósági kutatás), Aikido és OpenSourceMalware (Python-hatás), Wiz, Sysdig (észlelés).

A hét kontextusa: ez a „minden is Shell” hét újabb nagy hibája a PHP2Shell (két kritikus PHP-hiba, október 21-i javításokkal) után. A közös tanulság: a webes infrastruktúra mélyén lévő, ritkán emlegetett összetevők hibái egyszerre sok ökoszisztémát érintenek. ([The Hacker News](#))

Hasonló korábbi esetek (háttér): a beépített könyvtárak („vendored dependencies”) problémája régi ismerős: a zlib, a libwebp vagy az xz-utils esetében is az volt a nehézség, hogy egyetlen alsó szintű komponens hibája után minden, azt saját példányként tartalmazó terméknek külön kellett frissítenie. – **feltételezés** (szerkesztői párhuzam, nem e kutatás forrásaiból)

Hogyan működik

RED // TÁMADÓI SZEMMEL

- **Az alapötlet:** a tömörítés lényege, hogy kicsi adatból a kibontó nagy adatot állít elő, tehát a kibontó *megbíz* abban, amit a tömörített adat leír. Ha a leírás hibás, és a dekóder ezt nem veszi észre, a dekóder rossz helyre írhat a memóriában.
- **A gyengeség fogalmilag:** a nyilvános elemzések szerint a dekóder egyik része a „hibás adat” és a „még kell több adat” helyzetet ugyanúgy jelezte, és egy gyors ágon figyelmen kívül hagyta az eredményt. Így egy szándékosan elrontott adatfolyam rávehette, hogy egy kis belső pufferbe tovább fogadjon adatot, és túlírjon rajta. A javítás egyszerűen kemény formátumhibát ad vissza. ([Broccoli2Shell tracker](#); [Red Hat](#))
- **Honnan érkezhetsz a rossz adat:** két irányból.
- **Befelé:** valaki tömörített kérés-törzset küld a szervernek (Content-Encoding: br), és a webkeretrendszer automatikusan kibontja.
- **Kifelé:** a te alkalmazásod tölt le valamit egy idegen szerverről (webhook, linkelőnézet, crawler, API-hívás), és az HTTP-kliens automatikusan kibontja a Brotli-választ. Ez a kényesebb irány, mert ezt a

tűzfal vagy a WAF nem látja. ([Aikido](#); [Broccoli2Shell tracker](#))

- **Miért lehet rejtett:** az alkalmazás kódjában sehol nem kell a „Brotli” szónak szerepelnie. Elég, ha egy HTTP-kliens vagy middleware automatikus kibontást használ, vagy ha a csomag tranzitív függőségként fel van telepítve. ([Wiz](#); [Aikido](#))
- **Miért nem triviális:** a Red Hat szerint a támadás összetettsége magas, és a modern védelmek (ASLR, NX, FORTIFY_SOURCE, SELinux) megnehezítik a kód futtatást, de az összeomlást nem akadályozzák meg. A legvalószínűbb hatás ezért a szolgáltatásmegtagadás (DoS); a kód futtatás lehetséges, de nem megbízható. ([Red Hat](#); [The Hacker News](#))
- **A „rendszerfrissítés nem elég” csapda:** ha egy alkalmazás saját Brotli-példányt épít be (Node.js, a .NET egyes változatai, a PHP Windows-csomagjai, Git for Windows-szerű eszközök), azt a rendszer `libbrotli` frissítése nem javítja. És fordítva: a futó folyamat a régi kódot használja, amíg újra nem indítod. ([BleepingComputer](#); [SecurityWeek](#))

Hatás és magyar vonatkozás

- **Méret:** a Brotli a web egyik alapvető tömörítése; az érintett kör minden olyan szoftver, amely megbízhatatlan Brotli-adatot bont ki: Node.js, Bun, .NET, PHP Windows-csomagok, Python HTTP-kliensek, Envoy és Istio (szolgáltatáshálók, API-átjárók), Go-könyvtár, Java `brotli4j`, továbbá asztali eszközök. ([Wiz](#); [Aikido](#); [SecurityWeek](#))
- **Kit érint leginkább:** a szervezeteket és fejlesztőket, akik webes szolgáltatást, API-t, konténeres vagy szerver nélküli (serverless) alkalmazást üzemeltetnek; különösen ott, ahol a szolgáltatás felhasználó által megadott URL-eket tölt le. A magánszemélyt közvetlenül kevésbé: nála a böngésző és az alkalmazások szokásos frissítése a teendő.
- **Kár:** ismert kárról vagy támadásról 2026. október 23-ig nincs jelentés. ([Sysdig](#))
- **Magyar vonatkozás: magyar érintettség nem ismert.** Az NBSZ NKI riasztásai között a kutatás idején nem találtunk erre a hibára vonatkozó figyelmeztetést, és magyar sajtóban sem találtam érdemi beszámolót. Sok hazai webes szolgáltatás .NET-en vagy Node.js-en fut – ez valószínűsíti, hogy a hazai szervezetek is érintettek lehetnek, de konkrét adat nincs. – **feltételezés**
- **Régió:** közép-kelet-európai specifikus adatot nem találtunk.

