CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

SEPTEMBER 2025

TLP: WHITE

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

1 VJ CSIRT informuje o kybernetickom útoku, ktorý zasiahol automobilovú spoločnosť Jaguar Land Rover

Automobilová spoločnosť Jaguar Land Rover informovala v oficiálnom vyhlásení, že čelí kybernetickému útoku a podnikla kroky na obnovenie bežnej produkcie.

2 Rozsiahly útok na dodávateľský reťazec kompromitoval stovky NPM knižníc kryptodrainerom

Výskumníci z AIKIDO security zverejnili analýzu rozsiahleho útoku na dodávateľský reťazec, v rámci ktorého došlo ku kompromitácii vyše 500 populárnych NPM knižníc.

3 Slovenské školy sa pripravujú na AI

Ministerstvo školstva SR pripravuje zavedenie umelej inteligencie do školského systému tak, aby sa predišlo chybám z minulosti pri implementácii sociálnych sietí.

4 CISA plánuje väčšiu kontrolu nad programom CVE

CISA zverejnila dokument, v ktorom predstavila svoju víziu budúcnosti programu CVE (Common Vulnerabilities and Exposures). Podľa dokumentu CISA plánuje prevziať väčšiu kontrolu nad týmto globálnym štandardom pre identifikáciu zraniteľností.

5 Ransomvérový útok na COLLINS AEROSPACE ochromil viaceré letiská v Európe

Ransomvérový útok na spoločnosť COLLINS AEROSPACE negatívne ovplyvnil viaceré letiská, ktoré využívali ich informačný systém na check-in cestujúcich, tlač boarding passov a označovanie batožiny.

6 Nová phishingová kampaň zameraná na PyPI kradne prihlasovacie údaje

Spoločnosť Python Software Foundation (PSF) upozornila vývojárov na novú vlnu phishingových útokov, ktoré používajú falošnú webovú stránku Python Package Index (PyPI) na krádež prihlasovacích údajov.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci september 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 rámci podvodných e-mailov Vládna jednotka CSIRT prijala v septembri vzorku správy obsahujúcej číslo účtu vedené v slovenskej banke, ktorý mohol byť aktívne zneužívaný. Jednotka vykonala analýzu vzorky. Vzhľadom na to, že tento pokus o podvod obsahuje bankový účet, ktorý útočník aktívne zneužíva, alebo vlastní, bolo zrealizované aj stretnutie s NCODK ohľadne ďalších krokov.

CSIRT.SK prijal od partnera hlásenie škodlivej aktivity z IP adresy, ktorá patrí do sieťového rozsahu organizácie v jeho konštituencii. Aktivita bola vyhodnotená ako 'port scanner' a po analýze jednotka kontaktovala správcov IP adresného rozsahu s požiadavkou o preverenie problému.

Jednotka prijala tiež od partnera hlásenie na základe monitoringu otvorených zdrojov a potenciálnych hrozieb v kybernetickom priestore SR, ktoré upozorňovalo na potenciálnu kompromitáciu bližšie neurčeného e-mailového účtu v doméne verejnej organizácie v konštituencii CSIRT.SK. Na základe doplnenia informácií, ktoré jednotka partnerovi poskytla, bolo zistené, že zasiahnuté zariadenia boli infikované infostealerom, resp. škodlivým kódom slúžiacim pre krádež dát. Na základe identifikovaných účtov CSIRT.SK odporučil plošnú zmenu hesiel a rad ďalších nevyhnutných opatrení na zamedzenie škodlivej činnosti.

September sa zapísal kybernetickým incidentom s potenciálnym významným dopadom. Kriminálna skupina napadla a ransomvérom zneprístupnila dôležité údaje nemocničnej ambulancie slovenskej nemocnice. Lokálne oddelenie IT zistilo zmeny súborov viacerých informačných systémov, našlo tzv. ransomnote a identifikovalo potencionálne škodlivý proces, ktorý ukončilo. CSIRT.SK prevzal riešenie incidentu, prekonzultoval s nemocnicou potrebné opatrenia, a tiež vyžiadal zasiahnuté zariadenie na forenznú analýzu. Od spoločnosti poskytujúcej monitorovacie služby si vyžiadal logy. Súbežne CTI tím CSIRT.SK začal vykonávať činnosti spojené so získavaním dodatočných informácií. V súčasnosti prebieha forenzná analýza dodaných zariadení, logov a monitoring situácie. Tento incident je mementom, že ani Slovensku sa nevyhýbajú kybernetickí zločinci, ktorých činnosť môže ohroziť zdravie a životy občanov.

