NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2024. 26. hét

HÍREK

- Multifunkciós Android malware-el fertőzik a készülékeket
- Mirai alapú botnet használja ki a Zyxel NAS sérülékenységet
- Az Egyesült Államok szankciókkal sújtja a Kaspersky Lab 12 vezetőjét
- A Polyfill.io JavaScript támadása több mint 100 ezer webhelyet érint
- Új js2py sérülékenység, veszélyben többmillió Python felhasználó

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

Multifunkciós Android malware-rel fertőzik a készülékeket
(bleepingcomputer.com)

A “Rafel RAT” nevű nyílt forráskódú Android malware-t több kiberbűnöző is alkalmazza elavult Android eszközök megtámadására. Egyes csoportok célja, hogy egy ransomware lezárja az eszközt és a Telegr mon követelik a váltságdíjat. **Bővebben...**

Az Egyesült Államok szankciókkal sújtja a Kaspersky Lab 12 vezetőjét
(bleepingcomputer.com)

Az Egyesült Államok Pénzügyminisztériumának Külföldi Eszközök Ellenőrzéséért Felelős Hivatala (OFAC) szankciókat vezetett be egy tucatnyi, a Kaspersky Lab-nál vezetői és magas rangú vezetői pozíciót betöltő személy ellen, mert az orosz technológiai szektorban dolgoznak. **Bővebben...**

A Polyfill.io JavaScript támadása több, mint 100 ezer webhelyet érint
(bleepingcomputer.com)

Több mint 110 000 webhelyet érint az itthon is népszerű Polyfill.io szolgáltatás általi supply chain attack, miután egy kínai vállalat megszerezte a domaint, és a scriptet úgy módosította, hogy a felhasználókat rosszindulatú webhelyekre irányítsa át. **Bővebben...**

Új js2py sérülékenység, veszélyben többmillió Python felhasználó
(securityonline.info)

Kritikus sérülékenységet találtak a js2py nevű, széles körben használt Python könyvtárban, amelyet havonta több mint 1 millióan töltenek le. A sérülékenység számtalan webscrapert és alkalmazást tesz távoli kódfuttatás (RCE) támadások könnyű célpontjává. A hibát a CVE-2024-28397 kódon lehet nyomon követni (CVSS érték: 8.8). **Bővebben...**

ZYXEL NETWORKS

Mirai alapú botnet használja ki a Zyxel NAS sérülékenységet
(securityaffairs.com)

A Shadowserver Foundation kutatói arra figyelmeztetnek, hogy egy Mirai alapú botnet elkezdte kihasználni a **CVE-2024-29973 (CVSS érték: 9.8)** néven nyomon követett, nemrégiben nyilvánosságra hozott sebezhetőséget a Zyxel NAS termékek EoL eszközeiben. **Bővebben...**

NEMZETI KIBERVÉDELMI INTÉZET

1996 NEMZETBIZTONSÁGI SZAKSZOLGÁLAT Fortes fortuna adiuvat

ITBN CONFEXPO

Csatlakozzon hozzánk az idei ITBN konferencián!

Az idei rendezvényre minden
NKI ügyfél 30% kedvezményre jogosult
az alábbi kuponkód beírásával:

KEDV-Q84W95

További információkért, illetve a regisztrálófelületért látogasson el az alábbi weboldalra:

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

LinkedIn

Instagram

Facebook

További hírekért, látogasson el **weboldalunkra**!

NEMZETI KIBERVÉDELMI INTÉZET

1996 NEMZETBIZTONSÁGI SZAKSZOLGÁLAT Fortes fortuna adiuvat

KÖZLÖNY §

Megjelent a 7/2024. (VI. 24.) MK rendelet

Megjelent a Miniszterelnöki Kabinetirodát vezető miniszter **7/2024. (VI. 24.) MK rendelete** a **biztonsági osztályba sorolás követelményeiről** valamint az egyes biztonsági osztályok esetében alkalmazandó **konkrét védelmi intézkedésekről**.

További információk és részletes tájékoztatás elérhető a 2024. június 24-i Magyar Közlönyben.

Elolvasom

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

LinkedIn

Instagram

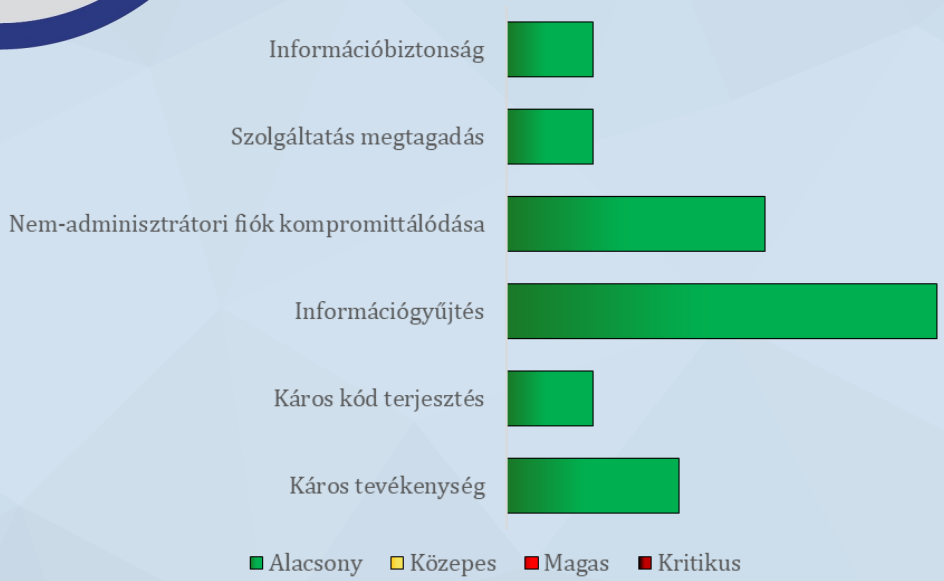
Facebook

Statisztikai Adatok

2024.06.21.-2024.06.27.

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: