



# HÍRLEVÉL

Nemzetközi  
IT-biztonsági sajtószemle  
2024. 20. hét



## HÍREK

- Feltörték az Europolt
- A Dell API kihasználásával 49 millió vásárló adatait szivárogtatták ki
- Az Apple és a Google közösen lép fel az illegális Bluetooth nyomkövetők ellen
- Négy nyilvános sebezhetőséget javított VMware termékeiben a Broadcom
- A Google számos biztonsági funkciót jelentett be



## SÉRÜLÉKENYSÉGEK

- Riasztás Adobe szoftverek sérülékenységeiről
- Riasztás Microsoft termékeket érintő sérülékenységekről



## 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

### Feltörték az Europol (bleepingcomputer.com)

Az Europol, az Európai Unió bűnüldöző szerve megerősítette, hogy az Europol szakértői platform (EPE) portálját feltörték. Egy fenyegető szereplő azt állította, hogy titkos adatokat tartalmazó "For Official Use Only" dokumentumokat lopott el. **Bővebben...**

### A Dell API kihasználásával 49 millió vásárló adatait szivárogtatták ki (bleepingcomputer.com)

A Dell adatszivárgás mögött álló támadó azt mondta, hogy hamis vállalatnak álcázva magát egy partner portál API-ját kihasználva jutott 49 millió vásárló adataihoz. **Bővebben...**

### Az Apple és a Google közösen lép fel az illegális Bluetooth nyomkövetők ellen (thehackernews.com)

Az Apple és a Google hivatalosan bejelentette egy új funkció bevezetését, amely értesíti az iOS és az Android a felhasználókat, ha egy Bluetooth nyomkövető eszközzel titokban, a tudtuk vagy beleegyezésük nélkül megfigyelik őket. **Bővebben...**

### Négy nyilvános sebezhetőséget javított VMware termékeiben a Broadcom (thehackernews.com)

A VMware Workstation és Fusion termékekben több olyan biztonsági hiba került nyilvánosságra, amelyeket a fenyegető szereplők kihasználva bizalmas információkhoz férhetnek hozzá, DoS állapotot idézhetnek elő, és bizonyos körülmények között kódot hajthatnak végre. **Bővebben...**



### A Google számos biztonsági funkciót jelentett be (thehackernews.com) (bleepingcomputer.com)

A Google I/O 2024-en jelentett be számos adatvédelmi és biztonsági funkciót, amelyek segítenek a felhasználók eszközeinek és adatainak védelmében.

A funkciók célja, hogy segítsenek megvédeni az adatokat a lopási kísérlet előtt, alatt és után – közölte a technológiai óriás, hozzátéve, hogy várhatóan a Google Play szolgáltatások frissítésével lesznek elérhetőek az Android 10-es vagy újabb verzióját futtató készülékek számára.

**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 szoftvrek széleskörű elterjedtsége miatt.

A Microsoft 2024. május havi biztonsági csomagjában összesen **61** különböző **biztonsági hibát javított**, köztük **3 nulladik napi (zero-day)** sebezhetőséget is, amelyek közül 2 esetben fennáll az aktív kihasználás lehetősége a sérülékeny rendszeren:

**CVE-2024-30040**

**CVE-2024-30051**

[Bővebben...](#)

## Riasztás 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...](#)



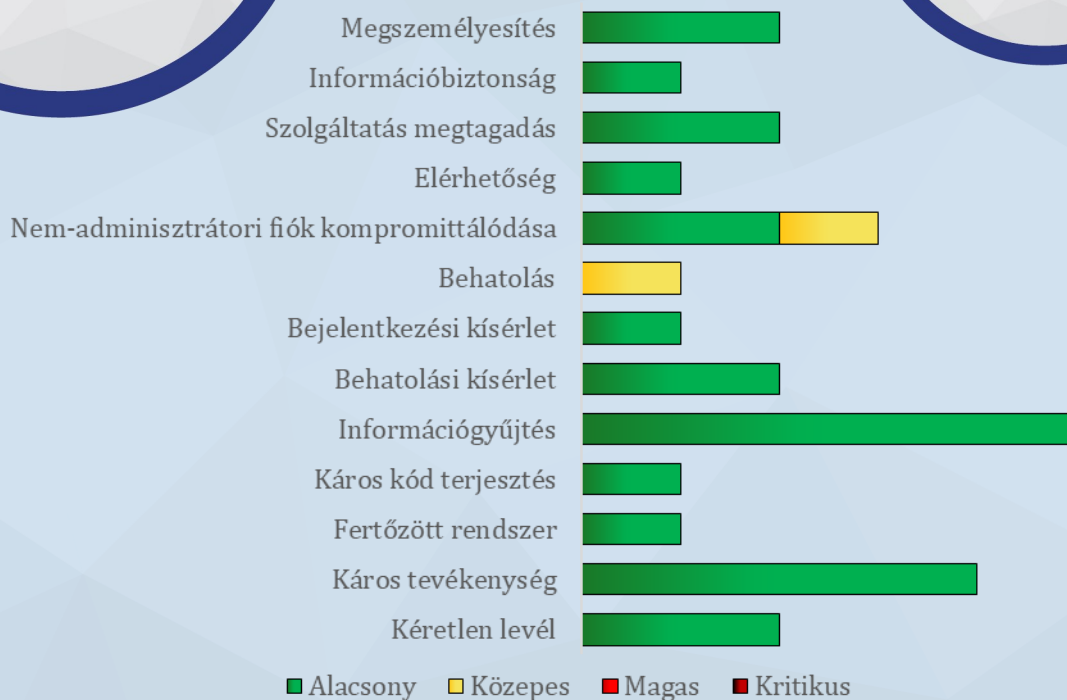
További tájékoztatóért, látogasson el **weboldalunkra!**

# Statisztikai Adatok

2024.05.10.-2024.05.16.

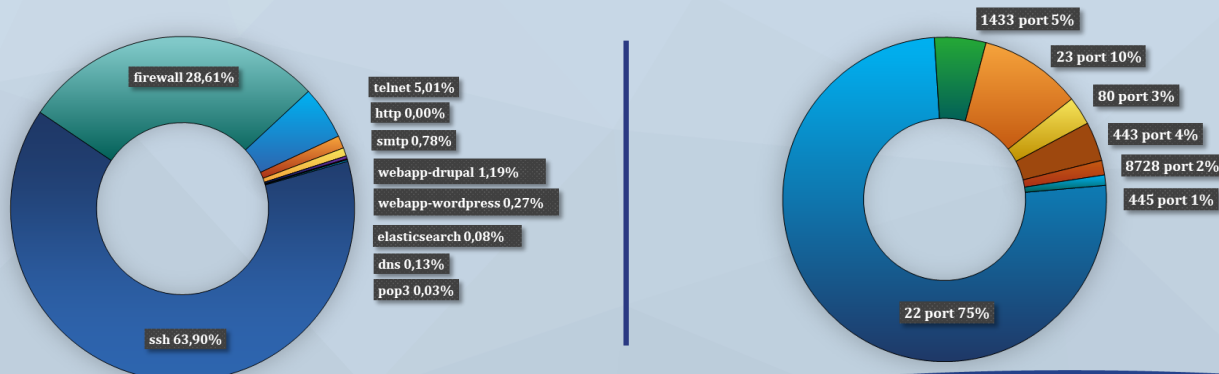
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: közepes



Incidensek eloszlása típus és kockázati besorolás szerint

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



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