CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

APRÍL 2025

TLP: CLEAR

Kybernetickým priestorom v apríli 2025 rezonovalo hneď niekoľko kľúčových udalostí a útokov. Doplňujúce informácie môžete nájsť v časti Významné udalosti vo svete.

1 Mobilný malvér CROCODILUS sa zameriava na bankové dáta a kryptopeňaženky

Bezpečnostní výskumníci z THREATFABRIC upozorňujú na nový malvér s názvom CROCODILUS, ktorý sa zameriava na používateľov systému Android s cieľom získať prístup k ich kryptopeňaženkám a bankovým údajom.

2 Únik citlivých údajov z kompromitovaného GitLab repozitára EUROPCAR MOBILITY GROUP

Útočník vystupujúci pod aliasom EUROPCAR na hackerskom fóre BREACHFORUMS zverejnil informácie o kompromitácii GitLab repozitára medzinárodnej spoločnosti na prenájom áut EUROPCAR MOBILITY GROUP.

3 Vishingová kampaň v Taliansku využíva AI na klonovanie hlasu

Prebieha podvodná kampaň vishingu v Taliansku, kde sa podvodníci vydávajú za ministra obrany Guida Crosetta a žiadajú peniaze na oslobodenie unesených novinárov.

4 Ransomvérová skupina HellCat zneužíva uniknuté prihlasovacie údaje do Jira

Skupina ransomvéru HellCat v apríli 2025 napadla štyri spoločnosti v USA a Európe. Útočníci získali prístup pomocou poverení Jira, ktoré získali prostredníctvom malvéru typu infostealer, ako sú StealC, Raccoon, Redline a Lumma Stealer.

5 USA ukončuje financovanie CVE programu pod hlavičkou MITRE

16. apríla 2025 oficiálne končí projekt finančnej podpory vlády USA pre program CVE (Common Vulnerabilities and Exposures) neziskovej organizácie MITRE.

6 PRODAFT infiltruje hackerské fóra cez odkúpené účty

Švajčiarska kyberbezpečnostná spoločnosť PRODAFT spustila iniciatívu s názvom „Sell your Source“, v rámci ktorej nakupuje overené a staršie účty na hackerských fórach, aby získala prístup do kyberkriminálnych komunít a zhromažďovala cenné spravodajské informácie.

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.

CSIRT.SK prijal v rámci hlásenia incidentu vzorku škodlivého mailu, ktorý niesol všetky znaky trestného činu. Vzorka obsahovala prvky nátlaku, vydierania a naznačovala ransomvérový útok. Ten bolo potrebné preveriť na základe prítomnosti artefaktov poukazujúcich na pripojenie cez Remote Desktop Connection (RDC). Po analýze a preverení všetkých možností sa ukázalo, že sa jednalo o podvodný pokus vylákať o obete finančné prostriedky / sociálne inžinierstvo.

Jednotka prijala informáciu o zasielaných podvodných SMS správach zneužívajúcich dizajn Ústredného portálu verejnej správy (slovensko.sk). Obsah týchto správ klamlivo informoval o údajných pokutách a vyzýval na ich úhradu prostredníctvom uvedeného podvodného odkazu. V SMS správe bolo uvedené skutočné číslo Ústredného kontaktného centra. Verejnosť bola o týchto smishingových správach informovaná prostredníctvom Ústredného portálu verejnej správy (slovensko.sk).

V apríli prišlo tiež nové hlásenie o fyzickej hrozbe namierenej vo všeobecnosti na budovu organizácie v konštituencii CSIRT.SK. Jednotka v rámci vyšetrovania požiadala o relevantné dáta a logy. Na základe Metodiky vyhodnocovania rizika bombových hrozieb, ktorá sa zameriava na proces vyhodnotenia stupňa rizika bombových hrozieb bola identifikovaná nízka úroveň možnosti naplnenia hrozby.

Na webovej stránke organizácie v konštituencii VJ CSIRT bol verejne prístupný súbor /info.php. Tento súbor obsahuje konfiguračné informácie PHP o verzii PHP, nainštalovaných rozšíreniach, nastaveniach servera a systémových cestách, čo môže potenciálny útočník zneužiť na identifikáciu zraniteľností webového servera. Z bezpečnostného hľadiska tento súbor nesmie byť nikdy verejne dostupný na produkčnom prostredí.

