NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2024. 3. hét

HÍREK

- Az Ivanti zero day-ek aktív kihasználását jelentették
- Kritikus sérülékenységre figyelmeztet a GitLab
- Kritikus RCE sebezhetőséget fedeztek fel a Juniper SRX tűzfalakban és EX switchekben
- Két új sebezhetőséget Javítottak a POST SMTP Mailer WordPress bővítményben
- A CISA aktívan kihasználtként jelölt meg egy MS SharePoint-ot érintő sérülékenységet

SÉRÜLÉKENYSÉGEK

- Riasztás Az Ivanti VPN termékeket érintő 0. napi kritikus sérülékenységek aktív kihasználásáról

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

Kritikus sérülékenységre figyelmeztet a GitLab

(twitter.com)

A GitLab biztonsági frissítéseket adott két kritikus sebezhetőség kezelésére, köztük egy olyanra, amely a felhasználói beavatkozás nélkül fiókok átvételére használható ki. **Bővebben...**

Kritikus RCE sebezhetőséget fedeztek fel a Juniper SRX tűzfalakban és EX switchekben

(thehackernews.com)

A Juniper Networks frissítéseket adott ki az SRX sorozatú tűzfalak és EX sorozatú switchek kritikus távoli kódfuttatási (RCE) sebezhetőségének javítására. **Bővebben...**

Két új sebezhetőséget Javítottak a POST SMTP Mailer WordPress bővítményben

(bleepingcomputer.com)

Két sebezhetőséget fedeztek fel a POST SMTP Mailer WordPress bővítményben, melyek kihasználásával a támadók teljeskörű irányítást képesek szerezni egy weboldal hitelesítő eljárásai felett. A plugint nagyjából 300 000 weboldal használja. **Bővebben...**

A CISA aktívan kihasználtként jelölt meg egy MS SharePoint-ot érintő sérülékenységet

(thehackernews.com)

Az amerikai Kiberbiztonsági és Infrastruktúrabiztonsági Ügynökség (CISA) egy, a Microsoft SharePoint Server-t érintő kritikus biztonsági sebezhetőséget vett fel a KEV (Known Exploited Vulnerabilities) katalógusába, utalva az aktív kihasználás bizonyítékaira. **Bővebben...**

ivanti

Az Ivanti zero day-ek aktív kihasználását jelentették

(bleepingcomputer.com)

Az Ivanti Connect Secure VPN és Policy Secure hálózati hozzáférés- ellenőrző eszközeit érintő két zero day sebezhetőség tömeges kihasználását jelentették. A Volexity fenyegetéselemző vállalat felfedezte, hogy a CVE-2023-46805 hitelesítési és a CVE-2024-21887 parancsinjekciós sebezhetőséget több csoport használja ki egyes támadásokban január 11-e óta.
Bővebben...

TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK

Kapcsolódó sérülékenységek

Juniper Networks Junos OS SRX sérülékenysége
CVE-2024-21591

WordPress POST SMTP Mailer plugin sérülékenysége
CVE-2023-6875

GitLab CE/EE sérülékenysége
CVE-2023-5356

Cisco Unity Connection sérülékenysége
CVE-2024-20272

Bővebben...

Riasztás az Ivanti VPN termékeket érintő 0. napi kritikus sérülékenységek aktív kihasználásáról

A NBSZ NKI frissített riasztást ad ki, az Ivanti Connect Secure és az Ivanti Policy Secure szoftvereket érintő 0. napi, kritikus kockázati besorolású sérülékenységek kihasználását célzó kibertámadások okán.

Bővebben...

Podcast

Aktuális tartalmak

KIBERTÁMADÁS! PODCAST

NEMZETI KIBERVÉDELMI INTÉZET

Mi az a NIS2? Változó információbiztonsági törvények! [aktuális]

Gondolkoztál már azon, hogy milyen intézkedések biztosítják az egész Unióban egységesen a magas szintű kiberbiztonságot?

Vendégünk **Dávid, a NIS2-es munkacsoport aktív tagja**, aki által betekintést nyerhetünk a NIS2 irányelv hazai implementálásának munkálataiba, illetve megtudhatjuk, hogy mi fog változni, mikor, kiket fog érinteni és hogyan lehet rá felkészülni.

Meghallgatom

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

Nemzeti Kibervédelmi Intézet

@nki.gov.hu

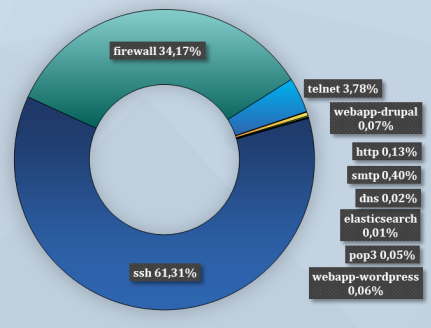
Statisztikai adatok

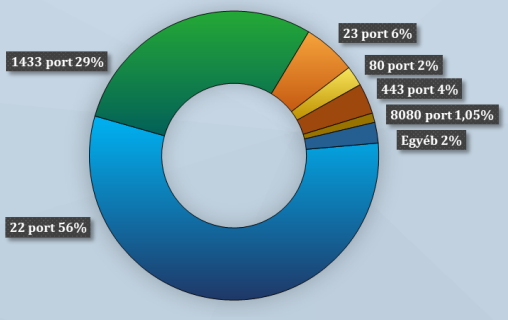
2024.01.12.-2024.01.18

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**!