NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2024. 5. hét

HÍREK

- Több exploitot tettek közzé a Jenkins sebezhetőségre
- 45 ezer nyilvános Jenkins szerver van kitéve RCE támadásoknak
- A Juniper Networks sürgős Junos OS frissítéseket adott ki
- Az Ivanti két új sérülékenységre figyelmeztet, valamint javított két korábbi 0-day-t
- Egy ATM feltörése QR kóddal

SÉRÜLÉKENYSÉGEK

- Riasztás Ivanti termékeket érintő magas kockázati besorolású 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

Több exploitot tettek közzé a Jenkins sebezhetőségre

(bleepingcomputer.com)

Több PoC exploitot hoztak létre a Jenkins kritikus sebezhetőségéének kihasználására, amelyek lehetővé teszik a hitelesítés nélküli támadók számára, hogy tetszőleges fájlokat olvassanak. Néhány kutató arról számolt be, hogy a támadók aktívan kihasználják a hibákat támadásokban. **Bővebben...**

45 ezer nyilvános Jenkins szerver van kitéve RCE támadásoknak

(bleepingcomputer.com)

A kutatók nagyjából 45000 olyan online Jenkins példányt találtak, amelyek sebezhetőek egy kritikus távoli kódfuttatási (RCE) hibával (CVE-2024-23897) szemben, amelyre több nyilvános proof-of-concept (PoC) exploitot publikáltak. **Bővebben...**

Az Ivanti két új sérülékenységre figyelmeztet, valamint javított két két korábbi 0-day-t

(bleepingcomputer.com)

Az Ivanti két újabb, a Connect Secure, Policy Secure és ZTA gateway-eket érintő sebezhetőségre figyelmeztet. Az egyik zero day sérülékenységet már aktívan kihasználják. **Bővebben...**

Egy ATM feltörése QR kóddal

(labs.ioactive.com)

Az IOActive Labs hozzáfért néhány Lamassu Douro ATM-hez. Ez lehetőséget biztosított számukra arra, hogy felmérjék ezeknek az eszközöknek a biztonságát és megpróbálják elérni a teljes ellenőrzést felettük. **Bővebben...**

Juniper Networks sürgős Junos OS frissítéseket adott ki

(thehackernews.com)

A Juniper Networks frissítéseket adott ki az SRX és az EX sorozat magas súlyosságú hibáinak kezelésére, amelyeket kihasználva egy támadó átveheti az irányítást a rendszerek felett.

CVE-2024-21619
(CVSS pontszám: 5,3)

CVE-2024-21620
(CVSS pontszám: 8,8)

Bővebben...

További hírekért, látogasson el **weboldalunkra**!

TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK

Riasztás az Ivanti termékeket érintő magas kockázati besorolású sérülékenységekről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet riasztást ad ki az **Ivanti Connect Secure** és az **Ivanti Policy Secure** szoftvereket érintő **magas kockázati besorolású** sérülékenységek kapcsán, azok súlyossága és aktív kihasználása miatt.

A sérülékenységek az összes támogatott verziót – 9.x és 22.x – érintik. A biztonsági rés lehetővé teszi a támadó számára a jogosultság kiterjesztését rendszeradminisztrátori szintig, illetve korlátozott erőforrásokhoz való hozzáférést.

Javasolt intézkedések

A gyártó a sebezhetőségek felfedezése után azonnal kiadott egy frissítést, mely letölthető a hivatalos frissítési/letöltési portálról az Ivanti Connect Secure (9.1R14.4, 9.1R17.2, 9.1R18.3, 22.4R2.2, 22.5R1.1) és a ZTA (22.6R1.3) verzióihoz.

Bővebben...

CVE-2024-21888

Az Ivanti Connect Secure (9.x, 22.x) és az Ivanti Policy Secure webes komponensének egy jogosultság kiterjesztési sebezhetősége lehetővé teszi a támadó számára, hogy adminisztrátori jogosultságra tegyen szert.

CVE-2024-21893

Az Ivanti Connect Secure (9.x, 22.x) és az Ivanti Policy Secure, illetve az Ivanti Neurons for ZTA SAML komponenseiben lévő szerver oldali kérést meghamisító sérülékenység lehetővé teszi a támadó számára, hogy bizonyos korlátozott erőforrásokhoz hitelesítés nélkül hozzáférjen.