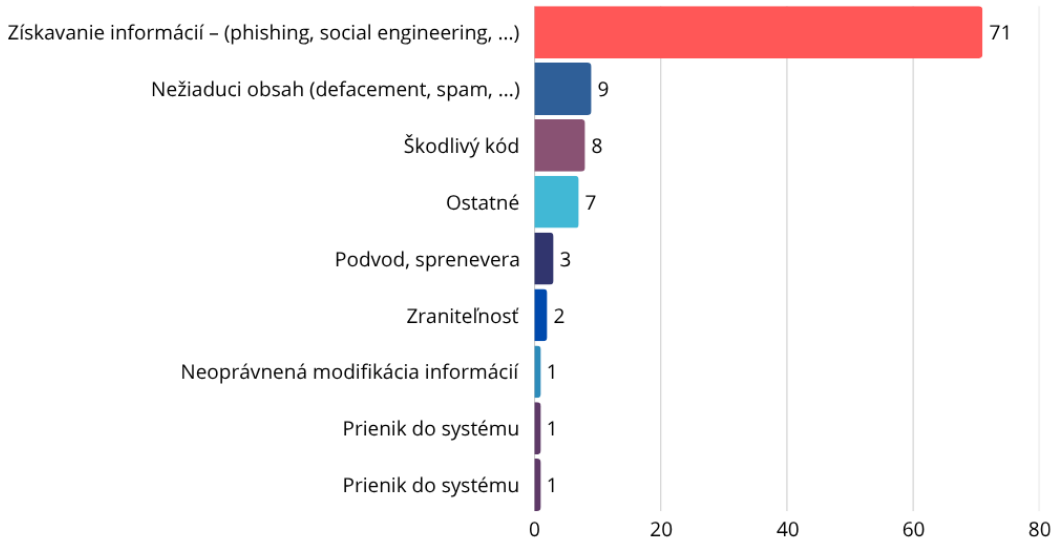
V rámci svojej proaktívnej činnosti jednotka CSIRT.SK vykonáva pravidelné skenovanie a overovanie zraniteľností v službách a zariadeniach IT infraštruktúr organizácií vo svojej konštituencii, ktoré sú vystavené do internetu. Využíva k tomu platformu Achilles, ktorú sama vyvíja a prevádzkuje. Systém Achilles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

Na svojej webstránke uverejnila CSIRT.SK návod na overenie úniku prihlasovacích údajov zamestnancov v rámci domény organizácie. Jeho aplikácia má potenciál pomôcť organizáciám odhaľovať úniky prihlasovacích údajov a vykonávať nápravné opatrenia pre zabezpečenie svojich IT infraštruktúr ešte pred ich kompromitáciou.

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 študentov SOŠ polytechnickej v Nitre, SOŠ ekonomickej v Spišskej Novej Vsi, SOŠ pedagogickej v Modre a Technickej Univerzity v Košiciach.

Členovia VJ CSIRT sa zúčastnili tiež na konferencii KyberTour 2025 v Žiline, ktorú organizovalo MIRRI SR v rámci série konferencií zameraných na aktuálne témy v oblasti kybernetickej bezpečnosti, nových legislatívnych zmien a inovácií v digitálnom priestore.

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



VÝZNAMNÉ UDALOSTI VO SVETE

Mobilný malvér Crocodilus sa zameriava na bankové dáta a kryptopeňaženky

Bezpečnostní výskumníci z THREATFABRIC upozorňujú na nový malvér s názvom CROCODILUS, ktorý sa zameriava na používateľov systému Android s cieľom získať prístup k ich kryptopeňaženkám a bankovým údajom. Crocodilus sa šíri prostredníctvom vlastného droppera, ktorý obchádza bezpečnostné opatrenia v systéme Android 13 a novších. Tento dropper inštaluje malvér bez aktivácie ochrany Play Protect a obchádza obmedzenia služby Accessibility Service. Keylogger v malvéri Crocodilus využíva služby na zariadeniach Android na sledovanie stlačených kláves a textových zmien na obrazovke, vrátane hesiel a kódov OTP. Tieto informácie sa následne posielajú útočníkom, ktorí môžu získať kontrolu nad zariadením a vykonávať podvodné aktivity, ako sú neoprávnené finančné transakcie. Článok obsahuje indikátory kompromitácie.