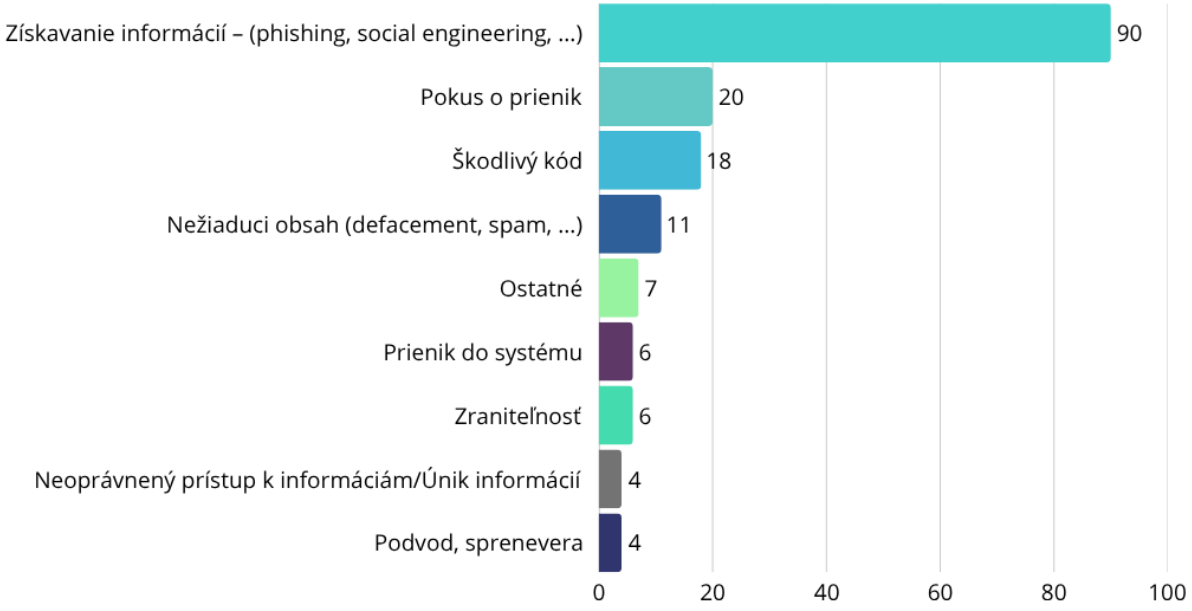
V rámci svojej proaktívnej činnosti jednotka CSIRT.SK vykonáva pravidelné skenovanie a overovanie zraniteľností v službách a zariadeniach IT infraštruktúr organizácií vo svojej konštituencii, ktoré sú vystavené do internetu. Využíva k tomu platformu Achilles, ktorú sama vyvíja a prevádzkuje. Systém Achilles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

V septembri CSIRT.SK plošne varoval svoju konštituenciu ohľadom aktívne zneužívaných zraniteľností CVE-2025–9961, CVE-2025-9377 a CVE-2023-50224 v routroch TP-Link (vrátane Archer AX10 a AX1500, Archer C7 a TL-WR841N/ND). Zraniteľnosti útočníci zneužívajú na vzdialené vykonávanie kódu a zapájanie zariadení do botnetu Quad7.

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 septembri jednotka prezentovala rôzne témy z oblasti kybernetickej bezpečnosti pre študentov Strednej zdravotníckej školy Celestíny Šimurkovej v Trenčíne a Gymnázia Jána Papánka v Bratislave.

Vládna jednotka CSIRT v spolupráci s odborom počítačovej kriminality a odborom kriminálnej polície Prezídia Policajného zboru spustila sériu špecializovaných školení pre policajných vyšetrovateľov. Prvou témou vzdelávacej aktivity pre policajných vyšetrovateľov a operatívcov z celého Slovenska bolo zaisťovanie digitálnych stôp pri rôznych formách phishingových útokov. Vládna jednotka CSIRT organizovala prezenčné školenie súčasne v Bratislave a Košiciach.

