NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2023.19. hét

HÍREK

- Kibertámadás ért ukrán kormányzati szerveket
- AMD TPM Exploit: Mégsem annyira biztonságos a TPM?
- Kritikus sérülékenység érint egy népszerű Cisco telefon adaptert
- Több kriptopénztárcára veszélyes a ViperSoftX malware, mint valaha
- Újabb 2FA kódokat lopó androidos kártevőt fedeztek fel

Heti IT biztonsági tipp

- Végre megérkezett a végpontok közötti titkosított csevegés a Twiterre

STATISZTIKAI ADATOK

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

TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK,

Riasztás Microsoft termékeket érintő sérülékenységekről – 2023. május

Tájékoztatás Adobe szoftverek sérülékenységeiről – 2023. május

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

NEWS

IT biztonsági
HÍREK

Kibertámadás ért ukrán kormányzati szerveket

(bleepingcomputer.com)

Az ukrán CERT (CERT-UA) állítása szerint orosz hackerek rosszindulatú e-mailekkel vették célba Ukrajna különböző kormányzati szerveit. **Bővebben...**

AMD TPM Exploit: Mégsem annyira biztonságos a TPM?

(tomshardware.com)

A Berlini Műszaki Egyetem biztonsági kutatói által kiadott új dokumentumból kiderül, hogy az AMD firmware alapú Trusted Platform Module (fTPM / TPM) teljesen kompromittálható egy feszültséghiba támadással (voltage fault injection attack), így teljes hozzáférést biztosítva az fTPM-ben tárolt kriptográfiai adatokhoz. **Bővebben...**

Kritikus sérülékenység érint egy népszerű Cisco telefon adaptert

(thehackernews.com)

A Cisco SPA112 2 portos telefonadapter kritikus sérülékenységének (CVE-2023-20126 – CVSS: 9,8 pont) kihasználása tetszőleges távoli kódfuttatást tesz lehetővé a támadók számára. A Cisco közleménye szerint a sérülékenység a firmware frissítési funkció egy hiányos hitelesítési folyamatából ered. **Bővebben...**

Több kriptopénztárcára veszélyes a ViperSoftX malware, mint valaha

(bleepingcomputer.com)

Felfedezték a ViperSoftX információlopást végző malware új verzióját, a Trend Micro kutatói szerint a mostani verzió célpontjai közé a kriptopénztárcák, webböngészők, valamint a jelszókezelők tartoznak. **Bővebben...**

IT biztonsági
TIPP

Újabb 2FA kódokat lopó androidos kártevőt fedeztek fel

(bleepingcomputer.com)

FluHorse névre keresztelték azt a hivatalos alkalmazásokat meghamisító rosszindulatú androidos kártevőt, amelyet a Check Point Research fedezett fel, és amellyel 2022. május óta vesznek célba kelet-ázsiai felhasználókat. A kártevőt e-mailben terjesztik azzal a céllal, hogy ellopja a felhasználók hitelesítő – beleértve a kétfaktoros azonosításhoz szükséges kódjait –, valamint hitelkártya adatait. **Bővebben...**

IT biztonsági Tipp

Az NBSZ NKI weboldalán bővebben olvashatnak a Twitter új végponttól-végpontig terjedő titkosított üzenetküldési funkciójáról.

További hírekért, látogasson el **weboldalunkra**!

Statisztikai adatok

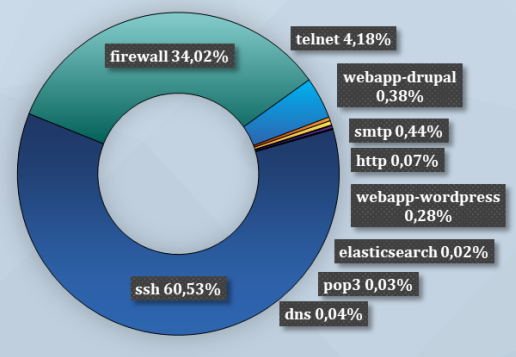
2023.05.05-2023.05.11.

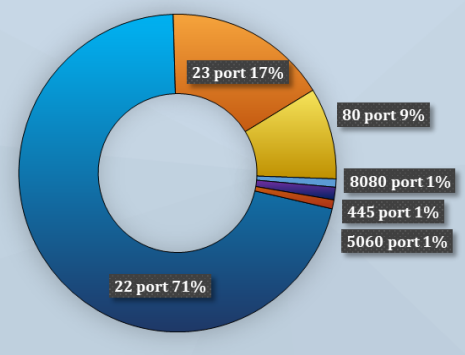
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: alacsony

Incidensek eloszlása típus és kockázati besorolás szerint

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





További információkért, látogasson el **weboldalunkra**!

TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK

Riasztás Microsoft termékeket érintő sérülékenységekről – 2023. május

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 2023. május havi biztonsági csomagjában összesen **38** különböző **biztonsági hibát javított**, köztük **6 kritikus** kockázati besorolású sebezhetőséget, amelyek kihasználása távoli kódfuttatást, szolgáltatásmegtagadást és jogosultság kiterjesztést tesz lehetővé a sérülékeny rendszeren. A javított sérülékenységek között **három nulladik napi (zero-day)** sebezhetőség is található:

- CVE-2023-29336
- CVE-2023-24932
- CVE-2023-29325

Az NBSZ NKI a biztonsági frissítések haladéktalan telepítését javasolja, amelyek elérhetőek az automatikus frissítéssel, valamint manuálisan is letölthetők a gyártói honlapokról.

Tovább olvasom

Tájékoztatás Adobe szoftverek sérülékenységeiről – 2023. május

Az 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 **14 különálló CVE számmal rendelkező sérülékenység** került javításra, *ebből – a gyártói besorolás szerint –* **11 kritikus** és **3 magas** besorolású.

Tovább olvasom