NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2024. 50. hét

HÍREK

- PoC exploitot kapott a Mitel MiCollab zero-day sérülékenysége
- Kriptovaluta bányász kártevőt találtak egy Python könyvtárban
- Kritikus Windows sebezhetőség: NTLM-hitelesítési adatok megszerzése vált lehetővé
- Maximális súlyosságú hibát javított az Ivanti
- Ezek voltak a leggyakoribb és a legveszélyesebb sérülékenység típusok idén a MITRE szerint

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

Kriptovaluta bányász kártevőt találtak egy Python könyvtárban

(thehackernews.com)

Egy ellátási lánc támadás során kiderült, hogy az ultralytics nevű népszerű Python mesterséges intelligencia (AI) könyvtár két verzióját kompromittálták, annak érdekében, hogy egy kriptovaluta-bányász programot telepítsenek az áldozatok gépén. **Bővebben...**

Kritikus Windows sebezhetőség: NTLM-hitelesítési adatok megszerzése vált lehetővé

(blog.0patch.com)

Biztonsági kutatok nyilvánosságra hoztak egy frissen felfedezett sebezhetőséget, amely minden Windows szerverre és munkaállomásra szánt verziót érint a Windows 7-től a Windows 11-ig (v24H2) és a Server 2008 R2-től a Server 2022 verzióig bezárólag. **Bővebben...**

Maximális súlyosságú hibát javított az Ivanti

(bleepingcomputer.com)

Az Ivanti figyelmeztetést adott ki a Cloud Services Appliance (CSA) megoldásában található új, maximális súlyosságú hitelesítés megkerülési sebezhetőség miatt. **Bővebben...**

Ezek voltak a leggyakoribb és a legveszélyesebb sérülékenység típusok idén a MITRE szerint

(mitre.org)

Elérhető a legveszélyesebb sérülékenységi kategóriákról (CWE) szóló idei Top 25-ös lista. **Bővebben...**

PoC exploitot kapott a Mitel MiCollab zero-day sérülékenysége

(bleepingcomputer.com)

A kutatók felfedeztek egy olyan zero-day sérülékenységet a Mitel MiCollab kollaborációs platformban, ami lehetővé teszi a támadók számára, hogy hozzáférjenek a szerver fájlrendszerén lévő fájlokhoz.
Bővebben...

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 2024. december havi biztonsági csomagjában összesen **73** különböző **biztonsági hibát javított**, köztük **1 nulladik napi (zero-day)** sebezhetőséget is, amit **a támadók aktívan kihasználnak**:

CVE-2024-49138

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.

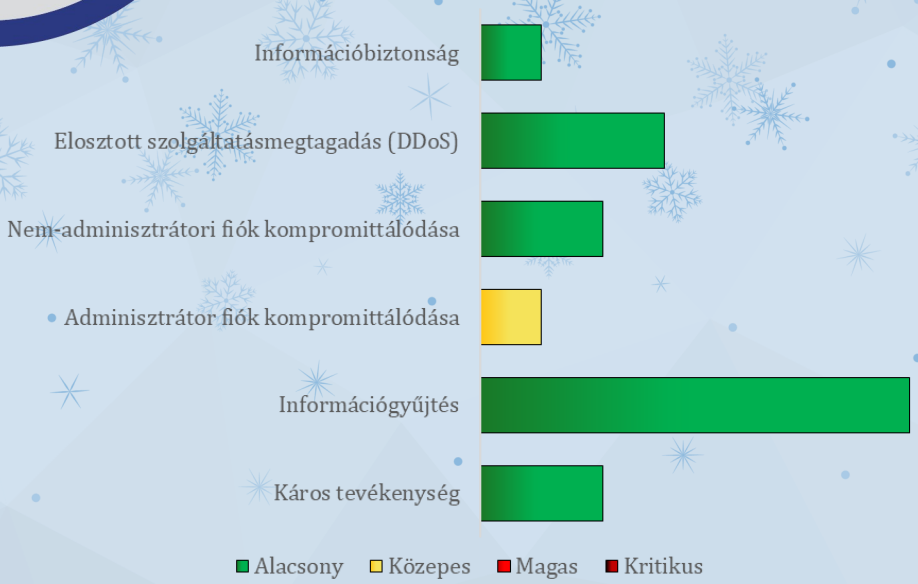
Bővebben...

Statisztikai adatok

2024.12.06.-2024.12.12.

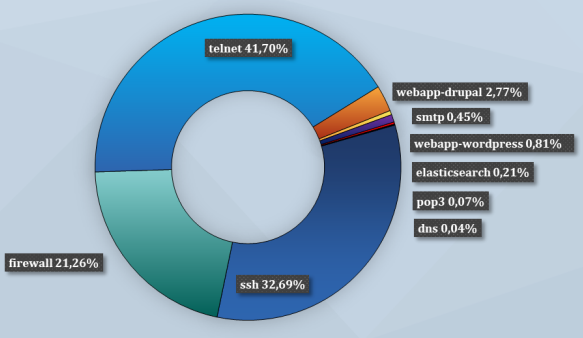
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

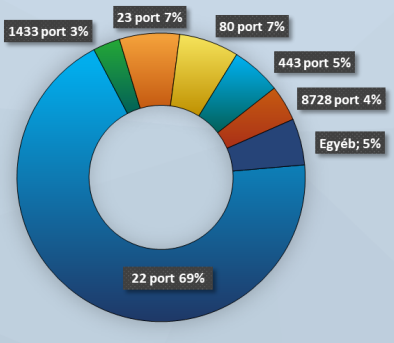
Fenyegetettségi szint: közepes



Incidensek eloszlása típus és kockázati besorolás szerint

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





További információkért, látogasson el **weboldalunkra**!