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



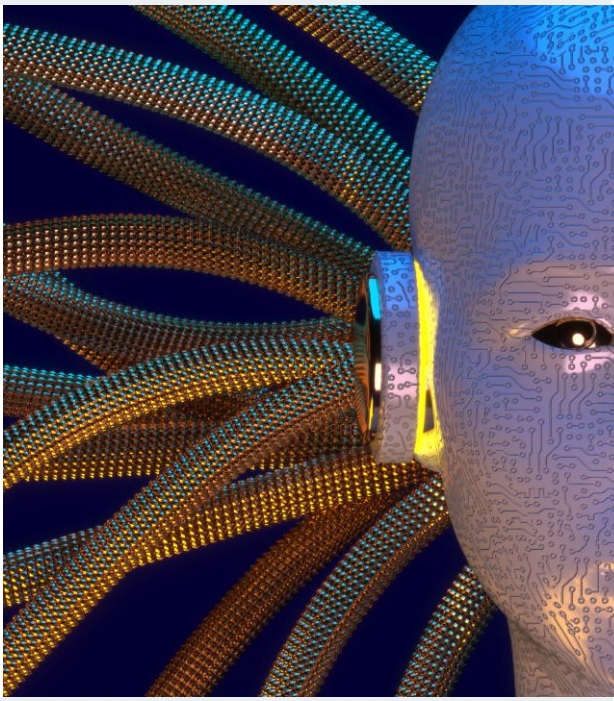
VÝZNAMNÉ UDALOSTI VO SVETE

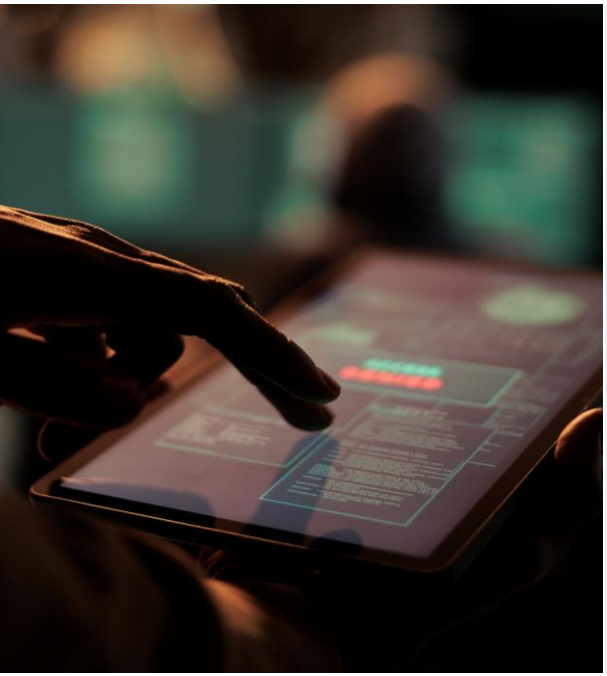
Odolali by ste útoku, ktorý zasiahol Jaguar Land Rover?

VJ CSIRT upozorňuje na kybernetický útok, ktorý zasiahol automobilovú spoločnosť Jaguar Land Rover. Automobilová spoločnosť Jaguar Land Rover informovala v oficiálnom vyhlásení, že čelí kybernetickému útoku a podnikla kroky na obnovenie bežnej produkcie. Britské denníky BBC a The Guardian sa o útoku dozvedeli počas jeho priebehu. Cieľom útočníkov bolo vymáhanie peňazí. Podľa aktuálnych informácií nedošlo k úniku dát zákazníkov, ale útok spôsobil pozastavenie viacerých prevádzok. Aktuálne sa k útoku hlási skupina "Scattered Lapsus$ Hunters", ktorá nebola stotožnená so žiadnou známou APT skupinou.

Útočníci zneužívajú AI GROK na šírenie škodlivých URL na platforme X

GUARDIO LABS zverejnila informácie o novej kampani, v rámci ktorej útočníci zneužívajú model umelej inteligencie GROK na obchádzanie obmedzení na zverejňovanie URL odkazov na platforme X, ktoré spoločnosť zaviedla na obmedzenie škodlivých reklám. Útočníci majú istý stupeň znalostí o internom fungovaní X, pretože samotné URL ukladajú do metadátového poľa "From:", ktoré nie je skenované. Následne pridajú komentár, v ktorom žiadajú GROK o informácie o videu. GROK naparsuje obsah skrytého poľa From a do nového komentára pridá sumarizáciu obsahu a URL linku na škodlivý obsah. Tak obchádza bezpečnostné mechanizmy pre bežné pridávanie odkazov. Výskumníci uvedenú metódu označili ako GROKKING. Uvedený mechanizmus útoku môže byť prítomný aj na ďalších platformách.





Útočníci zneužívajú súbory SVG v rámci phishingových kampaní na šírenie malvéru

Spoločnosť VirusTotal odhalila phishingovú kampaň, v ktorej útočníci ukrývajú škodlivý kód do súborov SVG. Vkladajú do nich JavaScript, ktorý zobrazuje napodobeninu portálu kolumbijského justičného systému, alebo tiež falošný priebeh sťahovania, pričom nútia obete stiahnuť archív ZIP s heslom. Archív obsahuje premenovanú aplikáciu Comodo Dragon a škodlivú knižnicu DLL, ktorá spustení aplikácie nainštaluje malvér. Bežné antivírusy tieto SVG súbory ignorujú, no systém VirusTotal AI Code Insight analyzoval ich správanie a identifikoval vyše 500 škodlivých vzoriek spojených s podobnými kampaňami. Incident poukazuje na riziká SVG dokumentov a taktiež výhody využitia AI pri detekcii malvéru.