Severokórejská APT Lazarus pokračuje v efektívnom zneužívaní techniky ClickFix

Severokórejská APT skupina Lazarus používa techniku "ClickFix" pri útokoch cielených na kryptomenové firmy. Skupina používa falošné chyby na webových stránkach alebo dokumentoch, ktoré vyzývajú používateľov k spusteniu príkazov PowerShell na "opravu" problému, čo v skutočnosti stiahne a spustí malvér v systéme obete. Skupina už dlhodobo robí falošné interview v tandeme s ClickFix. Spoločnosť Sekoia zdieľala Yara pravidlá, ktoré pomôžu organizáciám odhaliť a zablokovať aktivitu tzv. ClickFake. V článku poskytla zoznam indikátorov kompromitácie (IOC).

Ransomvérová skupina Hunters mení modus operandi a názov skupiny

Skupina kyberzločincov známa ako Hunters International sa premenovala na World Leaks a oznámila zmenu svojej stratégie – od ransomvérových útokov prechádza výhradne k vydieraniu prostredníctvom úniku dát. Tento model kopíruje štýl iných skupín ako Karakurt alebo BianLian, ktoré takisto opustili ransomvér. Veľa skupín upustilo od tradičného ransomvérového modelu a metódy double extortion, a namiesto toho sa zamerali na data leak extortion. Tento krok je pravdepodobne reakciou na zvyšujúci sa tlak a opatrenia proti ransomvéru. Data leak extortion je menej riskantná taktika, pretože nevyžaduje šifrovanie systémov, čo umožňuje efektívnejšie dosahovať finančný zisk a zároveň minimalizovať riziko zlyhania útoku. Článok obsahuje indikátory kompromitácie (IOC), techniky, taktiky a procedúry (TTP).

VÝZNAMNÉ UDALOSTI VO SVETE

Únik citlivých údajov z kompromitovaného GitLab repozitára Europcar Mobility Group

Útočník vystupujúci pod aliasom EUROPCAR na hackerskom fóre BREACHFORUMS zverejnil informácie o kompromitácii GitLab repozitára medzinárodnej spoločnosti na prenájom áut EUROPCAR MOBILITY GROUP. Útočník mal získať 37 GB dát obsahujúcich zálohy SQL, súbory s environmentálnymi premennými, detaily o cloudovej infraštruktúre, zdrojové kódy mobilných aplikácií a osobné údaje vyše 200 000 zákazníkov. Spoločnosť potvrdila pravosť údajov a v súčasnosti pracuje na riešení incidentu. Taktiež boli notifikovaní všetci zasiahnutí klienti.

Masívna kampaň cielená na používateľov kryptopeňaženiek Coinbase a Ledger

Bezpečnostní výskumníci zo spoločnosti SILENT PUSH zverejnili informácie o masívnej phishingovej kampani POISONSEED, ktorá sa zameriava na používateľov kryptopeňaženiek COINBASE a LEDGER. Útočníci z kompromitovaných účtov emailových distribučných služieb Mailchimp, SendGrid, HubSpot, Mailgun a Zoho rozosielajú emaily upozorňujúce na potrebu prevodu aktív na novú kryptopeňaženku. Výskumníci s touto kampaňou prepojili aj nedávnu kompromitáciu Mailchimp konta Troy Hunta a SendGrid účtu Akamai. Distribučné služby kompromitujú phishingovými útokmi, následne exportujú mailing listy, vytvárajú nové API kľúče na zabezpečenie perzistencie a kontá zneužívajú na rozosielanie phishingu. Článok obsahuje indikátory kompromitácie (IOC).

