CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

APRÍL 2026

TLP: CLEAR

Kybernetickým priestorom v apríli 2026 rezonovalo hneď niekoľko kľúčových udalostí a útokov. Doplňujúce informácie môžete nájsť v časti Významné udalosti vo svete.

1 Skupina TeamPCP kompromituje softvérové balíky a produkty

Skupina TeamPCP vedie kampaň zameranú na kompromitáciu softvérového dodávateľského reťazca cez platformy ako PyPI, GitHub či Docker Hub. Útočníci infikujú populárne nástroje a knižnice škodlivým kódom, čím zneužívajú dôveru používateľov v legitímny softvér a obchádzajú bezpečnostné mechanizmy.

2 Spojené kráľovstvo vyšetruje Telegram pre podozrenia zo šírenia CSAM obsahu

Britský regulátor Ofcom začal vyšetrovanie platformy Telegram a dvoch tzv. teen chat webov (Teen Chat a Chat Avenue) po tom, čo dostal od kanadskej organizácie na ochranu detí dôkazy naznačujúce šírenie materiálov so sexuálnym zneužívaním detí (CSAM) a riešil riziká tzv. groomingových aktivít.

3 Útok na dodávateľský reťazec cez npm knižnicu Axios

V období od 31. marca do 7. apríla 2026 bol zaznamenaný sofistikovaný útok na dodávateľský reťazec zameraný na populárny npm balík Axios.

4 Phishingová kampaň imituje webové formuláre VšZP

Internetom sa opakovane šíri phishingová kampaň zameraná na klientov VšZP (Všeobecná zdravotná poisťovňa), ktorá imituje webové formuláre VšZP.

5 FBI narušila kampaň FrostArmada ruskej APT28 zameranú na získavanie prístupov do Microsoft 365

V rámci medzinárodnej operácie FBI spolu s partnermi prerušili kampane FrostArmada, ktoré viedla skupina APT28 cez desaťtisíce SOHO routerov značiek ako MikroTik a TP Link.

6 Modul Quick Page/Post Redirect obsahoval 5 rokov skrytý backdoor umožňujúci injektovanie kódu a SEO podvody

Výskumník odhalil skryté zadné vrátka v module Quick Page/Post Redirect pre WordPress, ktorý útočníkom umožňoval na základe špeciálnej požiadavky injektovať a spúšťať ľubovoľný PHP kód na serveri.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci apríl riešil typicky najmä phishingové kampane zasahujúce jeho konštituenciu. Vyskytli sa tiež prípady kompromitovaných e-mailových účtov zamestnancov verejných inštitúcií, z ktorých útočníci rozposielali phishingové e-maily na ďalšie organizácie v konštituencii CSIRT.SK.

V apríli riešil CSIRT.SK kampaň phishingových e-mailov, ktoré prijala organizácia v jeho konštituencii. Jej bezpečnostné riešenie zaznamenalo problematický obsah. Organizácia preverila či došlo k interakcii s ním. Jednotka CSIRT.SK obsah analyzovala a vykonala kroky pre zneprístupnenie škodlivej webovej domény, na ktorú odkazoval. V súvislosti s kampaňou upozornil partner na možnú kompromitáciu oficiálneho e-mailového účtu obce na doméne centrum.sk. Jednotka kontaktovala zastupiteľstvo obce, ktoré prijalo odporúčané opatrenia.

V apríli prebiehala tiež phishingová kampaň šíriaca škodlivý kód Agent Tesla, ktorý má funkcionality RAT (remote access trojan). Slúži teda na vytvorenie zadných vrátok do infikovaného systému a prevzatie tichej kontroly nad ním. Nahlásené phishingové e-maily jednotka analyzovala a získané indikátory kompromitácie využila v rámci služby zdieľania informácií o aktuálnych hrozbách Afrodita.

Jednotka CSIRT.SK prijala od partnera hlásenie podozrivej aktivity zo slovenskej IP adresy na subjekt v konštituencii CSIRT.SK. Išlo o útok typu 'Command Injection'. Podozrivá IP adresa bola v sieti Govnet zablokovaná. CSIRT.SK vykonala analýzu a identifikovali, že sa jednalo o neúspešné zneužitie nahlasovaných CI dopytov a nadviazanie komunikácie s C2 serverom na ruskej IP adrese. Poskytovateľovi internetového pripojenia, ktorému bola podozrivá IP adresa pridelená, boli poskytnuté informácie z analýzy a odporúčania pre postup v prípade opätovnej detekcie podozrivej aktivity.

