NEMZETI KIBERVÉDELMI INTÉZET

# HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2024. 41. hét

## HÍREK

- A Fortinet RCE kritikus hibáját használják ki a támadások során
- Kritikus Zimbra sebezhetőséget használtak ki támadók
- Kritikus sebezhetőségek a DrayTek routereiben
- Az Apple kritikus iOS- és iPadOS frissítéseket ad ki a VoiceOver sebezhetőségének javítására
- Váratlan e-mailek a Google Pay-től: sikeresen „új kártya” került hozzáadásra a Google fiókhoz

## SÉRÜLÉKENYSÉGEK

- Tájékoztatás Adobe szoftverek sérülékenységeiről
- Riasztás Microsoft termékeket érintő sérülékenységekről

## STATISZTIKAI ADATOK

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

## KONTAKT

**edt@nki.gov.hu**

PGP kulcs

FBC3 88A2 E465 BF51
AD58 A2D0 E9DD E078
ABD3 E75D

# NEWS

IT biztonsági

# HÍREK

## A Fortinet RCE kritikus hibáját használják ki a támadások során a

**(bleepingcomputer.com)**

A kiberbűnözők aktívan kihasználják a FortiOS távoli kódfuttatási (RCE) kritikus sebezhetőségét. A CVE-2024-23113 néven nyomon követett hibát az okozza, hogy az fgfmd daemon program egy külsőleg vezérelt formátumstringet fogad el argumentumként. **Bővebben...**

## Kritikus Zimbra sebezhetőséget használtak ki támadók

**(securityweek.com)**

Biztonsági kutatók hívták fel a figyelmet arra, hogy egy kritikus sebezhetőséget használtak ki a kiberbűnözők a Zimbra platformján. A CVE-2024-45519-es azonosítóval ellátott hiba lehetővé teszi az adott támadó számára, hogy hitelesítés nélkül parancsokat futtasson egy sebezhető szerveren. **Bővebben...**

## Kritikus sebezhetőségek a DrayTek routereiben

**(hackread.com)**

A Censys kutatása 14 sebezhetőséget tárt fel a DrayTek Vigor routerekben, amelyeket 2024. október 2-án hoztak nyilvánosságra. A British Telecoms az egyik legsebezhetőbb hoszt, amelyet a vietnami, hollandiai, tajvani és német hosztok követnek. **Bővebben...**

## Az Apple kritikus iOS- és iPadOS frissítéseket ad ki a VoiceOver sebezhetőségének javítására

**(thehackernews.com)**

Az Apple iOS és iPadOS frissítéseket adott ki két biztonsági probléma megoldására, amelyek közül az egyik lehetővé tehette volna, hogy a VoiceOver a felhasználó jelszavát hangosan felolvassa. **Bővebben...**

## Váratlan e-mailek a Google Pay-től: sikeresen „új kártya” került hozzáadásra a Google fiókhoz

**(bleepingcomputer.com)**

A felhasználók váratlan e-maileket kaptak a Google Pay-től, miszerint sikeresen “hozzáadásra került egy új kártya” a Google fiókjukhoz. Az értesítés hatására a felhasználók megijedtek, hogy esetleg a fiókjuk kompromittálódott.
**Bővebben...**


# 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. október havi biztonsági csomagjában összesen **117** különböző **biztonsági hibát javított**, köztük **5 nulladik napi (zero-day)** sebezhetőséget is:

**CVE-2024-43573**

**CVE-2024-43572**

**CVE-2024-6197**

**CVE-2024-20659**

**CVE-2024-43583**

**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...**

További tájékoztatókért, látogasson el **weboldalunkra**!

NEMZETI KIBERVÉDELMI INTÉZET

1996 NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

Fortes fortuna adiuvat

KÖZLÖNY §

# Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója

A NBSZ NKI az érintett szervezetek számára útmutatót ad ki a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló *7/2024. (VI. 24.) MK rendelet* alapján.

Az **EiR** útmutató kézikönyvekre bontva megtalálható az **IT Biztonsági Segédletek** között.

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

**LinkedIn**

**Instagram**

**Facebook**

# Aktuális tartalmak

## A kriptográfia napjainkban

*CTI jelentés*

Jelen dokumentum célja, hogy bemutassa a titkosítási módszereket, a jelenleg leggyakrabban használt algoritmusokat.

A dokumentumból megtudhatjuk, hogy ezek az algoritmusok mennyire biztonságosak, emellett ismerteti a titkosítás felhasználási területeit, valamint a kriptográfia jövőbeni változásait.

