NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2024. 8. hét

HÍREK

- A SolarWinds több kritikus sérülékenységet javított
- Sérülékenységet találtak egy 25 éves szabványban
- WordPress sérülékenység aktív kihasználását jelentette a gyártó
- Elkapták a LockBit két tagját, dekódoló érhető el!
- Akár 97000 Microsoft Exchange kiszolgáló is sebezhető lehet

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 SolarWinds több kritikus sérülékenységet javított

(bleepingcomputer.com)

A SolarWinds öt távoli kódfuttatási hibát javított az ARM megoldásában, köztük három kritikus súlyosságú sebezhetőséget, amelyek hitelesítés nélküli kihasználást tesznek lehetővé. Az Access Rights Manager lehetővé teszi a vállalatok számára a hozzáférési jogok kezelését és ellenőrzését az IT infrastruktúrájukban. **Bővebben...**

Sérülékenységet találtak egy 25 éves szabványban

(bleepingcomputer.com)

A CVE-2023-50387 néven nyomon követhető **KeyTrap** a DNSSEC tervezési problémája, és az összes népszerű DNS (Domain Name System) implementációt vagy szolgáltatást érinti. **Bővebben...**

WordPress sérülékenység aktív kihasználását jelentette a gyártó

(bleepingcomputer.com)

A hackerek aktívan kihasználják a Brick Builder Theme-t érintő kritikus RCE hibát, amelynek segítségével rosszindulatú PHP kódot futtathatnak a sebezhető webhelyeken. Február 10-én egy "snicco" nevű kutató felfedezett egy sebezhetőséget, amelyet CVE-2024-25600 néven követnek nyomon, és amely az alapértelmezett konfigurációval telepített Brick Builder Theme-t érinti. **Bővebben...**

Elkapták a LockBit két tagját, dekódoló érhető el

(bleepingcomputer.com)

A bűnüldöző szervek letartóztatták a LockBit zsarolóvírus csoport két újabb tagját. Miután egy nemzetközi művelet során feltörték a kiberbűnöző banda szervereit, lefoglaltak több mint 200 kriptotárcát és létrehoztak egy dekódoló eszközt a titkosított fájlok ingyenes visszaállítására. **Bővebben...**

Akár 97000 Microsoft Exchange kiszolgáló is sebezhető lehet

(bleepingcomputer.com)

A CVE-2024-21410 néven nyomon követett, kritikus súlyosságú jogosultságnövelési hiba, amelyet a hackerek aktívan kihasználnak, lehetővé teszi, hogy hitelesítés nélküli támadók NTLM relay támadásokat hajtsanak végre a sebezhető Microsoft Exchange szervereken, és növeljék jogosultságaikat a rendszerben.

Bővebben...

Aktuális tartalmak

NEMZETI KIBERVÉDELMI INTÉZET

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NBSZ NKI a LinkedInen!

Amennyiben nem szeretne lemaradni az Intézetünket érintő **legfrissebb hírekről**, **szakmai rendezvényeinkről**, továbbá kíváncsi arra, hogy pontosan **mivel is foglalkoznak az NBSZ NKI egyes szakterületei**, akkor érdemes a Linkedinen is velünk tartani, mert az elkövetkezendő posztjainkból ez is kiderül!

Megnézem

Az oldal csak a LinkedInre való bejelentkezés után érhető el.

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

Nemzeti Kibervédelmi Intézet

@nki.gov.hu

Nemzeti Kibervédelmi Intézet

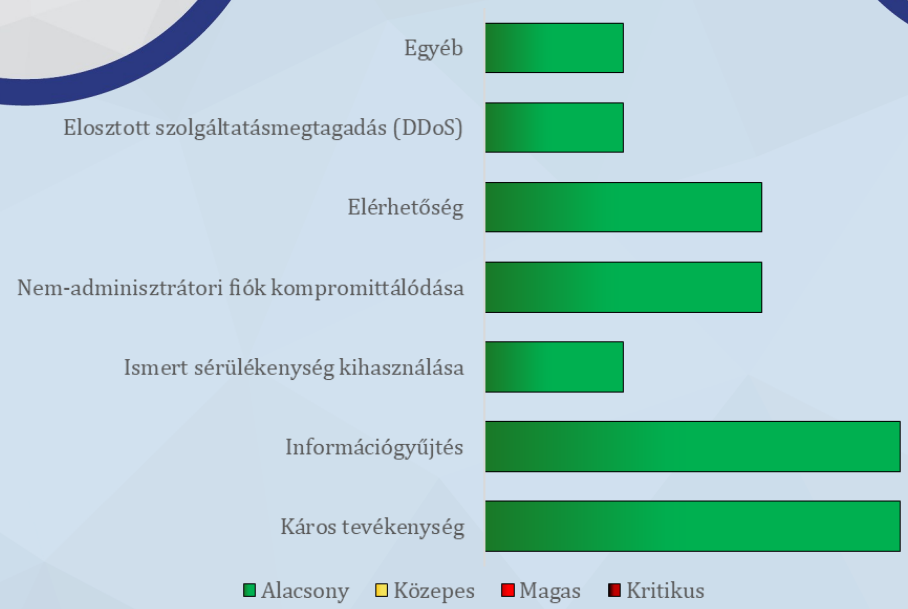
További érdekességekért, látogasson el **Facebook oldalunkra**!

Statisztikai adatok

2024.02.16-2024.02.22.

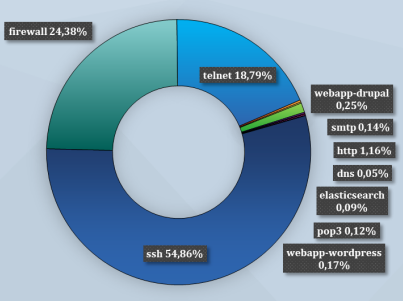
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

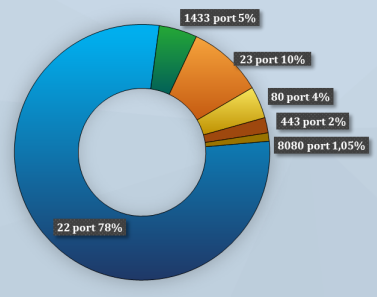
Fenyegetettségi szint: alacsony



Incidensek eloszlása típus és kockázati besorolás szerint

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





További információkért, látogasson el **weboldalunkra**!