NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 31. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- TÁJÉKOZTATÁS
- CTI ELEMZÉS

KIBERTÁMADÁS! PODCAST

NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍREK

Hamis Notepad++ csomaggal támadnak ukrán szervezeteket

(bleepingcomputer.com)

Az ukrán CERT-UA újabb kiberbiztonsági kampányt azonosított, amelyben a UAC-0099 nevű APT csoport legitimnek tűnő Notepad++ csomag segítségével próbál megfertőzni célpontokat. A támadók egy PDF dokumentumnak álcázott VBS szkripten keresztül juttatják el a káros ZIP-archívumot, amely a valódi Notepad++ 8.8.3 alkalmazás mellett egy manipulált bővítményt is tartalmaz. **Bővebben...**

Iráni kötődésű támadók PLC-ket céloznak

(cisa.gov)

A CISA az ipari vezérlők, vagyis PLC-k elleni aktív támadási kampányra hívja fel a figyelmet. A CISA szerint a támadási kampány mögött iráni kötődésű támadók állnak, akik internetre kitett PLC-ket céloznak a kritikus infrastruktúrában. **Bővebben...**

Veszélyes PowerShell-parancsok terjednek a Steam fórumain

(bleepingcomputer.com)

A Steam közösségi fórumain terjedő új ClickFix-kampány során a támadók hamis hibaelhárítási útmutatókkal próbálják rávenni a felhasználókat rosszindulatú PowerShell-parancsok futtatására. A csalók frissen létrehozott Steam-fiókokkal arra veszik rá a felhasználókat, hogy rendszergazdai jogosultsággal futtassanak egy PowerShell-parancsot, amely állítólag megoldja a problémát. **Bővebben...**

Több száz Claude-beszélgetés vált kereshetővé az interneten

(bbc.com)

Több száz, az Anthropic Claude nevű mesterséges intelligencia chatbotjával folytatott felhasználói beszélgetés vált nyilvánosan hozzáférhetővé az interneten.
Bővebben...

KindaRails2Shell: új kritikus Rails hiba

(cyberkendra.com)

A Ruby on Rails egy kritikus sebezhetőség miatt sürgősségi frissítéseket adott ki július 29-én, mert a hiba lehetővé teheti, hogy egy nem hitelesített támadó fájlokat olvasson ki a szerverről. A sérülékenységet CVE-2026-66066 azonosítón tartják nyilván, és a KindaRails2Shell becenevet kapta.
Bővebben...

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

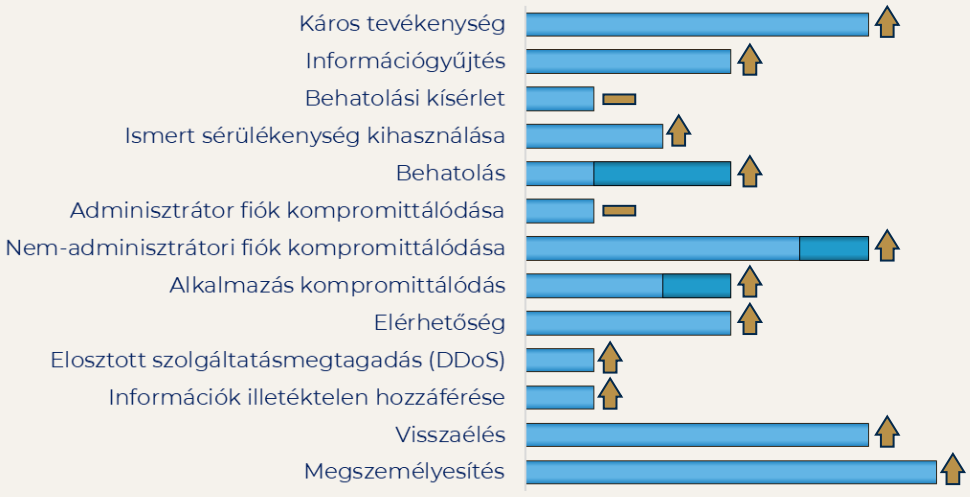
2026. 07. 24. - 2026. 07. 30.

Fenyegetettségi szint:

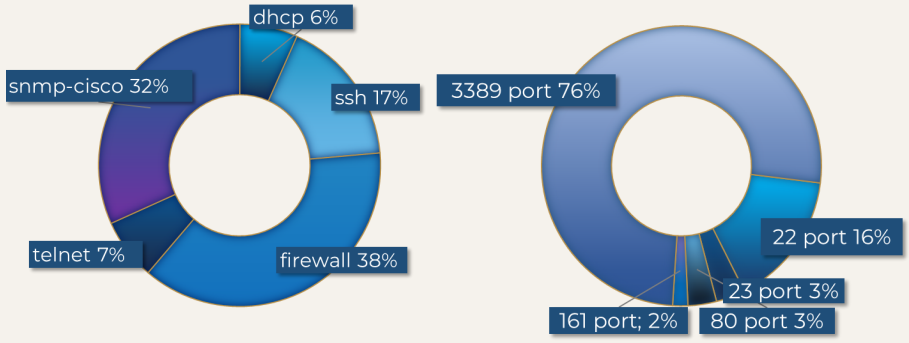
alacsony | közepes | magas | kritikus

Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok

Az adatsorok melletti nyilak az előző héthez viszonyított változásokat mutatják.



Az elosztott kormányzati IT biztonsági csapdarendszerből (GovProbe1) származó adatok



NEMZETI KIBERBIZTONSÁGI INTÉZET

TÁJÉKOZTATÁS

Tájékoztatás az Európai Parlament és a Tanács 2024/2847 rendeletéről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ NKI) **tájékoztatót ad ki** az Európai Parlament és a Tanács által meghatározott, **a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről**.

Az Európai Parlament és a Tanács (EU) 2024/2847 rendeletének (a továbbiakban: CRA) 14. cikk (1) bekezdése az alábbi kötelezettséget írja elő:

A gyártónak – amennyiben ilyen a tudomására jut – a digitális elemeket tartalmazó termékben található bármely **aktívan kihasznált sérülékenységről** egyidejűleg értesítenie kell a **koordinátorként kijelölt Incidenskezelő Központot (CSIRT)** és az **ENISA-t**.

Elolvasom

Sérülékenységek listája

Kövesse folyamatosan frissülő sérülékenység listánkat, hogy naprakész maradhasson a legújabb, és legaktuálisabb fenyegetésekkel kapcsolatban!

NEMZETI KIBERBIZTONSÁGI INTÉZET

CTI ELEMZÉS

Az XZ Utils backdoor elemzése

Ebben a dokumentumban bemutatjuk **a nyílt forráskódú szoftverfejlesztés menetét**, **előnyeit és biztonsági kockázatait** az XZ Utils backdoor elemzésén keresztül. Az elemzés bemutatja egy évekre visszanyúló supply-chain attack **lépéseit és motivációit**, illetve a **sérülékenység felfedezését és elhárítását** is. Kiemelten foglalkozunk azokkal a nyílt forráskódú segédprogramokkal, amelyek elérhetősége természetesnek tűnhetnek, de a **karbantartásukért egy-egy ember vagy egy kisebb csapat felel**, nagyban megnehezítve az **esetleges rosszindulatú kód változások észrevételét és javítását**.

Elolvasom

Érdekesnek találta elemzésünket? Szívesen olvasna hasonló témakörben?

Figyelmébe ajánljuk *„Az IDN homográf támadások”* című elemzésünket!