**Elolvasom**

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

**LinkedIn**

**Instagram**

**Facebook**

# Aktuális tartalmak

## A letöltések veszélye: hogyan járj túl a rosszindulatú mobilapplikációk eszén – SANS OUCH! – 2024. október

Megjelent a **SANS** és a Nemzetbiztonsági Szakszolgálat **Nemzeti Kibervédelmi Intézet** közös kiadványának **2024. októberi száma**, melyben azzal foglalkozunk, hogyan bizonyosodhatunk meg arról, hogy megbízható, biztonságos mobilapplikációt töltünk le.

**Elolvasom**

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

**LinkedIn**

**Instagram**

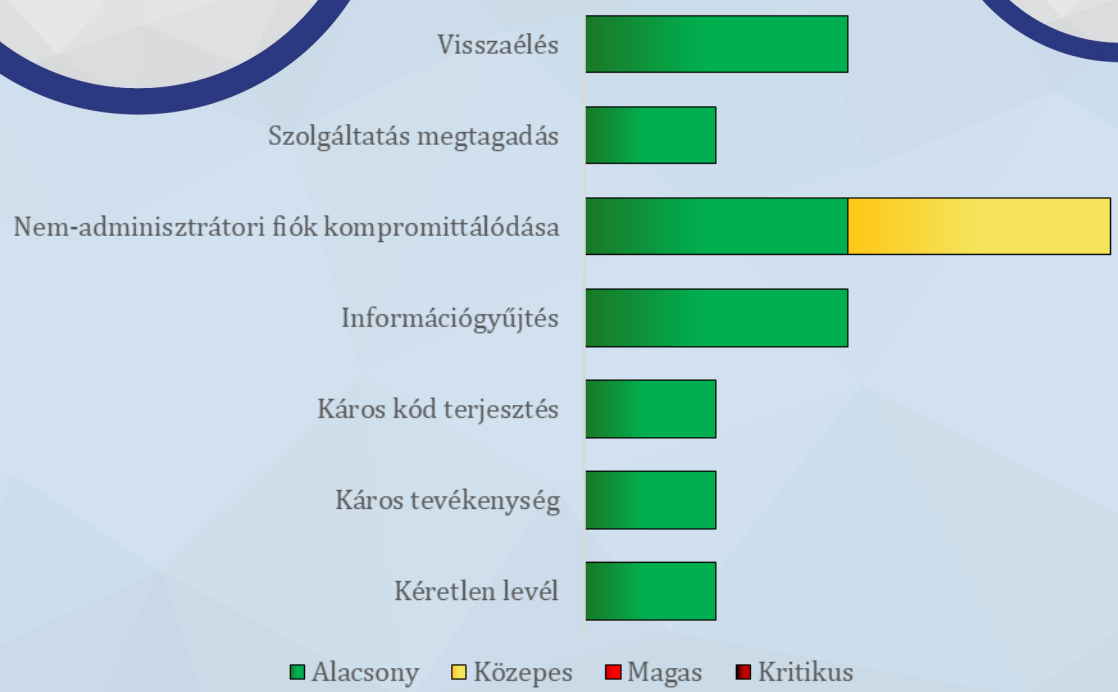
**Facebook**

# Statisztikai Adatok

2024.10.04.-2024.10.10.

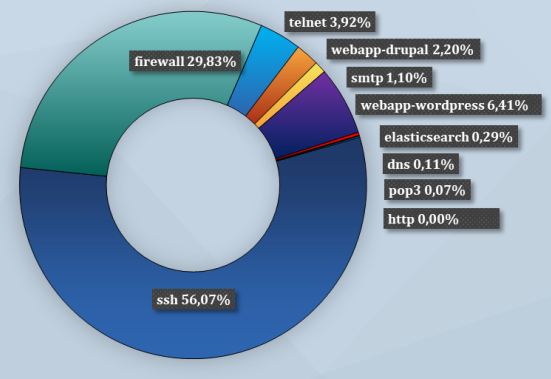
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

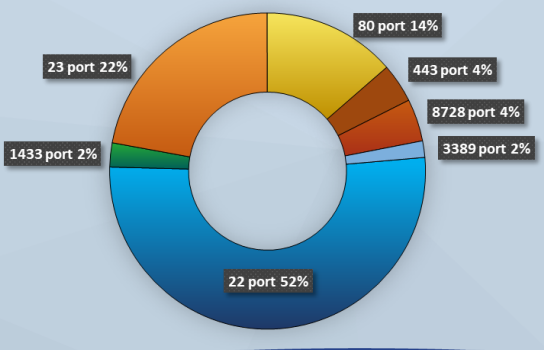
Fenyegetettségi szint: közepes




## Incidensek eloszlása típus és kockázati besorolás szerint

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




További érdekességekért, látogasson el **weboldalunkra**!