VJ CSIRT sa v apríli obrátil na partnera so žiadosťou o súčinnosť v súvislosti s informáciou o ransomvérovom útoku na súkromnú spoločnosť, ktorá je dodávateľom pre viacero organizácií verejnej správy. Cieľom bolo posúdiť, či predmetný kybernetický útok mohol ohroziť tieto organizácie prostredníctvom ich dodávateľského reťazca.

V apríli sa odohral bezpečnostný incident v informačnom systéme EduPage, ktorý používa väčšina škôl v SR. Informácie o incidente zverejnili aj niektoré médiá (napríklad tu a tu). Podľa dostupných informácií došlo ku kompromitácii používateľských účtov zamestnancov viacerých škôl. VJ CSIRT na základe žiadosti o spoluprácu preverila situáciu spolu s partnermi. Analýzou získaných informácií sa ukázalo, že došlo k zneužitiu hesiel, ktoré unikli nie v dôsledku napadnutia EduPage, ale mimo jeho prostredia. Spoločnosť, ktorá službu prevádzkuje, spolupracovala s bezpečnostnou firmou, ktorá monitorovala webové stránky pre prípad, že by sa uniknuté heslá niekto pokúšal predávať alebo šíriť.

Apríl priniesol aj zaujímavý kybernetický bezpečnostný incident spojený s kompromitáciou webových stránok organizácie verejnej správy. Útočník umiestnil na webe organizácie nežiaduci obsah, ktorý dokázal obnoviť po jeho odstránení aj po vykonaní hardeningu webového servera a zabezpečení zrejmých vektorov prieniku. V tejto súvislosti požiadala organizácia tím CSIRT.SK o vykonanie tzv. „code review“, teda kontroly zdrojového kódu webstránky, s cieľom odhaliť ukryté zadné vrátka útočníka. Tím CSIRT.SK započal tiež forenznú analýzu webového servera a dodaných dát. Prvé výsledky ukázali napríklad infekciu viacerými vzorkami škodlivých súborov php, vydávaných za legitímne aplikácie.

V rámci svojej proaktívnej činnosti jednotka CSIRT.SK vykonáva pravidelné skenovanie a overovanie zraniteľností v službách a zariadeniach IT infraštruktúr organizácií vo svojej konštituencii, ktoré sú vystavené do internetu. Využíva k tomu platformu Achilles, ktorú sama vyvíja a prevádzkuje. Systém Achilles slúži tiež na monitoring dostupnosti webových domén, ktorú monitoruje modul Domino.

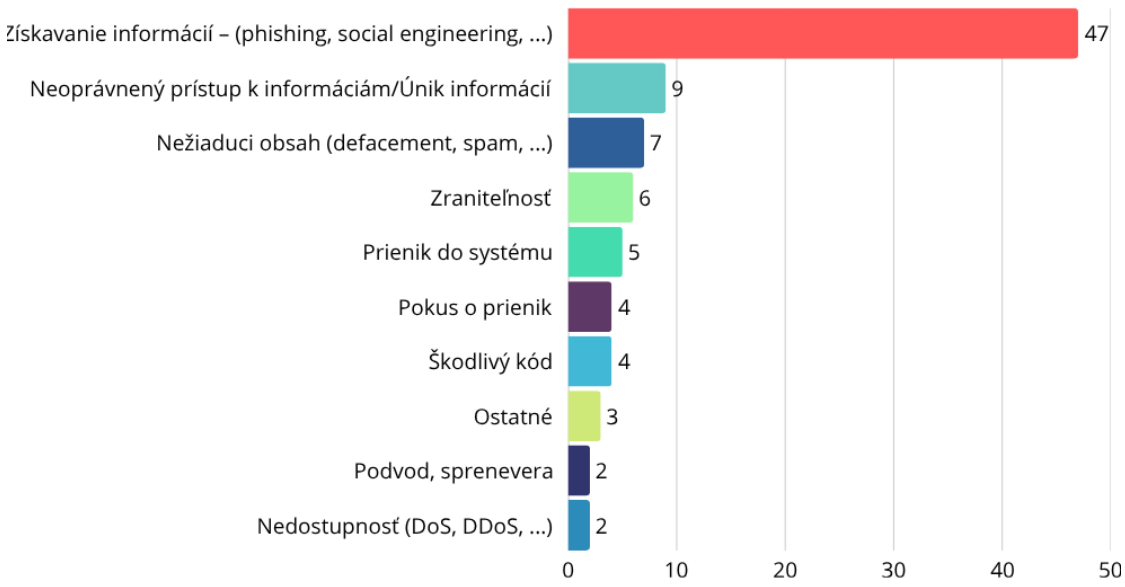
V rámci služby Ares boli vykonané penetračné testy jednej webovej aplikácie a infraštruktúrnych prvkov jednej organizácie. V rámci služby Afrodita prebiehal pravidelný monitoring hrozieb v kybernetickom priestore a zdieľanie indikátorov kompromitácie zo známych kampaní na ochranu vládnej siete Govnet.