Mit tegyél

BLUE // MIT TEGYÉL MOST

Magánszemély

- **Frissítsd** a böngésződet, a telefonodat és az asztali alkalmazásaidat, ha frissítést kínálnak; a gyártók a saját beépített Brotli-példányukat így javítják.
- **Ha fejlesztői eszközöket használsz** (Node.js, Python, Git, PHP a saját gépeden), frissítsd azokat is a legújabb verzióra.
- **Ne ess pánikba:** vadonbeli támadásról nincs hír, és a hiba elsősorban szervereket és fejlesztői eszközöket érint. A böngészők érintettségéről nincs ellenőrzött adat (lásd Nyitott kérdések), ezért a szokásos automatikus frissítés a teendő.

Kisvállalkozás

- **Kérdezd meg** a tárhely- vagy fejlesztő partneredet: Node.js, .NET, PHP (Windows) vagy Python fut-e a weboldalad, webshopod alatt, és frissítették-e október 21. után.

- **Ha te üzemeltetsz:** frissítsd a Node.js-t (22.23.4 / 24.22.1 / 26.12.1), a .NET-et (8.0.33 / 9.0.22 / 10.0.14), a Python Brotli-t (1.2.1) és brotlicffi-t (1.2.1.0), majd **indítsd újra** a szolgáltatásokat.
- **Ha Windows alatt PHP-t futtatsz:** cseréld a csomagot a „-1” végű buildre (pl. 8.5.12-1), és a php.net letöltési oldalán ellenőrizd az SHA-256 hash-t; a php -v ugyanazt a verziót mutatja, tehát abból nem látod.
- **Ha a Node.js-ed 20.x, 23.x vagy 25.x:** ezek életciklusuk végén vannak, javítás nem jár hozzájuk; tervezd a váltást 22-re, 24-re vagy 26-ra.

Szervezet

- **Készíts leltárt** arról, hol van Brotli a környezetben: runtime-ok, csomagok, lockfájlok, konténerképek, CI-, build- és fejlesztői gépek, beépített (vendored) példányok. Ne hagyatkozz csak a sebezhetőség-szkennerre: a beszámolók szerint egyes eszközök eleinte nem jelezték megbízhatóan az érintett PyPI-verziókat. ([Broccoli2Shell tracker](#); [Aikido](#))
- **Priorizálj az elérhetőség szerint:** előbb azokat a szolgáltatásokat frissítsd, amelyek idegen URL-eket töltenek le, vagy Brotli-tömörített kéréstörzset fogadnak. ([Broccoli2Shell tracker](#); [Wiz](#))
- **Frissíts, építs újra, indíts újra:** a csomagfrissítés után építsd újra a konténerképeket javított alapképre, frissítsd a lockfájlokat, indítsd újra a folyamatokat, és ellenőrizd, hogy a futó bináris valóban a javított. ([SecurityWeek](#); [SOC Prime](#))
- **Átmeneti enyhítés, ha nem tudsz azonnal frissíteni:** utasítsd el a Content-Encoding: br kéréstörzseket a proxy-n, terheléelosztón vagy WAF-on; kapcsold ki az automatikus Brotli-kibontást; Pythonban távolítsd el a Brotli/brotlicffi csomagot (a kliensek gzipre esnek vissza). Az Accept-Encoding-ból a br törlése önmagában **nem véd**, mert a szerver ettől még küldhet Brotli-választ. ([Broccoli2Shell tracker](#); [The Hacker News](#); [BleepingComputer](#))
- **Linuxon nézd meg, melyik Brotli fut:** a Red Hat szerint a Node.js és a .NET egyes változatai a rendszer Brotliját, mások a beépítettet használják; ettől függ, hogy a brotli/libbrotli vagy a runtime csomagot kell frissíteni. ([Red Hat](#))
- **Figyeld a jeleket:** webes Node.js- vagy .NET-folyamatok ismételt összeomlása, shellt indító szolgáltatás, váratlan kimenő kapcsolat. ([Sysdig](#))

Szakmai blokk

CVE: CVE-2026-111497 – határon túli írás (out-of-bounds write) a Brotli C-dekóder blokktypus-váltást kezelő részében.

Pontszámok: - Google: CVSS 4.0 – 9,2 (kritikus) - Red Hat: CVSS 3.1 – 8,1 (fontos), AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H - Microsoft: CVSS 3.1 – 8,1, jogosultságkiterjesztés, „Exploitation More Likely” - Node.js: „High” ([The Hacker News](#); [Red Hat](#); [SecurityWeek](#))

Érintett → javított verziók:

Komponens	Érintett	Javított	Forrás
Google Brotli (C)	1.0.3–1.2.0	1.0.10, 1.1.1, 1.2.1	Wiz , SecurityWeek
Node.js	22.x, 24.x, 26.x a javítás előtt; 20/23/25 EOL, javítás nélkül	22.23.4, 24.22.1, 26.12.1	The Hacker News , Sysdig
.NET	8, 9, 10, 11 előzetes	8.0.33, 9.0.22, 10.0.14, 11 RC3	BleepingComputer , SecurityWeek

Komponens	Érintett	Javított	Forrás
Visual Studio, PowerShell	VS 2019/2022/2026; PowerShell 7.4/7.5/7.6	2026. október 25-i frissítések	SecurityWeek
PHP Windows-csomagok	8.2–8.5 (Brotli 1.2.0 a korábbi buildekben)	8.5.12-1, 8.4.27-1, 8.3.36-1, 8.2.35-1	The Hacker News
Python Brotli	1.0.3–1.2.0	1.2.1	Aikido , Wiz
Python brotlicffi	1.0.3–1.2.0.x	1.2.1.0	Aikido , Wiz
Bun	1.0.21–1.4.3	1.4.4	Wiz , Sysdig
Envoy	1.36.11, 1.37.7, 1.38.5, 1.39.2	1.36.12, 1.37.8, 1.38.6, 1.39.3, 1.40.0	Wiz
Istio	1.29.0–1.29.8, 1.30.0–1.30.5, 1.31.0–1.31.1	1.29.9, 1.30.6, 1.31.2	Wiz
Go andybalholm/brotli	< v1.2.7	v1.2.7	Wiz

Elérési utak (fogalmilag): - Node.js: node:zlib közvetlen használata; a beépített fetch() (undici) automatikus kibontása; Express 5 alapértelmezett törzsfeldolgozása; Koa, Fastify tömörítő bővítménnyel. ([Sysdig](#); [The Hacker News](#)) - .NET: ASP.NET Core request decompression, HttpClient automatikus válaszkibontás, System.IO.Compression Brotli API-k; alpból egyik sincs bekapcsolva. ([BleepingComputer](#)) - PHP (Windows): a cURL-bővítmény, ha az automatikus kibontás be van kapcsolva (CURLOPT_ENCODING; üres érték = minden támogatott formátum). Alpból ki van kapcsolva, de HTTP-kliens könyvtárak bekapcsolhatják. ([The Hacker News](#)) - Python: urllib3/requests, httpx (brotli extrával), aiohttp, Scrapy – ha a csomag telepítve van; importálni nem kell. ([Aikido](#)) - curl: csak ha Brotlival van fordítva, és a kibontás be van kapcsolva; a szerver Content-Encoding: br fejléce önmagában elindítja a kibontást. ([Lilting](#); [The Hacker News](#))

Nyilvános tracker szerint még javítatlan (2026. október 26.): DuckDB, Apache Arrow, 7-Zip-zstd, p7zip, EDK II és mások; a lista nem teljes. ([SecurityWeek](#); [Broccoli2Shell tracker](#))

MITRE ATT&CK (szerkesztői leképezés): T1190 (nyilvános alkalmazás kihasználása), T1499 (végponti szolgáltatásmegtagadás), T1059 (parancsértelmező – sikeres kód futtatás után), T1105 (eszközletöltés), T1552 (titkok a futtatókörnyezetből). – **feltételezés**