Vishingová kampaň v Taliansku využíva AI na klonovanie hlasu

Prebieha podvodná kampaň vishingu v Taliansku, kde sa podvodníci vydávajú za ministra obrany Guida Crosetta a žiadajú peniaze na oslobodenie unesených novinárov. Umelá inteligencia (AI) zvyšuje nebezpečenstvo hlasového phishingu, známeho ako "vishing". Scammeri dokážu klonovať hlasy skutočných osôb, čo im umožňuje presvedčivo napodobniť napríklad rodinných príslušníkov alebo kolegov. Technológia využíva pokročilé modely, ako je WaveNet od Google DeepMind na napodobenie ľudských hlasových vzorov. Vishing alebo „hlasový phishing“ je forma sociálneho inžinierstva, kde podvodníci používajú telefonáty na oklamanie obetí, aby odhalili citlivé informácie alebo uskutočnili podvodné platby. V rámci SR boli zaznamenané deepfake-ové videá zneužívajúce identitu verejne známych osôb na propagáciu investícií do kryptomien. **VJ CSIRT sleduje technologický vývoj v oblasti AI a možnosti jej zneužitia v rámci kybernetických útokov, vrátane klonovania hlasu.**

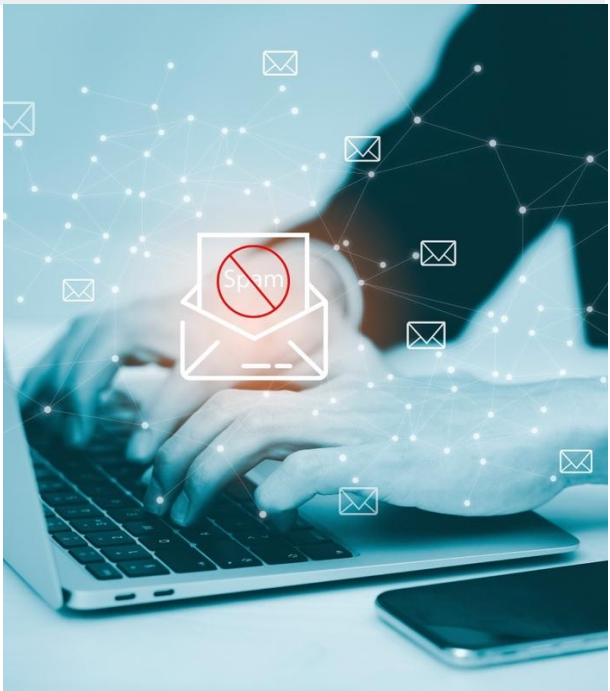
VÝZNAMNÉ UDALOSTI VO SVETE

Ransomvérová skupina HellCat zneužíva uniknuté prihlasovacie údaje do JIRA

Ransomvérová skupina HellCat v apríli 2025 napadla štyri spoločnosti v USA a Európe. Útočníci získali prístup pomocou poverení Jira, ktoré získali prostredníctvom malvéru typu infostealer, ako sú StealC, Raccoon, Redline a Lumma Stealer. Malvér mesiace alebo dokonca roky zhromažďoval prihlasovacie údaje zamestnancov. Po získaní týchto poverení sa útočníci prihlásili do systémov Jira cieľových spoločností, čo im umožnilo pohybovať sa po interných systémoch a získavať citlivé údaje. Medzi zasiahnuté firmy patrili Asseco Poland, HighWire Press, Racami a LeoVegas Group. HellCat následne požadoval výkupné výmenou za nezverejnenie alebo nepredanie ukradnutých údajov. V screenshotoch únikov spoločností ASSECO sa nachádzajú aj dokumenty v slovenčine.

Phishing-as-a-service Tycoon2FA implementuje nové mechanizmy maskovania činnosti

Bezpečnostní výskumníci zo spoločnosti TRUSTWAVE zverejnili informácie o novej verzii platformy phishing-as-a-service TYCOON2FA, ktorá sa špecializuje na kompromitáciu účtov Microsoft365 a Gmail a obchádzanie viacfaktorovej ochrany. Nová verzia prináša funkcionality pre maskovanie svojej činnosti. Prvou z metód je zneužívanie neviditeľných znakov Unicode na skrývanie binárnych dát v súboroch JavaScript, ktoré výrazne limitujú možnosti identifikácie škodlivého kódu založených na manuálnej inšpekcii kódu a vyhľadávaní signatúr. Druhou je prechod z Cloudflare Turnstile na vlastné mechanizmy CAPTCHA renderované pomocou HTML5 canvasu. Treťou je implementácia anti-debugovacích techník, ktoré v prípade detekcie automatizovaného prehliadača blokujú funkcionalitu a návštevníka presmerujú na neškodnú stránku.