V apríli CSIRT.SK plošne varoval svoju konštituenciu ohľadom kampane severokórejskej skupiny UNC1069, ktorá kompromitovala populárny npm balík Axios pre JavaScript a zverejnila upravené verzie so škodlivou závislosťou obsahujúcou malvér. Viac informácií uverejnil na svojej webovej stránke.

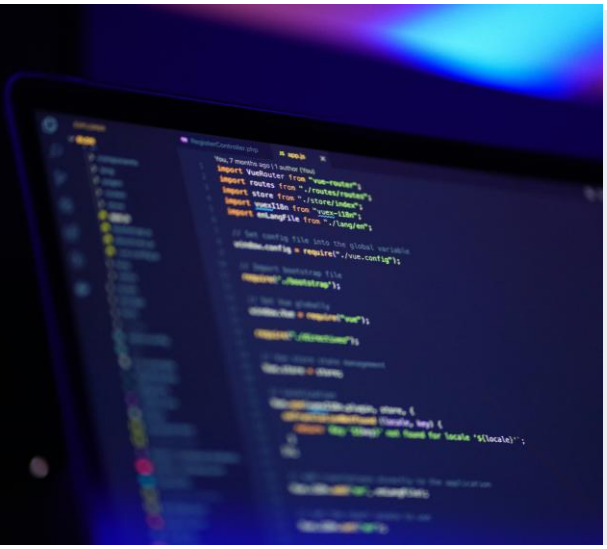
CSIRT.SK v rámci preventívnych činností organizuje aj vzdelávanie v oblasti kybernetickej bezpečnosti pre zamestnancov organizácií verejnej a štátnej správy, ako aj pre študentov stredných škôl. V apríli jednotka prezentovala rôzne témy z oblasti kybernetickej bezpečnosti pre riaditeľov škôlok a základných škôl bratislavskej mestskej časti Petržalka. Prednášala aj študentom Strednej odbornej školy stavebnej v Nitre, Strednej zdravotníckej školy v Dunajskej Strede, Strednej priemyselnej školy strojníckej a SPŠ elektrotechnickej v Košiciach, Strednej odbornej školy dopravy a služieb v Nových Zámkoch, Strednej odbornej školy ekonomickej v Spišskej Novej Vsi a Gymnázia a SOŠ obchodu a služieb v Sobranciach. Pre učiteľov prednášala na Hotelovej akadémii Mikovíniho 1 v Bratislave.

Členovia tímu CSIRT.SK prednášali aj na konferencii OpenCamp 2026, ktorú organizovala Fakulta informatiky a informačných technológií STU. Predstavili na nej nové funkcionality v platforme Achilles určenej pre preventívnu kybernetickú bezpečnosť, najmä odhaľovanie a včasné nahlasovanie zraniteľností organizácií, ktoré túto službu využívajú. Na FIIT STU sa v apríli tím CSIRT.SK zúčastnil aj 21. ročníka súťažnej konferencia Junior Internet 2026, kde zastával úlohu člena odbornej hodnotiacej komisie, a tiež prednášal o etickom hackingu.

VJ CSIRT poskytuje tiež školenia a cvičenia pre svoju konštituenciu v rámci výcvikového a školiaceho strediska Kyberaréna.



