NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2024. 34. hét

HÍREK

- Észak-koreai hackerek nulladik napi Windows sérülékenységet kihasználva telepítettek rootkitet
- A kiberbűnözők Jenkins sérülékenységet használnak ki zsarolóvírus-támadásokban
- Kritikus biztonsági rést javítottak a GitHub Enterprise Serverben
- A GiveWP WordPress Plugin sebezhetősége több mint 100 000 webhelyet veszélyeztet
- Figyelem! Új adathalász technikával lopnak banki adatokat az internetes csalók

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

Észak-koreai hackerek nulladik napi Windows sérülékenységet kihasználva telepítettek rootkitet

(bleepingcomputer.com)

A Gen Digital adott hírt arról, hogy észak-koreai hackerek szofisztikált technikával támadásokat hajtottak végre a Windows néhány hete patchelt AFD.sys driverének zero-day sebezhetőségét (CVE-2024-38193) kihasználva. **Bővebben...**

A kiberbűnözők Jenkins sérülékenységet használnak ki zsarolóvírus-támadásokban

(bleepingcomputer.com)

A CISA egy aktívan kihasznált, kritikus Jenkins sérülékenységre figyelmeztet, amely távoli kódfuttatási elérést (RCE) tesz lehetővé a támadók számára. **Bővebben...**

Kritikus biztonsági rést javítottak a GitHub Enterprise Serverben

(thehackernews.com)

A GitHub publikált egy frissítést, amely három biztonsági hibát orvosol az Enterprise Server termékében, köztük egy kritikus hibát is, amelyet kihasználva a támadók adminisztrátori jogosultságokat is szerezhetnek a felületen. **Bővebben...**

A GiveWP WordPress Plugin sebezhetősége több mint 100 000 webhelyet veszélyeztet

(thehackernews.com)

Maximális súlyosságú biztonsági hiba került nyilvánosságra a WordPress GiveWP adománygyűjtési pluginjában, amely által több mint 100 000 weboldal van kitéve RCE (távoli kódfuttatási) támadásoknak. **Bővebben...**

Figyelem! Új adathalász technikával lopnak banki adatokat az internetes csalók

(bleepingcomputer.com)

Kártékony aktorok progresszív webes alkalmazásokat (PWA) kezdtek használni arra, hogy banki alkalmazásokat személyesítsenek meg és hitelesítő adatokat lopjanak el Android és iOS felhasználóktól.

Bővebben...

Statisztikai Adatok

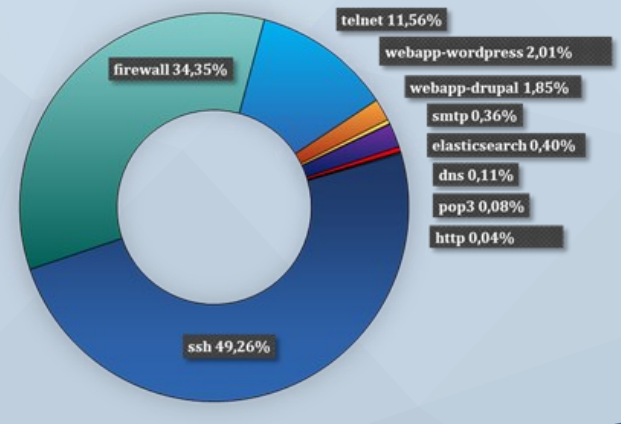
2024.08.16.-2024.08.22.

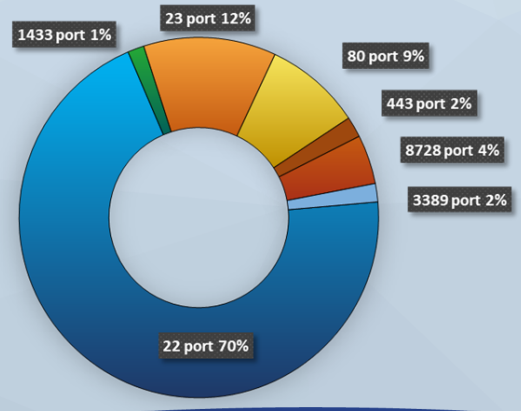
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: alacsony

Incidensek eloszlása típus és kockázati besorolás szerint

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





További érdekességekért, látogasson el **weboldalunkra**!