Észlelési ötletek: - runtime-szenzor maga a túlírást nem látja; a sikeres kihasználás *utáni* viselkedést kell figyelni: összeomlás után programindítás ugyanabban a munkaterhelésben, shell a webes folyamat alatt, váratlan kimenő kapcsolat; ([Sysdig](#)) - ismétlődő összeomlás ugyanazon a szolgáltatáson (próbálkozás jele lehet); - Content-Encoding: br kérések olyan végpontokon, ahol ez nem szokásos (elérhetőségi jel, nem javítás); - leltár: futó Node.js-verzió és beépített Brotli-verzió, betöltött libbrotlidec, pip/lockfájl-függőségfák. ([Broccoli2Shell tracker](#))

Indikátorok: hivatalos IOC-lista nem ismert; a Broccoli2Shell tracker kifejezetten nem közöl IOC-t és támadási szignatúrát.

Hivatalos ajánlások: Microsoft .NET-biztonsági közlemény (dotnet/announcements #494), Red Hat RHSA-2026-015, Node.js 2026. októberi biztonsági kiadás, PHP Windows-letöltési oldal (SHA-256 hash-ek).

Ellentmondások és nyitott kérdések

Nyitott kérdések

- **Mennyire súlyos valójában?** A pontszámok 8,1 és 9,2 között szórnak, és a kutatók megosztottak: az Imperva egy hivatalos Node.js-buildön kódfuttatást demonstrált (nem minden próbálkozásra), a nyilvános PoC viszont csak szándékosan gyengített buildön futtatott kódot, alapbuilden összeomlást és korlátozott memóriaolvasást okozott. Egyes kutatók szerint a hiba gyakorlatban csak szolgáltatásmegtagadásra jó. ([The Hacker News](#); [SecurityWeek](#))
- **PoC-k leírása eltér:** a BleepingComputer szerint „PoC exploitok jelentek meg a GitHubon”, a SecurityWeek és a The Hacker News pontosít: a nyilvános PoC kódfuttatást csak gyengített buildön ért el. ([BleepingComputer](#); [SecurityWeek](#))
- **Miért ilyen késői a riasztás?** A gyökérok javítása már februárban a forrásban volt, de biztonsági jelölés nélkül; így a beépített példányokat használók nem tudtak róla. Hogy ez hogyan fordulhatott elő, arról a projekt részletes magyarázatát nem találtunk.
- **Böngészők és asztali alkalmazások:** a nyilvános anyagok nem tárgyalják részletesen, hogy a nagy böngészők és az Electron-alapú alkalmazások érintettek-e.
- **Linux-disztribúciók:** a javítások fokozatosan érkeznek; a backportolt verziószámok régebbinek tűnhetnek, mint az upstream, ezért a disztribúció saját közleménye a mérvadó.
- **Magyarország:** hazai hatósági figyelmeztetés és hazai érintettségi adat a kutatás idején nem ismert.

Forrásértékelés

Forrás	Típus	Megbízhatóság	Mit támaszt alá
Red Hat – CVE-2026-111497	cég (gyártói tanácsadás)	magas	gyökérok helye, CVSS 3.1, rendszer- vs. beépített Brotli, védelmek hatása
SecurityWeek	sajtó	magas	ökoszisztémák, Microsoft-javítások, felfedezés, PoC-vita, tracker
BleepingComputer	sajtó	magas	.NET-verziók, elérési utak, enyhítések
The Hacker News – PHP Windows	sajtó	közepes–magas	PHP „-1” buildek, cURL-út, pontszámok, CISA-állapot
The Hacker News – Node.js-kiadás	sajtó	közepes–magas	Node.js-verziók, a kiadás többi CVE-je, idővonal
The Hacker News – Imperva-demó	sajtó	közepes–magas	kihasználhatóság, PoC-állapot
Wiz	kutató (biztonsági cég)	magas	verziótábla (Bun, Envoy, Istio, Go), teendők
Sysdig	kutató (biztonsági cég)	magas	részletes idővonal, észlelés, EOL-ágak
Aikido	kutató (biztonsági cég)	közepes–magas	Python-hatás, HTTP-kliensek, elnevezés
Broccoli2Shell tracker	háttér (független összesítő)	közepes	gyökérok közérthetően, érintett/javítatlan lista, enyhítések
SOC Prime	kutató (biztonsági cég)	közepes	enyhítések, incidenskezelési teendők
Lilting	háttér (egyéni teszt-blog)	közepes	curl-viselkedés automatikus kibontásnál