VÝZNAMNÉ UDALOSTI VO SVETE

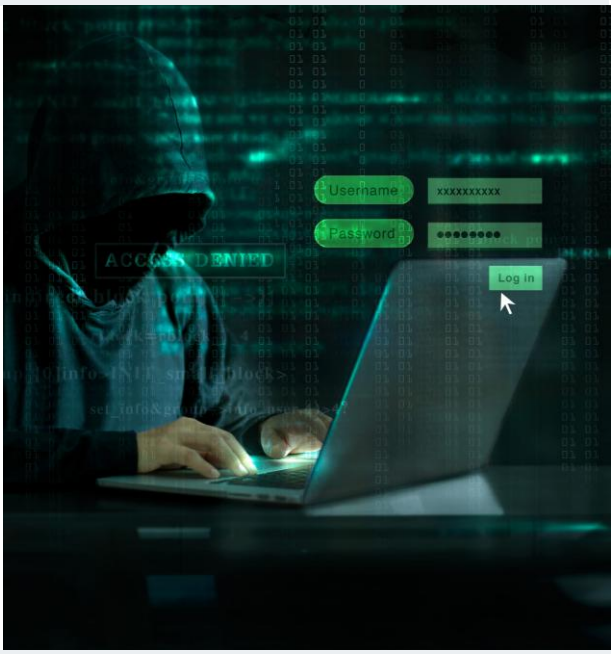


Spoločnosť Anthropic omylom zverejnila zdrojový kód Claude Code na NPM

Spoločnosť Anthropic omylom zverejnila zdrojový kód nástroja Claude Code cez npm balík, keď doň zahrnula súbor s mapou zdrojového kódu určený pre ladenie (angl. debugging), ktorý umožnil verejnosti spätne rekonštruovať veľkú časť interného kódu vrátane architektúry, funkcií a niektorých ešte nevydaných funkcionalít. Incident vznikol chybou pri publikovaní, neodhalil používateľské dáta ani kľúče, no poskytol konkurencii aj bezpečnostným výskumníkom detailný pohľad na fungovanie nástroja a upozornil na slabiny v interných procesoch firmy.

Útok na dodávateľský reťazec cez NPM knižnicu Axios

VJ CSIRT upozornila, že v období od 31. marca do 7. apríla 2026 bol zaznamenaný sofistikovaný útok na dodávateľský reťazec zameraný na populárny npm balík Axios. Útok je pripisovaný severokórejskej skupine UNC1069, ktorá kompromitovala účet správcu balíka a publikovala infikované verzie knižnice. Útočníci použili verzie Axios 1.14.0 a 0.30.3, v ktorých pridali škodlivú závislosť plain-crypto-js do súboru package.json. Falošná závislosť po inštalácii automaticky nasadzovala malvér typu Remote Access Trojan (RAT), ktorý umožňoval útočníkom vzdialený prístup k napadnutým systémom a exfiltráciu citlivých údajov. Napriek krátkemu trvaniu incidentu predstavuje tento útok vysoké riziko vzhľadom na masové využitie knižnice Axios.



FBI narušila kampaň ruskej APT28 zameranú na získavanie prístupu do Microsoft 365

V rámci medzinárodnej operácie FBI spolu s partnermi prerušila kampaň FrostArmada, ktoré viedla skupina APT28 cez desaťtisíce SOHO routerov značiek MikroTik a TP-Link. Menila ich DNS nastavenia, aby presmerovala komunikáciu a získavala prihlasovacie údaje a OAuth tokeny pre účty Microsoft 365. Útoky umožnili odpočúvať DNS komunikáciu a ukradnúť prihlasovacie údaje približne 18 000 zariadení v 120 krajinách. FBI a U.S. Department of Justice sprístupnili detekčné IoC (indikátory kompromitácie) a odporúčania na ochranu sietí a zariadení. Organizácie musia dôsledne zabezpečiť SOHO routery, sledovať DNS nastavenia, zavádzať viacfaktorovú autentifikáciu a pravidelne kontrolovať IoC, aby minimalizovali riziko krádeže prihlasovacích údajov a kompromitácie služieb ako Microsoft 365. **Na danú aktivitu upozornila aj VJ CSIRT, ktorá identifikovala súvisiacu hrozbu a vydala varovanie v súlade s aktuálnymi bezpečnostnými informáciami.**

VÝZNAMNÉ UDALOSTI VO SVETE

CERT UA varuje pred masívnou phishingovou kampaňou s malvérom AGEWHEEZE

CERT UA upozornil, že skupina útočníkov pod označením UAC-0255 rozoslala približne 1 milión phishingových e-mailov tak, že sa vydávala za ukrajinskú bezpečnostnú agentúru CERT UA. Cieľom bolo presvedčiť obete, aby stiahli archív vo formáte ZIP nazvaný „CERT_UA_protection_tool.zip“ s heslom, ktorý následne inštaloval malvér pre vzdialený prístup AGEWHEEZE. Kampaň cielila na štátne organizácie, nemocnice, bezpečnostné firmy, školy, finančné inštitúcie a softvérové spoločnosti.

