NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2023. 37. hét

HÍREK

- Kritikus sebezhetőség a Google Chrome-ban
- A kínai Redfly kritikus infrastruktúrákat céloz a ShadowPad kampányban
- Egyre több macOS-es káros kód jelenik meg a kiberbűnözői piacon
- Agent Teslát terjeszt egy újabb kifinomult adathalász kampány
- Sérülékenység az Atlas VPN-ben: hozzáférhető a felhasználók valódi IP-címe

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 kínai Redfly kritikus infrastruktúrákat céloz a ShadowPad kampányban
(thehackernews.com)

A Kínával összefüggésbe hozott APT csoportok egyre szélesebb körben célozzák a különböző iparágak szervezeteit. A Symantec jelentése szerint a Redfly fenyegetési aktor mintegy 6 hónapon keresztül használta a ShadowPad elnevezésű rosszindulatú programot egy meg nem nevezett ázsiai ország villamoshálózata ellen. **Bővebben...**

Egyre több macOS-es káros kód jelenik meg a kiberbűnözői piacon
(bleepingcomputer.com)

A Mac-es termékek népszerűsége miatt egyre több káros kód készül erre a platformra, amit a magánfelhasználók mellett a vállalkozásoknak is érdemes tisztában lenni. A Stealer, Pureland, Atomic Stealer és Realst után a legújabb macOS-re összpontosító információ lopó program a MetaStealer. **Bővebben...**

Agent Teslát terjeszt egy újabb kifinomult adathalász kampány
(thehackernews.com)

Egy szofisztikált adathalász kampány Microsoft Word dokumentumot használ az Agent Tesla, az OriginBotnet és az OriginLogger nevű káros kódok terjesztésére és információgyűjtésre. **Bővebben...**

Sérülékenység az Atlas VPN-ben: hozzáférhető a felhasználók valódi IP-címe
(bleepingcomputer.com)

Az Atlas VPN Linux kliensében talált nulladik napi sérülékenységen keresztül kiszivároghatnak a felhasználók valódi IP-címei, például egy weboldal meglátogatásakor. **Bővebben...**

Google

Kritikus sebezhetőség a Google Chrome-ban
(thehackernews.com)

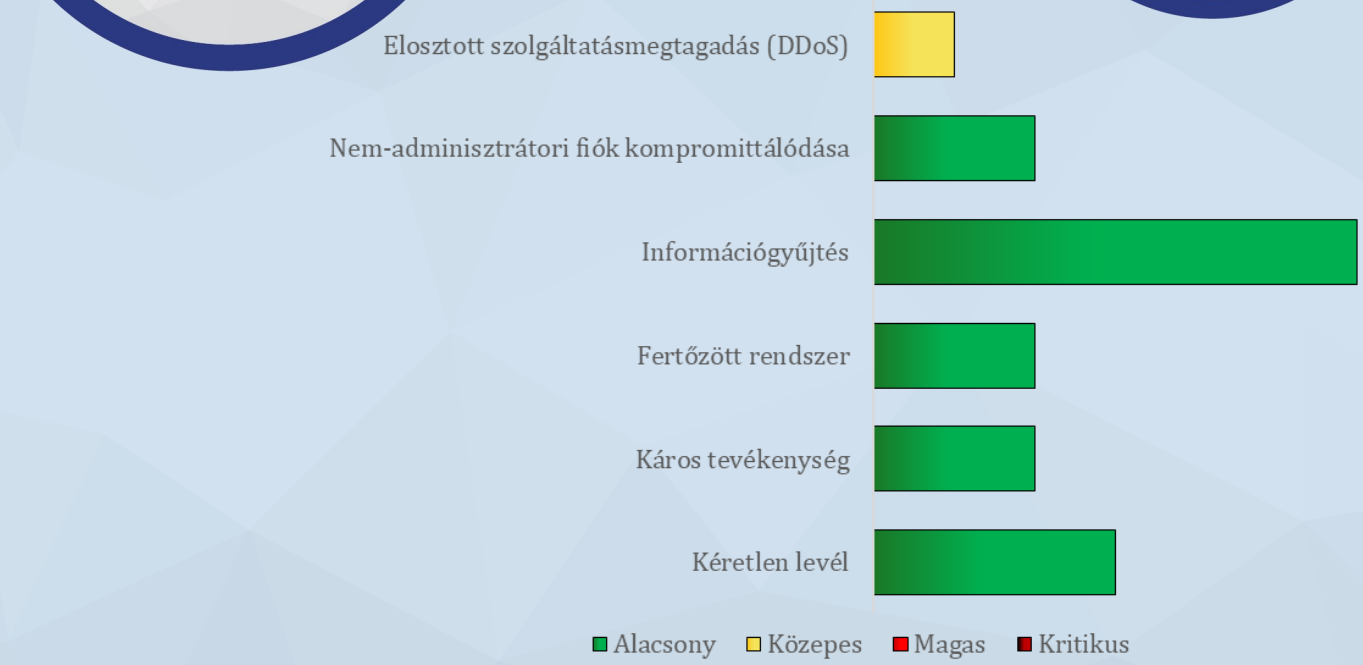
A Google szeptember 11-én soron kívüli biztonsági javításokat adott ki a webböngészőjének kritikus biztonsági hibájára, amelyet a vállalat közlése szerint a kiberbűnözők aktívan kihasználnak.
A CVE-2023-4863 sérülékenység leírása szerint a WebP képformátumban található heap buffer overflow esete, amely tetszőleges kód-futtatást vagy rendszerösszeomlást eredményezhet.**Bővebben...**