USA ukončuje financovanie programu CVE pod hlavičkou MITRE

16. apríla 2025 oficiálne končí projekt finančnej podpory vlády USA pre program CVE (Common Vulnerabilities and Exposures) neziskovej organizácie MITRE. Tento program je jedným zo základných pilierov kybernetickej bezpečnosti a predstavuje de facto štandard pre identifikáciu, popis, hodnotenie závažnosti a záznam informácií o bezpečnostných zraniteľnostiach. Barsoum, ktorý je viceprezidentom MITRE, v otvorenom liste pre riadiaci výbor CVE poukázal na možné riziká vyplývajúce z ukončenia podpory. Spoločnosť VULNCHECK, ktorá je CNA autoritou, preventívne zarezervovala 1000 CVE.

VÝZNAMNÉ UDALOSTI VO SVETE

Slopsquatting ohrozuje komunitu vývojárov využívajúcich AI

Bezpečnostný výskumník upozornil na nový fenomén a bezpečnostné riziko súvisiace s halucináciou jazykových modelov používaných pri programovaní. Pojem SLOPSQUATTING označuje generovanie výstupov obsahujúcich referenciu na knižnicu s neexistujúcim názvom, ktorá vytvára potenciál pre rôzne útoky na dodávateľský reťazec. Útoky na dodávateľský reťazec založené na vytváraní knižníc PyPI alebo NPM s názvami napodobňujúcimi legitímne knižnice sú v súčasnosti obľúbenou metódou útočníkov, ktorí sa doteraz spoliehali na nepozornosť programátorov. V prípade slopsquattingu útočník negeneruje len knižnice s typosquatting názvami, ale aj reťazcami používanými jazykovými modelmi v rámci generovania príkladov kódu. Príchod metód pre poisoning modelov, rozmach vibe codingu a dôvery vo výstupy jazykových modelov prinášajú úplne nové riziká. Programátori a používatelia by nikdy nemali slepo dôverovať výstupom AI modelov a mali by manuálne overovať minimálne názvy referencovaných balíkov a knižníc.

PRODAFT infiltruje hackerské fóra cez odkúpené účty

Švajčiarska kyberbezpečnostná spoločnosť PRODAFT spustila iniciatívu s názvom „Sell your Source“, v rámci ktorej nakupuje overené a staršie účty na hackerských fórach, aby získala prístup do kyberkriminálnych komunít a zhromažďovala cenné spravodajské informácie. Cieľom je odhaliť škodlivé operácie a platformy prostredníctvom infiltrácie týchto prostredí. Prodaft má záujem o účty na fórach ako XSS, Exploit.in, RAMP4U, Verified a BreachForums. Predajcovia môžu spoločnosť kontaktovať anonymne prostredníctvom TOX alebo e-mailu a po schválení účtu dostanú ponuku na odkúpenie. Platba prebieha v kryptomenách ako Bitcoin, Monero alebo iných podľa preferencie predajcu. Jedná sa o mimoriadne sofistikovaný ťah, ktorý výskumníkom umožní získať prístup k platformám, na ktorých je registrácia často podmienená pozvánkou, overením alebo zaplatením poplatku. Pokročilejšie platformy ako napr. BREACHFORUMS dokonca aplikujú dodatočné mechanizmy brániace automatizovanému prechádzaniu príspevkov, ktoré sú založené na behaviorálnej analýze aktivity používateľských účtov a kreditovom systéme.