Spear-phishingová kampaň ruskej APT28 cielená na Ukrajinu a NATO šíri nový malvér PRISMEX

Útočníci skupiny APT28 vedú spear-phishingovú kampaň proti Ukrajine a partnerom NATO, v ktorej doručujú malvér PRISMEX, ktorý kombinuje pokročilú steganografiu, COM hijacking a zneužitie legitímnych cloudových služieb pre C2 infraštruktúru. Aktivita je pozorovaná aspoň od septembra 2025 a ciele zahŕňajú centrálne orgány štátov, obranné a logistické služby v Ukrajine, Poľsku, Rumunsku, Slovinsku, Turecku, Slovensku a Česku. Útočníci rýchlo zneužívajú odhalené zraniteľnosti ako CVE-2026-21509 a CVE-2026-21513, používajú komponenty PrismexSheet, PrismexDrop a PrismexLoader na načítanie škodlivého obsahu skrytého v obrázkoch do pamäte. Nasadzujú aj malvér Covenant Grunt pre pevné C2. Výskumy dokumentujú popri špionáži aj potenciál na sabotáž cez spúšťanie deštruktívnych príkazov.

Výskumníci z Citizen Lab zdokumentovali spravodajskú platformu Webloc využívanú bezpečnostnými a spravodajskými zložkami v USA, Maďarsku a El Salvadore

Výskumníci zo spoločnosti Citizen Lab odhalili, že viacero štátnych bezpečnostných a policajných orgánov používalo systém Webloc od firmy Cobwebs Technologies (neskôr Penlink) na rozsiahle sledovanie pohybu stoviek miliónov mobilných zariadení po celom svete. Tento nástroj využíva údaje z reklamných technológií, mobilných aplikácií a IP adresy na vytváranie detailných profilov, určovanie polohy a pohybu ľudí, často aj spätne za pomerne dlhé obdobie. Podľa zistení ho mali využívať napríklad americké imigračné a policajné zložky, ale aj orgány v iných krajinách, čo vyvoláva obavy z masového sledovania bez dostatočnej právnej kontroly a zásahov do súkromia používateľov.

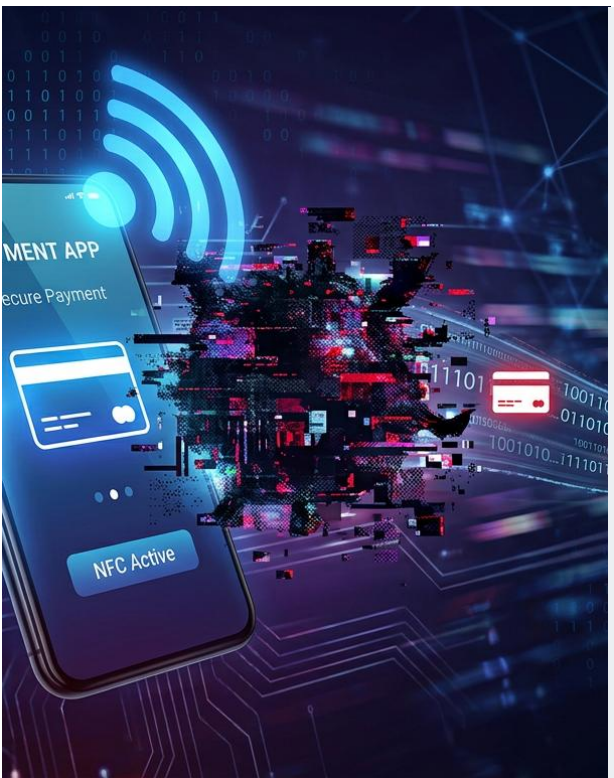
VÝZNAMNÉ UDALOSTI VO SVETE

Google zablokoval 8,3 miliardy škodlivých reklám za rok 2025

Spoločnosť Google oznámila, že v roku 2025 zablokovala alebo odstránila približne 8,3 miliardy reklám, ktoré porušovali jej pravidlá. Zároveň pozastavila takmer 25 miliónov reklamných účtov, pričom väčšinu škodlivých reklám zachytila automatizovane ešte pred ich zobrazením používateľom. Spoločnosť tento pokles podvodných reklám pripisuje najmä nasadeniu AI systémov (Gemini), ktoré lepšie rozpoznávajú podvodné kampane, spam a malvertising. Upozorňuje však, že útočníci čoraz častejšie využívajú generatívnu AI na tvorbu presvedčivých škodlivých reklám. Google posúva detekciu na úroveň jednotlivých reklám namiesto plošného blokovania účtov.

