NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2025. 33. hét

HÍREK

- Komoly veszélyben a járműbiztonság: A Flipper Zero új firmware-je áttöri a rolling kódos védelmet
- Kritikus sebezhetőségek a WinRAR és 7-Zip szoftverekben
- ChatGPT 5 – 24 óra alatt jailbreak-elték meg
- A kártékony kódok elrejtésének új generációja
- Chipgyártói Patch Kedd: Számos sebezhetőséget orvosolt az Intel, az AMD és az Nvidia

STATISZTIKAI ADATOK

- Incidensek eloszlása típus és kockázati besorolás szerint
- Események eloszlása csapdatípusok alapján
- Támadott port szerinti eloszlás

TÁJÉKOZTATÁSOK, RIASZTÁSOK

- Riasztás Microsoft termékeket érintő sérülékenységekről
- Tájékoztatás Adobe szoftverek sérülékenységeiről

AKTUÁLIS TARTALMAK

- Az IDN homográf támadások
- Hogyan ismerhetjük fel az online álláshirdetős csalásokat? - SANS OUCH!

KONTAKT

edt@nki.gov.hu

PGP kulcs

FBC3 88A2 E465 BF51
AD58 A2D0 E9DD E078
ABD3 E75D

NEWS

IT biztonsági
HÍREK

Komoly veszélyben a járműbiztonság: A Flipper Zero új firmware-je áttöri a rolling kódos védelmet

(gbhackers.com)

Az autóipar egyik legkomolyabb biztonsági válságát idézheti elő az a nemrég felfedezett firmware, amely a népszerű Flipper Zero eszköz számára lehetővé teszi, hogy teljes mértékben megkerülje a rolling kódos védelmi rendszereket, amelyek jelenleg több millió modern jármű kulcsnélküli hozzáférését biztosítják világszerte. **Bővebben...**

Kritikus sebezhetőségek a WinRAR és 7-Zip szoftverekben

(gbhackers.com) (thehackernews.com)

2025 nyarán két népszerű fájlarchiváló szoftver, a WinRAR és a 7-Zip is komoly biztonsági problémák miatt került reflektorfénybe. **Bővebben...**

ChatGPT 5 – 24 óra alatt jailbreak-elték meg

(securityweek.com)

Két különböző biztonsági kutatócsoport is tesztelte az OpenAI nemrég bemutatott GPT-5 nyelvi modelljét, és mindkettő komoly biztonsági hiányosságokat fedezett fel. **Bővebben...**

A kártékony kódok elrejtésének új generációja

(gbhackers.com)

A kiberbiztonsági közösség figyelmét egyre inkább leköti a kártékony payload-ok (használati kódok) elrejtésének fejlődése, amely komoly kihívást jelent a webalkalmazás tűzfalak (WAF), az automatizált biztonsági eszközök és egyéb védelmi mechanizmusok számára. **Bővebben...**

AMD NVIDIA intel

Chipgyártói Patch Kedd: Számos sebezhetőséget orvosolt az Intel, az AMD és az Nvidia

(securityweek.com)

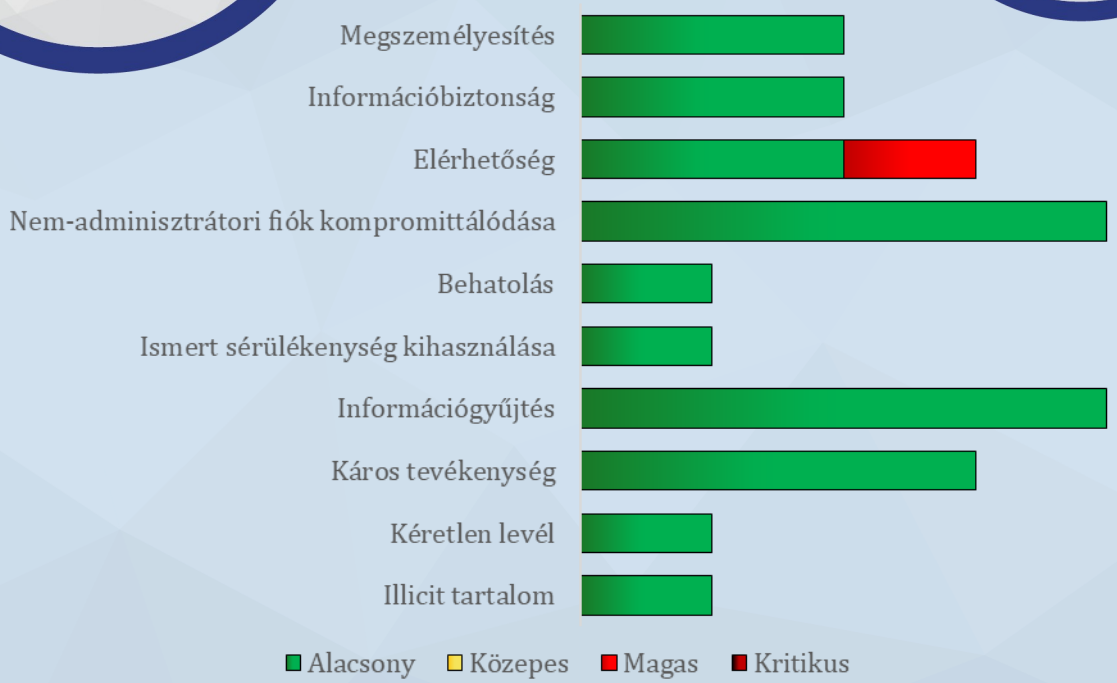
Kedden több tucat biztonsági közleményt adott ki az Intel, az AMD és az Nvidia, melyek a közelmúltban azonosított biztonsági hibákról tájékoztatták az ügyfeleket. **Bővebben...**