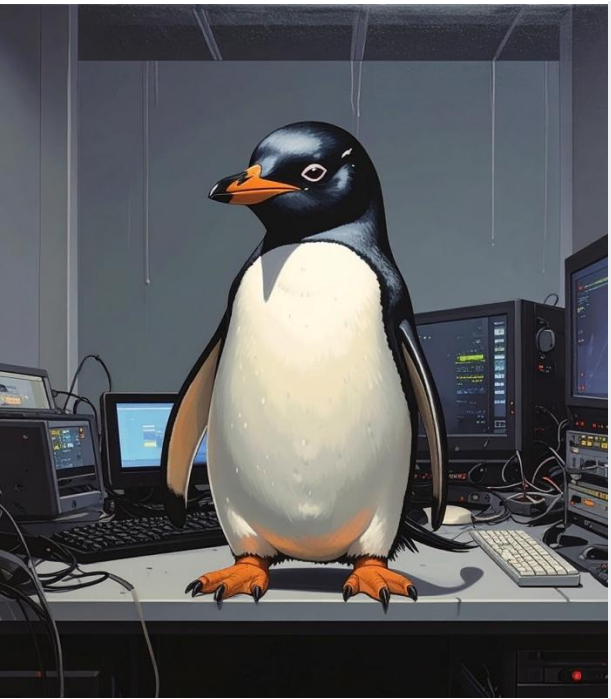
VÝZNAMNÉ UDALOSTI VO SVETE

PhaaS platforma Darcula zneužíva AI na kopírovanie vizuálu objektu impersonácie

Kyberzločinecká skupina stojaca za platformou Darcula, ktorá poskytuje phishing ako službu (PhaaS), nedávno aktualizovala svoj nástroj darcula-suite o generatívnu umelú inteligenciu (AI). Táto aktualizácia zjednodušuje tvorbu podvodných webových stránok, čím umožňuje aj technicky menej zdatným útočníkom rýchlo vytvárať personalizované phishingové kampane. Nástroj darcula-suite umožňuje používateľom zadať URL adresu legitímnej webovej stránky, ktorú systém navštívi, stiahne jej obsah a vytvorí editovateľnú verziu. Útočníci môžu do tejto klonovanej stránky vložiť škodlivé prvky, ako sú formuláre na získavanie prihlasovacích údajov. Tento proces nevyžaduje programátorské znalosti, čím sa znižuje technická náročnosť a zvyšuje dostupnosť phishingových nástrojov.

Útočníci zneužívajú slabiny Google OAuth na realizáciu DKIM replay útokov

Útočníci zneužili slabinu v systéme Google OAuth a techniku DKIM replay na rozposielanie phishingových e-mailov, ktoré sa tvárili ako oficiálne správy od „no-reply[at]google.com“. Tieto emaily obsahovali falošné upozornenia, napríklad o údajnej právnej žiadosti, a presmerovali používateľov na podvodné stránky vytvorené cez službu Google Sites, ktoré napodobňovali legitímne portály technickej podpory. Útočníci vytvorili vlastné aplikácie v rámci Google OAuth, pričom celý text podvodnej správy zadali ako názov aplikácie, čím dosiahli, že e-maily prešli overením DKIM a vyhli sa spamovým filtrom. Článok obsahuje indikátory kompromitácie (IOC).



Linuxový mechanizmus io_uring umožňuje rootkitom obísť detekciu bezpečnostných nástrojov

Výskumníci zo spoločnosti ARMO odhalili, že mechanizmus io_uring v Linuxe predstavuje vážnu bezpečnostnú medzeru, ktorú zneužívajú rootkity na obchádzanie bezpečnostných nástrojov. Io_uring umožňuje asynchrónne vstupno-výstupné operácie bez použitia tradičných systémových volaní, čím sa vyhýba detekcii. ARMO vytvorila ukážkový koncept rootkitu s názvom Curing, ktorý využíva výhradne io_uring, čím demonštruje schopnosť úplne obísť existujúce bezpečnostné opatrenia. Hoci niektorí dodávatelia reagovali opravami, väčšina sektora zostáva voči tejto hrozbe zraniteľná. ARMO odporúča implementáciu pokročilejších detekčných mechanizmov, ako je KRSI (Kernel Runtime Security Instrumentation), pre efektívne monitorovanie takýchto útokov.

VÝZNAMNÉ UDALOSTI VO SVETE

- Phishingová kampaň zameraná na subjekty na Ukrajine je navrhnutá na šírenie trójskeho koňa Remcos RAT.

- Bezpečnostní výskumníci zo spoločnosti F5 LABS odhalili novú kampaň cielenú na webové stránky v rámci ktorej dochádza k zneužitiu EC2 INSTANCE METADATA prostredníctvom rôznych SSRF (Server Side Request Forgery) zraniteľností.

- Ukrajinský tím CERT-UA odhalil novú sériu kybernetických útokov zameraných na ukrajinské inštitúcie, najmä vojenské jednotky, orgány činné v trestnom konaní a miestne samosprávy v blízkosti východnej hranice Ukrajiny.

- Výskumný tím Seqrite Labs odhalil nové taktiky pakistanskej APT skupiny SideCopy, ktorá od konca decembra 2024 rozšírila svoje útoky na viaceré sektory v Indii vrátane železníc, ropného a plynárenského priemyslu a ministerstva zahraničných vecí.