Spojené kráľovstvo vyšetruje Telegram a chatové platformy pre podozrenia zo šírenia obsahu zneužívania detí

Britský regulátor Ofcom začal vyšetrovanie platformy Telegram a dvoch tzv. teen chat webov (napr. Teen Chat a Chat Avenue) po tom, čo dostal od kanadskej organizácie na ochranu detí dôkazy naznačujúce šírenie materiálov so sexuálnym zneužívaním detí (CSAM) a riziká groomingových aktivít. Vyšetrovanie sa zameriavalo na to, či platformy dodržiavajú britský Online Safety Act a či majú dostatočné mechanizmy na prevenciu, detekciu a odstraňovanie nelegálneho obsahu. Ak by sa zistilo porušenie, spoločnostiam by hrozili vysoké pokuty alebo obmedzenie pôsobenia v UK.



Malvér NGate Android zneužíva NFC aplikáciu HandyPay na krádež platobných údajov kariet

Spoločnosť Eset zdokumentovala malvér NGate Android, ktorý sa šíri cez podvodné weby a falošné inštalačné balíky, ktoré napodobňujú legitímne NFC platobné aplikácie ako HandyPay. Útočníci modifikujú aplikáciu tak, aby po nainštalovaní na zariadenie obete zachytávala NFC komunikáciu z platobných kariet. Malvér dokáže v reálnom čase čítať údaje z kariet priložených k infikovanému telefónu, vrátane citlivých autentifikačných dát a PINu. Následne ich exfiltruje na server útočníkov, kde ich môžu zneužiť na vytváranie virtuálnych kariet alebo klonovanie platobných údajov. Analýza ukazuje, že ide o evolúciu staršieho malvéru NGate, ktorý sa už v minulosti zameriaval na útoky na NFC. Nová verzia vylepšuje maskovanie a využíva legitímne aplikácie, čo zvyšuje šancu na úspešné obídenie bezpečnostných kontrol a zneužitie údajov v reálnych finančných transakciách.

VÝZNAMNÉ UDALOSTI VO SVETE

Skupina UNC6692 v rámci phishingových kampaní zneužíva MS Teams a nástroje RMM na nasadenie novej malvérovej sady SNOW

Nová útočná skupina APT UNC6692 sa zameriava na firmy a zamestnancov. Vydáva sa za IT podporu a cez Microsoft Teams presviedča obete, aby prijali správy alebo spustili opravy na odstránenie problémov s e-mailmi. Útočníci najprv zaplavia inbox obete spamom, aby vyvolali stres, a následne ju kontaktujú cez Teams ako falošná IT podpora. Následne ju donútia kliknúť na phishingové odkazy alebo nainštalovať nástroje na vzdialený prístup. Tento postup vedie k nasadeniu vlastného malvéru SNOWBELT, ktorý útočníkom umožňuje exfiltráciu dát, laterálny pohyb v sieti a postupné preberanie kontroly nad kompromitovanými systémami.

Deštruktívny malvér Fast16 sa stáva prvým malvérom na báze Lua

Výskumníci zo spoločnosti SentinelOne Labs opisujú malvér Fast16, ktorý zrekonštruovali zo starého odkazu v uniknutých materiáloch skupiny Shadow Brokers. Analýza ukázala, že táto platforma vznikla už okolo roku 2005, teda približne 5 rokov pred Stuxnetom. Útočníci ho navrhli ako sofistikovaný nástroj na sabotovanie výpočtov v tzv. high-precision softvéri, kde upravoval výsledky vedeckých a inžinierskych simulácií bez toho, aby si to používatelia všimli. Fast16 sa šíril po sieti, cielil na špecifické programy (napr. LS-DYNA, PKPM či MOHID) a manipuloval ich numerické výpočty tak, aby produkovali nesprávne výsledky. Výskumníci ho považujú za jeden z najskorších známych príkladov štátom podporovaného softvérového sabotážneho nástroja tejto úrovne.

Modul Quick Page/Post Redirect pre WordPress obsahoval 5 rokov skrytý backdoor

Výskumník odhalil skryté zadné vrátka v module Quick Page/Post Redirect pre WordPress (~70k inštalácií), ktorý útočníkom umožňoval na základe špeciálnej požiadavky injektovať a spúšťať ľubovoľný kód PHP na serveri. Dával útočníkom plnú kontrolu nad webom vrátane nasadenia webshellu, presmerovaní či ďalšieho malvéru. Kompromitáciu odhalili až pri analýze napadnutých stránok. Analýza poukazuje na to, že útočník vložil škodlivý kód priamo do modulu v rámci kompromitácie dodávateľského reťazca.