Statisztikai Adatok

2025.08.08.-2025.08.14.

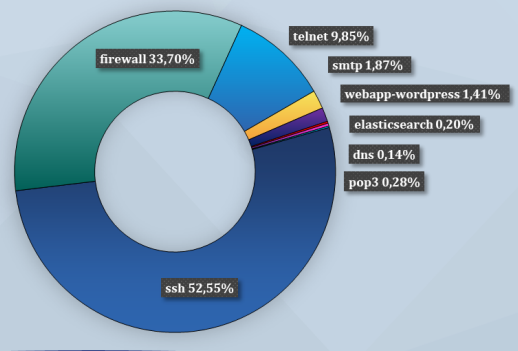
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

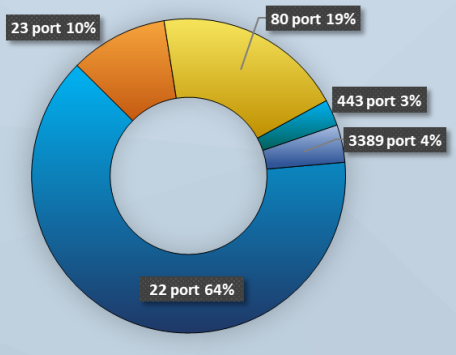
Fenyegetettségi szint: magas



Incidensek eloszlása típus és kockázati besorolás szerint

Az elosztott kormányzati IT-biztonsági csapdarendszerből (Gov1probe) származó adatok:





További érdekességekért, látogasson el **weboldalunkra**!

TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK

Riasztás Microsoft termékeket érintő sérülékenységekről

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet riasztást** ad ki a **Microsoft szoftvereket érintő** kritikus kockázati besorolású **sérülékenységek** kapcsán, azok súlyossága, kihasználhatósága és a szoftverek széleskörű elterjedtsége miatt.

A Microsoft 2025. augusztus havi biztonsági csomagjában összesen **111 különböző biztonsági hibát** javított, köztük **1 db nulladik napi** (zero-day) sebezhetőséget is amelyet a Microsoft tájékoztatása szerint **támadók még nem használtak ki**, de már a javítás előtt publikálásra került:

CVE-2025-53779

Bővebben...

Tájékoztatás Adobe szoftverek sérülékenységeiről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **tájékoztatót** ad ki az **Adobe** szoftverfejlesztő cég **termékeit érintő sérülékenységekkel kapcsolatban**, azok súlyossága, valamint az egyes biztonsági hibákat érintő aktív kihasználások miatt.

Bővebben...

Aktuális tartalmak

Az IDN homográf támadások
kiberbiztonsági elemzés

Jelen dokumentumunk célja bemutatni **a homografikus támadások veszélyeit és egyéb részleteit**. A homográfia eredetileg nyelvészeti és matematikai fogalom, amely **azonos írásmódú, de eltérő jelentésű** szavakat, illetve projektív transzformációkat jelöl. A kiberbiztonságban új értelmet nyert: itt a homografikus támadások olyan módszerek, amelyek **különböző, de vizuálisan hasonló karaktereket használnak fel hamis domain nevek létrehozására**.
Ezek a megtévesztő webcímek a felhasználók becsapását célozzák.

Elolvasom

További érdekességekért és IT biztonsággal kapcsolatos tartalmakért látogasson el LinkedIn oldalunkra!

Linked in

További érdekességekért, látogasson el **weboldalunkra**!

Aktuális tartalmak

Hogyan ismerhetjük fel az online álláshirdetős csalásokat?

SANS OUCH!

Megjelent a **SANS** és a **Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet** közös kiadványának 2025. augusztusi száma, melyben az **online álláshirdetések veszélyeivel** foglalkozunk. Bemutatjuk azt, hogy miért hatékonyak az ilyen típusú csalások, és miként védekezhetünk ellenük.

Elolvasom

További érdekességekért és IT biztonsággal kapcsolatos tartalmakért látogasson el LinkedIn oldalunkra!

Linked in

További érdekességekért, látogasson el **weboldalunkra**!