Aktuális tartalmak

NEMZETI KIBERVÉDELMI INTÉZET

KIBERTÁMADÁS! PODCAST

Megnyílt a GPT store: innováció vagy fenyegetés? [aktuális]

Tudtad, hogy nemrég megnyílt a GPT store, azaz a chatGPT azon felülete, ahol a felhasználók egyedileg konfigurált mesterséges intelligenciákat oszthatnak meg egymással?
Ebben az adásban ennek előnyeiről, és ami még fontosabb: veszélyeiről beszélgetünk!

Meghallgatom

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

Nemzeti Kibervédelmi Intézet

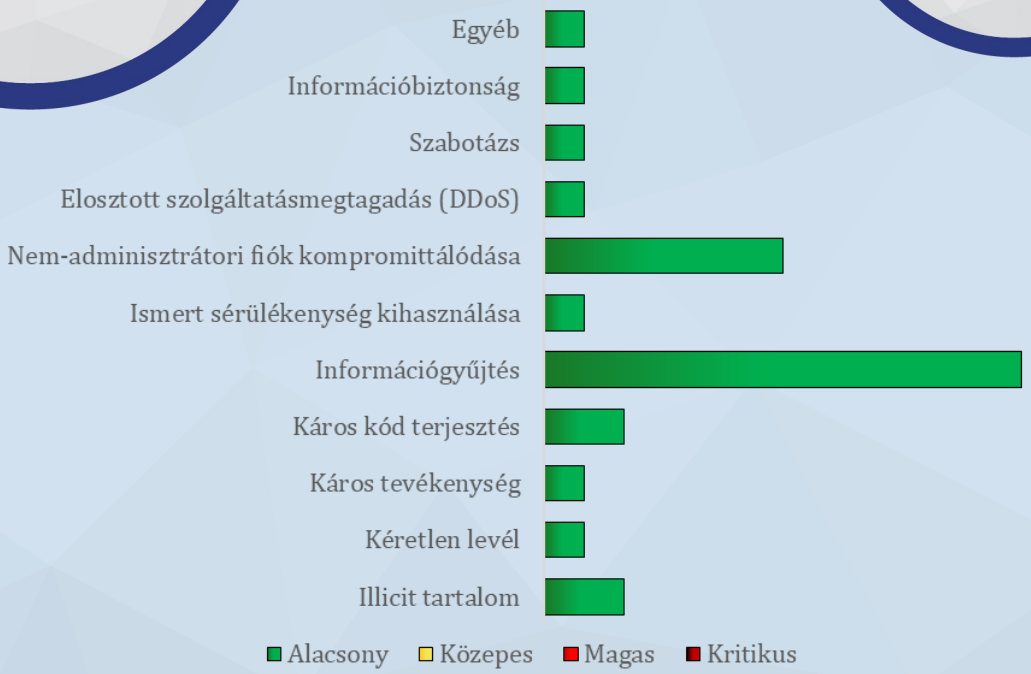
@nki.gov.hu

Statisztikai adatok

2024.01.26..-2024.02.01

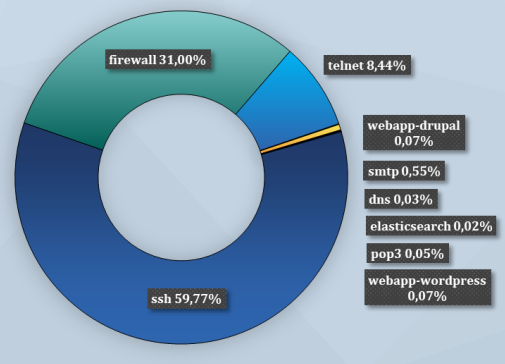
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

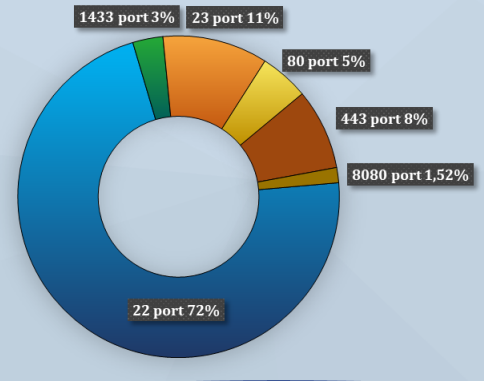
Fenyegetettségi szint: alacsony



Incidensek eloszlása típus és kockázati besorolás szerint

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





További információkért, látogasson el **weboldalunkra**!