- Spoločnosť Microsoft opakovane upozornila na blížiaci sa koniec podpory produktu Exchange 2016 a Exchange 2019, ktorý nastane 14. októbra 2025.

- Hackerská skupina "Elusive Comet" vykonala útoky sociálnym inžinierstvom na vybraných používateľov kryptomien. Využili na to platformu Zoom a jej funkciu vzdialeného ovládania na oklamanie používateľov, aby im povolili vzdialený prístup cez Zoom do svojich zariadení.

- Aplikácia WhatsApp zaviedla novú funkciu Advanced Chat Privacy na ochranu citlivých informácií vymieňaných v súkromných chatoch a skupinových konverzáciách.

- Severokórejskí útočníci ukradli v rámci jedného dňa kryptomeny v hodnote viac ako 137 miliónov dolárov od používateľov platformy TRON.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Apple vydali opravy 213 zraniteľností v iOS, iPadOS a macOS, aktualizovali aj staršie systémy

Spoločnosť Apple vydala aktualizačné balíky pre svoje systémy iOS, iPadOS a macOS, v ktorých opravuje množstvo bezpečnostných chýb. Zároveň aktualizovala aj staršie systémy iOS a iPadOS verzií 15, 16 a 17 a macOS 13 a 14, s cieľom odstrániť aktívne zneužívané zraniteľnosti zverejnené v posledných mesiacoch. Opravy vydala aj pre tvOS a visionOS.

Kritická zraniteľnosť CrushFTP umožňuje obísť prihlasovanie

CrushFTP obsahuje aktívne zneužívanú kritickú zraniteľnosť vo svojom autentifikačnom mechanizme, ktorá dovoľuje prihlásiť sa len s uvedením prihlasovacieho mena.

Vysoko závažné zraniteľnosti v produktoch Splunk

Spoločnosť Splunk vydala bezpečnostné aktualizácie na svoje produkty Splunk Enterprise, Splunk Cloud Platform a Splunk Secure Gateway, ktoré opravujú 8 bezpečnostných zraniteľností, z čoho 2 sú označené ako vysoko závažné. CVE-2025-20229 možno zneužiť na vzdialené vykonanie kódu a CVE-2025-20231 na získanie neoprávneného prístupu k citlivým údajom. Aktualizácie taktiež opravujú viacero zraniteľností v komponentoch tretích strán, ktoré sú v rámci produktov využívané.

Kritické zraniteľnosti v úložiskách Dell Unity, Dell UnityVSA a Dell Unity XT

Spoločnosť Dell vydala bezpečnostné aktualizácie na svoje úložiská Dell Unity, Dell UnityVSA a Dell Unity XT, ktoré opravujú 15 zraniteľností, z čoho 2 sú označené ako kritické. Kritickú zraniteľnosť s označením CVE-2025-22398 možno zneužiť na vzdialené vykonanie kódu a zraniteľnosť CVE-2025-24383 na vykonanie neoprávnených zmien v systéme, ktoré môžu spôsobiť úplnú nedostupnosť služieb.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritická zraniteľnosť v Apache Parquet

Vývojári stĺpcovo orientovaného formátu súborov Apache Parquet vydali bezpečnostné aktualizácie pre svoju knižnicu pre Java, ktoré opravujú kritickú zraniteľnosť. CVE-2025-30065 by vzdialený neautentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémami využívajúcimi predmetnú knižnicu.

Aktívne zneužívaná zraniteľnosť v produktoch Ivanti ICS, IPS a ZTA Gateway

Spoločnosť Ivanti vydala bezpečnostné aktualizácie pre svoje produkty Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS) a ZTA Gateways, ktoré opravujú aktívne zneužívanú kritickú zraniteľnosť. CVE-2025-22457 možno zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom.

Google opravil 2 aktívne zneužívané zero-day zraniteľnosti operačného systému Android

Spoločnosť Google vydala bezpečnostné aktualizácie pre svoj operačný systém Android, ktoré opravujú 62 zraniteľností, z čoho 4 je označených ako kritické a 2 ako aktívne zneužívané. CVE-2024-53150 a CVE-2024-53197 v kerneli možno zneužiť na eskaláciu privilégií a získanie neoprávneného prístupu k citlivým údajom.

