



# HÍRLEVÉL

Nemzetközi  
IT-biztonsági sajtószemle  
2024. 24. hét



## HÍREK

- Súlyos következményei vannak a Synnovist ért ransomware támadásnak
- Aktívan kihasznált sérülékenységek a Mali GPU kernel illesztőprogramjában
- A GitHub nevében adathalász emaileket kapnak a fejlesztők
- A Frontier Communications adatszivárgás több mint 750.000 embert érintett
- Az FBI megszerzett több mint 7000 LockBit dekódoló kulcsot



## SÉRÜLÉKENYSÉGEK

- Riasztás Adobe szoftverek sérülékenységeiről
- Riasztás Microsoft termékeket érintő sérülékenységekről



## IT BIZTONSÁGI TIPP

- KiberKedd: Napi átutalási limit beállítás  
Mit lehet róla tudni?



## STATISZTIKAI ADATOK

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



## KONTAKT

[edt@nki.gov.hu](mailto:edt@nki.gov.hu)

PGP kulcs

FBC3 88A2 E465 BF51  
AD58 A2D0 E9DD E078  
ABD3 E75D



# NEWS

## IT biztonsági HÍREK

### Súlyos következményei vannak a Synnovist ért ransomware támadásnak (bleepingcomputer.com)

Június 4-én a Synnovis patológiai és diagnosztikai részlegét ért zsarolóvírus támadás több londoni kórház működésében okozott komoly zavarokat. A támadást a Qilin (más néven Agenda) orosz hacker csoport indította a Synnovis ellen. **Bővebben...**

### Aktívan kihasznált sérülékenységek a Mali GPU kernel illesztőprogramjában (bleepingcomputer.com)

Biztonsági figyelmeztetést adott ki az Arm, amely a Bifrost és Valhall GPU kernel driverek memóriakezelési sebezhetőségéről szól. A sérülékenység a [CVE-2024-4610](#) néven követhető nyomon. **Bővebben...**

### A GitHub nevében adathalász emaileket kapnak a fejlesztők (bleepingcomputer.com)

A hackerek egy folyamatban lévő zsarolókampányban az adathalász támadások során a GitHub biztonsági és toborzási részlegeit veszik célba, hogy rosszindulatú OAuth szolgáltatással megosszák a tárhelyeket, majd törörlék a feltört adattárakat. **Bővebben...**

### A Frontier Communications adatszivárgás több mint 750.000 embert érintett (securityaffairs.com)

A RansomHub ransomware csoport azt közölte, hogy több mint 2 millió ügyfél adatait – nagyjából 5GB méretű fájl – lopta el az amerikai Frontier Communicationstól. **Bővebben...**



### Az FBI megszerzett több mint 7000 LockBit dekódoló kulcsot (securityweek.com)

Az FBI több mint 7000 dekódoló kulcsot szerzett meg, és arra sűrgeti az áldozatokat, hogy lépjenek kapcsolatba az Internet Crime Complaint Center-rel (IC3). **Bővebben...**

További hírekért, látogasson el **weboldalunkra!**



# TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK

## Riasztás Microsoft termékeket érintő sérülékenységekről

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

A Microsoft 2024. június havi biztonsági csomagjában összesen **51** különböző **biztonsági hibát javított**, köztük **1 nulladik napi (zero-day)** sebezhetőséget is, e sérülékenység esetében jelenleg nem áll fenn az aktív kihasználás lehetősége a sérülékeny rendszeren:

**CVE-2023-50868**

**CVE-2024-30080**

**CVE-2024-30078**

[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.

Összesen **167** különálló **CVE számmal rendelkező sérülékenység** került javításra, ezek közül – a gyártói besorolás szerint – **14 kritikus, 150 magas** és **3 alacsony** kockázati besorolású.

[Bővebben...](#)

További tájékoztatóért, látogasson el **weboldalunkra!**





# KiberKedd

IT biztonsági  
Tipp



**KiberPajzs**  
Védelem a pénzügyekben

## Napi átutalási limit beállítás Mit lehet róla tudni?

E havi **KiberKedd** tippünkben a bankszámlákhoz tartozó **napi átutalási limit** beállításának pénzügyi szaknyelvben: **műveleti értékhatár módosítás** szükségességére szeretnénk felhívni a figyelmet, amellyel a már esetlegesen sérelmünkre elkövetett csalások esetén is minimalizálható az okozott kár.

[Elovasom](#)

További érdekességekért és IT biztonsággal kapcsolatos tartalmakért látogasson el közösségi oldalainkra!



LinkedIn



Instagram



Facebook

További hírekért, látogasson el **weboldalunkra!**

Aktuális  
tartalmak



## DoS-támadások

az *ENISA Threat Landscape for DoS Attacks  
(January 2022 to August 2023)* című  
tanulmánya alapján

*CTI jelentés*

2023 novemberében kiadásra került az *ENISA Threat Landscape for DoS Attacks (January 2022 to August 2023)* című kiadvány, melynek konkrét célkitűzése, hogy egy átfogó tudásanyagot adjon át a legújabb DoS-támadásokról, beleértve a támadások motivációjának elemzését és a támadások hatását is.

Jelen CTI jelentés a fent említett tanulmány feldolgozásával kíván mélyebb betekintést nyújtani a legújabb támadási trendekről.

[Elovasom](#)

További érdekességekért  
és IT biztonsággal  
kapcsolatos tartalmakért  
látogasson el közösségi  
oldalainkra!



LinkedIn



Instagram



Facebook

További érdekességekért, látogasson el [weboldalunkra!](#)





# Statisztikai Adatok

2024.06.07.-2024.06.13.

Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:



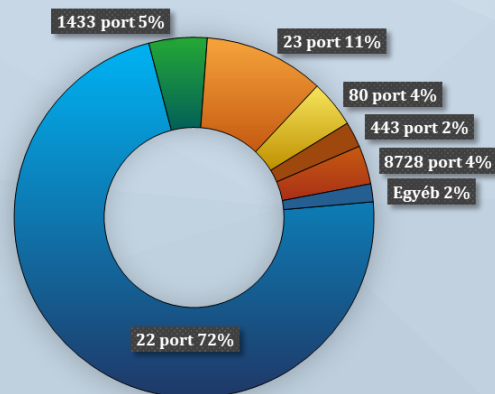
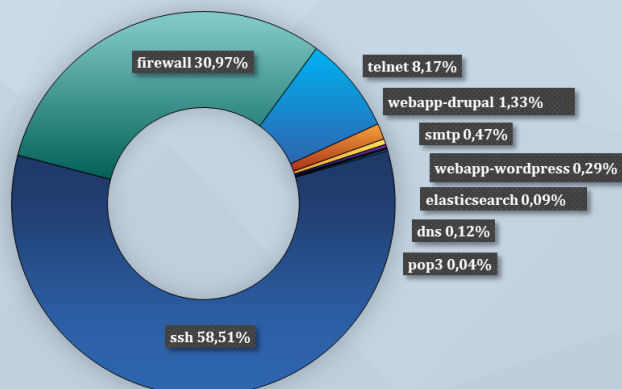
Fenyegetettségi szint: alacsony



■ Alacsony ■ Közepes ■ Magas ■ Kritikus

## Incidensek eloszlása típus és kockázati besorolás szerint

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



További érdekességekért, látogasson el [weboldalunkra!](#)