Statisztikai adatok

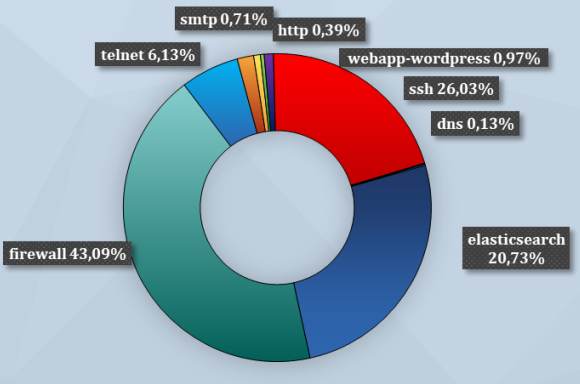
2023.09.08.-2023.09.14.

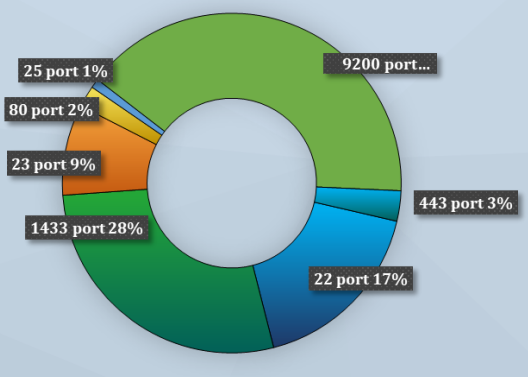
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: közepes



Incidensek eloszlása típus és kockázati besorolás szerint
Az elosztott kormányzati IT-biztonsági csapdarendszerből (Gov1probe) származó adatok:





További információkért, látogasson el **weboldalunkra**!

Aktuális tartalmak

Riasztás és rendkívüli tájékoztató

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) Microsoft szoftvereket érintő **kritikus kockázati besorolású** sérülékenységek kapcsán **riasztást**, az Adobe szoftverfejlesztő cég termékeit érintő sérülékenységekkel kapcsolatban **rendkívüli tájékoztatót** adott ki.

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

A biztonsági figyelmeztetések az alábbi hivatkozásokon keresztül érhetőek el:

Riasztás **Tájékoztató**

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

Nemzeti Kibervédelmi Intézet

@nki.gov.hu

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