Zraniteľnosť aplikácie WhatsApp for Windows umožňovala vzdialené vykonanie kódu

Spoločnosť Meta vydala bezpečnostné aktualizácie pre aplikáciu WhatsApp for Windows, ktoré opravujú bezpečnostnú zraniteľnosť CVE-2025-30401. Napriek tomu, že sa jedná o zraniteľnosť strednej závažnosti, možno ju zneužiť na vzdialené vykonanie škodlivého kódu.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľnosti v databázovom systéme SQLite

Vývojári databázového systému SQLite vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú dve zraniteľnosti. Ich zneužitím možno vyvolať poškodenie pamäte a zneprístupnenie služby kvôli pádu aplikácie.

Kritické zraniteľnosti v produktoch SAP

Spoločnosť SAP vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú 20 zraniteľností, z ktorých 3 sú označené ako kritické. CVE-2025-27429 a CVE-2025-31330 v produktoch SAP S/4HANA a SAP Landscape Transformation možno zneužiť na vzdialené vykonanie kódu. CVE-2025-30016 v produkte SAP Financial Consolidation možno zneužiť na obídenie mechanizmov autentifikácie.

Kritické zraniteľnosti v nástroji pgAdmin 4

Vývojári nástroja na administráciu databáz PostgreSQL pgAdmin 4 vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú 2 kritické zraniteľnosti. CVE-2025-2946 možno zneužiť na realizáciu XSS útokov a CVE-2025-2945 na vzdialené vykonanie kódu.

Zraniteľnosť v OpenVPN možno zneužiť na zneprístupnenie služby

Vývojári OpenVPN vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú vysoko závažnú zraniteľnosť. Zraniteľnosť s identifikátorom CVE-2025-2704 možno zneužiť na zneprístupnenie služby.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritická zraniteľnosť v zariadeniach Fortinet FortiSwitch

Spoločnosť Fortinet vydala bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť v zariadeniach FortiSwitch. Zraniteľnosť možno zneužiť na neoprávnenú zmenu prihlasovacích údajov administrátorských účtov a následné získanie úplnej kontroly nad systémom.

Kritické bezpečnostné zraniteľnosti v produktoch Adobe

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty ColdFusion, After Effects, Media Encoder, Bridge, Experience Manager (AEM) Forms on JEE, Premiere Pro, Photoshop, Animate, Experience Manager (AEM) Screens, FrameMaker, XMP-Toolkit-SDK, Commerce, Commerce B2B a Magento Open Source, ktoré opravujú 58 zraniteľností, z čoho 28 je označených ako kritické. Najzávažnejšie kritické zraniteľnosti by vzdialený útočník mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom a vykonanie škodlivého kódu.

Active! Mail má kritickú zero-day zraniteľnosť

Spoločnosť Qualitia opravila kritickú zraniteľnosť v mailovom klientovi Active! Mail, ktorá umožňuje vzdialené vykonávanie kódu. Zraniteľnosť útočníci aktívne zneužívajú.

Kritická zraniteľnosť v SonicWall SonicOS SSLVPN

Spoločnosť SonicWall vydala bezpečnostné aktualizácie svojho operačného systému SonicOS, ktoré opravujú vysoko závažnú zraniteľnosť v rozhraní SSLVPN Virtual Office. CVE-2025-32818 by vzdialený neautentifikovaný útočník mohol zneužiť na zneprístupnenie služby.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritická zraniteľnosť vo frameworku PyTorch

Vývojári pythonového open-source frameworku pre strojové učenie PyTorch vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú kritickú zraniteľnosť. CVE-2025-32434 možno zneužiť na vzdialené vykonanie kódu.

Kritická zraniteľnosť v knižnici Erlang/OTP

Vývojári knižnice Erlang OTP (Open Telecom Platform) vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú kritickú zraniteľnosť v serverovom komponente SSH. Zraniteľnosť s identifikátorom CVE-2025-32433 možno zneužiť na vzdialené vykonanie kódu.

MESAČNÍK ZRANITEĽNOSTÍ APRÍL 2025

VJ CSIRT pravidelne vydáva mesačný prehľad kritických zraniteľností.

https://csirt.sk/posts/2330.html