NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 18. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- CTI JELENTÉS
- RIASZTÁSOK

KIBERTÁMADÁS! PODCAST

NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍREK

Újabb sérülékenységekkel bővült a CISA listája

(thehackernews.com)

A CISA további négy, ezúttal a SimpleHelp, aSamsung MagicINFO 9 Server és a D-Link DIR 823X sorozatú routereket érintő sérülékenységeket vette fel az ismerten kihasznált sebezhetőségeket tartalmazó KEV (Known Exploited Vulnerabilities) katalógusába. **Bővebben...**

Firestarter backdoor mutatja meg, miért nem elég az egyszerű patchelés

(bleepingcomputer.com)

Az amerikai CISA és a brit NCSC olyan, Firestarter néven azonosított egyedi backdoorra figyelmeztetett, amely Cisco Firepower és Secure Firewall eszközökön, ASA vagy FTD szoftverkörnyezetben képes tartós hozzáférést biztosítani a támadónak. A kampányt az UAT-4356 néven követett szereplőhöz kötik, amely korábban az ArcaneDoor műveletek kapcsán vált ismertté. **Bővebben...**

Az USA-ban 2025-ben több mint 2,1 milliárd dollárt veszítettek közösségi médiás csalások miatt

(bleepingcomputer.com)

Az amerikai Federal Trade Commission (FTC) arra hívta fel a figyelmet, hogy 2020 óta jelentősen megnőtt a közösségi médiához köthető csalások száma. 2025-ben az összeg meghaladta a 2.1 milliárd dollárt, azaz a jelenlegi forint árfolyamra átszámítva nagyjából 655,3 milliárd forintot. **Bővebben...**

Adathalász linkeket juttattak a Robinhood legitim e-mailjeibe

(bleepingcomputer.com)

A Robinhood online kereskedelmi platform fióklétrehozási folyamatának egy sérülékenységét kihasználva, a csalók rendszerüzenetnek álcázva küldtek ki adathalász e-maileket. **Bővebben...**

Az ADT adatszivárgás 5,5 millió felhasználót érint

(bleepingcomputer.com)

Az ADT elleni kibertámadás során mintegy 5,5 millió felhasználó személyes adatai kerültek illetéktelen kezekbe a Have I Been Pwned elemzése szerint. A támadás a ShinyHunters zsaroló csoporthoz köthető. **Bővebben...**

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

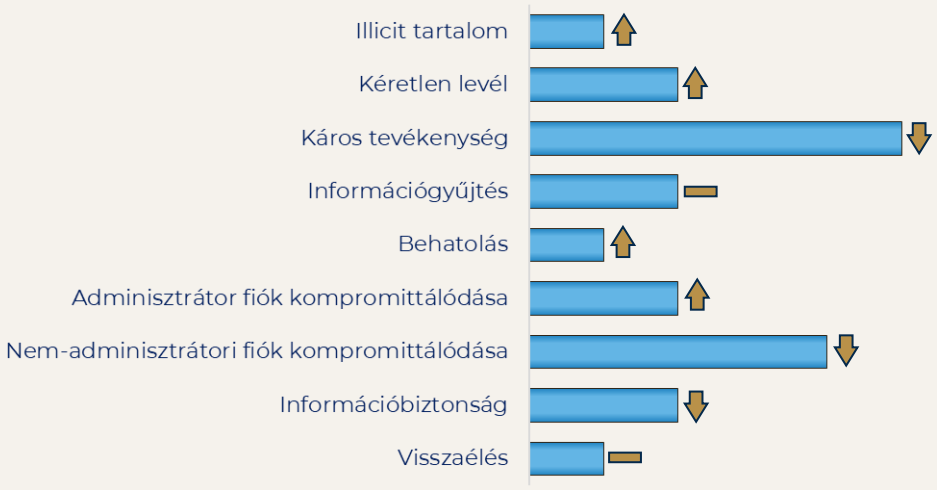
2026. 04. 24. — 2026. 04. 29.

Fenyegetettségi szint:

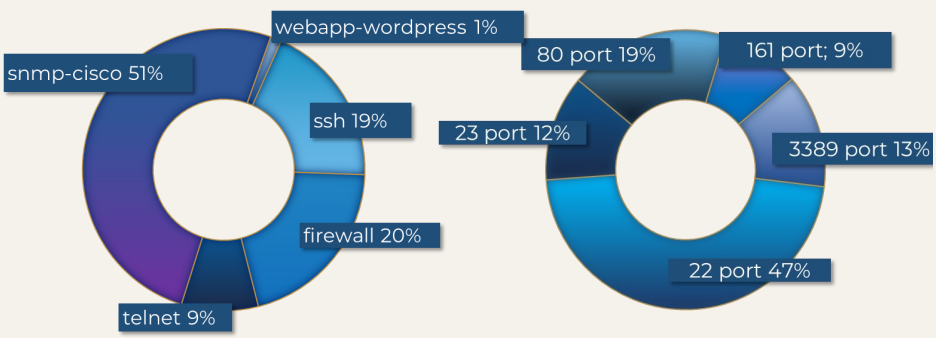
alacsony | közepes | magas | kritikus

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

CTI JELENTÉS

SS7 protokoll sérülékenységei

Jelen dokumentumunkban részletes betekintést nyújtunk az **SS7 protokoll világába**, amely a modern távközlési rendszerek egyik alapvető, ugyanakkor gyakran rejtett működési eleme. Az elemzés bemutatja a technológia **működését, fejlődéstörténetét** és legfontosabb **sajátosságait**, miközben feltárja az ebből eredő **biztonsági kockázatokat**. Kiemelten foglalkozunk az olyan visszaélési lehetőségekkel, mint a **kommunikáció eltérítése**, a **helyadatok lekérdezése** és a **hálózati szintű támadások**, amelyeket valós példákon keresztül is szemléltetünk.

Elolvasom

Érdekesnek találta elemzésünket? Szívesen olvasna hasonló témakörben?

Figyelmébe ajánljuk *„A SIEM rendszerek működése”* című jelentésünket!

RIASZTÁS

Riasztás
a Linux rendszereket érintő Copy Fail sérülékenységről

A Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet
riasztást ad ki a Copy Fail néven ismert, Linux rendszereket érintő, magas kockázatú kernel sebezhetőségről.

A **CVE-2026-31431** és **EUVD-2026-24639** azonosítón nyomon követett hiba a Linux kernel kriptográfiai alrendszeréhez kapcsolódik.
A sérülékenység CVSS v3.1 szerinti pontszáma 7,8, besorolása magas.

Elolvasom

További érdekességekért és IT biztonsággal kapcsolatos tartalmakért látogasson el LinkedIn oldalunkra!