VÝZNAMNÉ UDALOSTI VO SVETE

- Silver Fox infikuje čínsky hovoriace obete RAT malvérom AtlasCross RAT.
- FBI varuje pred rizikami čínskych mobilných aplikácií pre ochranu dát.
- Microsoft varuje pred malvérom šíreným cez WhatsApp.
- Nový nástroj CrystalRAT na špionáž a krádež dát.
- Ransomvérová skupina Qilin exfiltrovala údaje nemeckej politickej strany Die Linke.
- Ransomvérové skupiny Qilin a Warlock zneužívajú BYOVD a DLL side-loading na spúšťanie EDR killerov.
- Malvérová kampaň čínskej skupiny TA416 infikuje európsky vládny a diplomatický sektor malvérom PlugX.
- Podľa sumáru kybernetickej kriminality FBI došlo za rok 2025 v USA ku škodám vo výške 21 miliárd dolárov.
- Project Glasswing od Anthropic odhalil tisícky bezpečnostných zraniteľností využitím nového AI modelu Claude Mythos.
- Nová PhaaS platforma VENOM zneužíva na distribúciu phishingových URL QR kódy renderované znakmi Unicode.
- Prepravná spoločnosť Eurail potvrdila únik citlivých údajov vyše 300 000 subjektov.
- Prienik do interných systémov Bitcoin Depot umožnil krádež kryptomien v hodnote 3.6 milióna dolárov.
- Francúzska vláda plánuje postupne nahradiť Windows v štátnych počítačoch Linuxom v rámci stratégie digitálnej suverenity.
- Evolúcia kampane GlassWorm zneužíva binárky kompilované v jazyku Zig na infekciu IDE, ktoré podporujú VS Code.
- Falošné kryptopeňaženky cielia na čínsky App Store a kradnú frázy seed používateľov.
- Spoločnosť Vercel odhaľuje ďalšie kompromitované účty v prebiehajúcom incidente.
- FBI pridala na zoznam US Most Wanted čínskych aktérov asociovaných so spear-phishingovou kampaňou zameranou na získavanie citlivých údajov od zamestnancov NASA, vzdelávacích a výskumných organizácií.

- Skupina ShinyHunters prostredníctvom vishingového útoku kompromitovala účet Okta SSO zamestnanca americkej spoločnosti ADT a exfiltrovala citlivé údaje.

- Európske policajné zložky rozložili kyberkriminálnu skupinu špecializujúcu sa na investičné podvody v oblasti kryptomien.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Fortinet opravila zneužívanú kritickú zraniteľnosť FortiClientEMS

Spoločnosť Fortinet opravila kritickú aktívne zneužívanú zraniteľnosť svojho produktu FortiClientEMS, ktorá umožňuje obísť autentifikáciu a vzdialene vykonávať kód.

Zraniteľnosť Docker Engine umožňuje obísť kontrolu autorizácie

Vývojári Docker Engine opravili vysoko závažnú zraniteľnosť modulov AuthZ, ktorá dovoľuje útočníkom obchádzať kontroly autorizácie a vytvárať napríklad privilegované kontajnery.

Riešenie Aktívne zneužívaná kritická zraniteľnosť modulu WordPress Ninja Forms – File Uploads

Vývojári populárneho modulu pre WordPress, Ninja Forms – File Uploads, vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú aktívne zneužívanú kritickú zraniteľnosť. Jej zneužitie umožňuje nahrávanie ľubovoľných súborov na server.

Zraniteľnosť Apache ActiveMQ Classic umožňuje vykonávanie kódu

Vývojári opravili vysoko závažnú zraniteľnosť v open-source serveri Apache ActiveMQ Classic, ktorá umožňuje vzdialené vykonávanie kódu. Chyba sa v serveri nachádzala 13 rokov.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľné smerovače spoločnosti TP-Link môžu umožniť zneužitie DNS a odcudzenie prístupových údajov

VJ CSIRT vydala varovanie aby organizácie preverili, či sa pri vzdialenom prístupe do interných systémov nepoužívajú zraniteľné alebo nepodporované smerovače SOHO. Podľa varovania FBI a partnerov útočníci zneužívali kompromitované smerovače na zmenu DHCP a DNS nastavení, čím presmerovali DNS dopyty na vlastné prekladače a následne vedeli cielene podvrhnúť odpovede pre vybrané služby. Takto mohli zachytávať prihlasovacie údaje, tokeny a ďalšie citlivé údaje, najmä ak používateľ pokračoval aj po upozornení na chybu certifikátu. Medzi zneužívané zariadenia patrili aj smerovače TP-Link obsahujúce zraniteľnosť **CVE-2023-50224**.

IC3 vo varovaní neuvádza jeden konkrétny model, iba všeobecne „smerovače TP-Link zraniteľné na CVE-2023-50224“. Výrobca TP-Link následne spresnil, že ide o **viaceré staršie modely po ukončení podpory**, pričom medzi explicitne uvádzané patria napríklad **TL-WR841N / TL-WR841ND** a **Archer C7**. V novšom bezpečnostnom oznámení TP-Link sú medzi dotknutými zariadeniami uvedené aj ďalšie zastarané (angl. legacy) modely, napríklad **TL-MR6400, Archer C5, TL-WDR3600, TL-WDR4300, TL-WR740N, TL-WR741ND, TL-WR840N, TL-WR941ND, TL-WA801ND a TL-WA901ND**.

Kritická zraniteľnosť SAP Business Planning and Consolidation a SAP Business Warehouse

Vývojári spoločnosti SAP opravili kritickú zraniteľnosť v produktoch Business Planning and Consolidation a Business Warehouse, ktorá dovoľuje injektovať príkazy SQL. Útočník s nízkymi oprávneniami môže čítať, prepisovať a mazať dáta v databáze.

Cisco opravila kritické zraniteľnosti v ISE a ISE-PIC

Spoločnosť Cisco opravila štyri kritické zraniteľnosti produktov Identity Services Engine (ISE) a ISE Passive Identity Connector (ISE-PIC). Chyby zabezpečenia umožňujú útočníkom vykonávať systémové príkazy, čítať ľubovoľné súbory, eskalovať oprávnenia na úroveň používateľa root a spôsobovať nedostupnosť zraniteľných uzlov.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľnosť Splunk Enterprise a Splunk Cloud Platform umožňuje vykonávať kód.

Splunk Enterprise a Splunk Cloud Platform obsahuje zraniteľnosť, ktorá umožňuje útočníkovi s oprávneniami bežného používateľa vzdialene vykonávať kód nahraním škodlivého súboru do dočasného adresára. Zraniteľnosť Splunk MCP Serveru dovoľuje čítať používateľské tokeny vo voľnom texte.

BRIDGE:BREAK –zraniteľnosti ohrozujú priemyselné prevodníky Silex a Lantronix

Tím Forescout Research – Vedere Labs objavil sadu 22 zraniteľností prevodníkov sériovej komunikácie na IP od spoločností Silex a Lantronix. Útočník s prístupom do lokálnej siete ich môže zneužiť na prevzatie kontroly nad dôležitými priemyselnými riadiacimi prvkami obete. Môže napríklad obchádzať prihlásenie, získať administrátorské oprávnenia a vykonávať v ich kontexte systémové príkazy, či získavať citlivé informácie. Zraniteľnosti dostali súhrnný názov BRIDGE:BREAK.

Kritická zraniteľnosť SGLang

Platforma SGLang pre multimodálne modely AI obsahuje kritickú zraniteľnosť, ktorá umožňuje podvrhnutím škodlivej chatovej šablóny renderovaciemu procesu spôsobiť vykonanie ľubovoľného vloženého kódu v jazyku Python.

Pack2TheRoot: eskalácia oprávnení v PackageKit

Red Team z Deutsche Telekom objavil vysoko závažnú zraniteľnosť, ktorá je v manažéri PackageKit prítomná aspoň 12 rokov. Používateľovi s nízkymi oprávneniami umožňuje inštalovať balíky RPM a vykonávať RPM skriptlety s oprávneniami používateľa root.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľnosť GitHub umožňuje vykonávať príkazy na serveri

Vývojári spoločnosti GitHub opravili vysoko závažnú zraniteľnosť na platformách GitHub Enterprise Server, GitHub Enterprise Cloud a github.com, ktorá umožňovala používateľom s oprávnením vykonávať príkaz git push vzdialene vykonávať ľubovoľné príkazy na hostiteľskom serveri.

MESAČNÍK ZRANITEĽNOSTÍ APRÍL 2026

VJ CSIRT pravidelne vydáva mesačný prehľad kritických zraniteľností.

https://csirt.sk/posts/3419.html