VÝZNAMNÉ UDALOSTI VO SVETE

Útok na Salesforce cez kompromitované OAuth tokeny

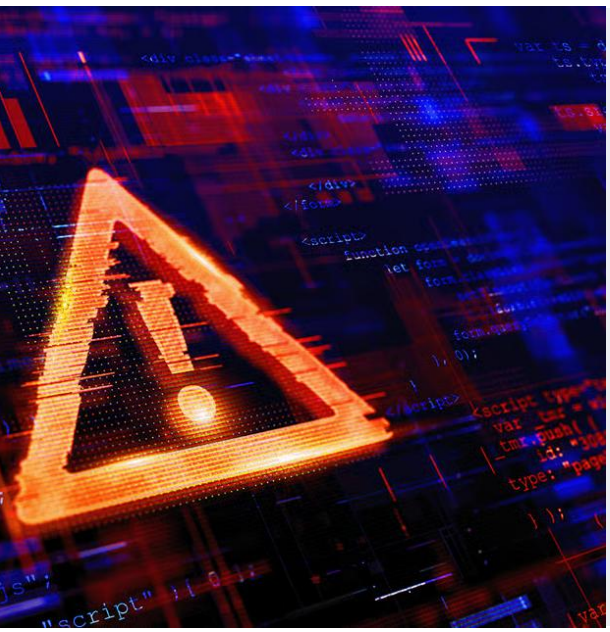
Spoločnosť Cloudflare potvrdila, že útočníci zneužili kompromitované OAuth tokeny spojené s integráciou Salesforce chatovacieho agenta Salesloft Drift, aby mohli exfiltrovať údaje z inštancií Salesforce zákazníkov spoločnosti Salesloft. Získali textové údaje zo zákazníckej podpory vrátane kontaktov, predmetov prípadov a samotných správ, v ktorých zákazníci mohli zdieľať citlivé informácie ako tokeny či konfigurácie. Cloudflare ihneď zrušila všetkých 104 API tokenov, ktoré objavila v ukradnutých dátach, aj keď žiadne neštandardné aktivity nezaznamenala. Následne upozornila zákazníkov, aby si bezodkladne obnovili akékoľvek poverenia, ktoré zdieľali touto cestou. Spoločnosť Salesloft dočasne odstavila službu Drift po tom, čo útočníci zneužili ukradnuté OAuth tokeny na prístup k údajom zákazníkov v Salesforce.

Útok prebiehal od 8. do 18. augusta a zasiahol viac než 700 organizácií, vrátane Cloudflare, Google Workspace, PagerDuty, Palo Alto Networks, SpyCloud, Tanium a Zscaler. Útočníci zneužili zraniteľnosť v integrácii medzi Salesloft a Salesforce a zneužili OAuth tokeny spojené s AI chatbotom Drift na získanie citlivých údajov. Spoločnosť Palo Alto Networks zaznamenala únik dát, keď útočníci zneužili kompromitované OAuth tokeny zo Salesloft Drift na prístup k ich prostrediu Salesforce a získali citlivé informácie z prípadov zákazníckej podpory vrátane kontaktov, hesiel a autentifikačných údajov. Spoločnosť okamžite deaktivovala aplikáciu v Salesforce, útok neovplyvnil žiadne produkty ani systémy Palo Alto Networks a útočníci sa zamerali na získavanie údajov vrátane AWS kľúčov, Snowflake tokenov, prihlasovacích údajov VPN či kľúčových slov ako „heslo“, „tajomstvo“ alebo „kľúč“.

Spoločnosť WORKIVA, uznávaný poskytovateľ cloudových služieb SaaS, potvrdila, že útočníci prenikli do ich inštancie Salesforce a získali údaje zákazníkov. Podľa dostupných informácií dodávateľ CRM informoval Workivu o prieniku cez pripojenú aplikáciu, čo naznačuje súvis s únikom OAuth tokenov zo Salesloft Drift. Spoločnosť upozornila všetky zasiahnuté subjekty a varovala pred možnými spear-phishingovými kampaňami.

Tento incident zdôrazňuje dôležitosť pravidelnej rotácie a ochrany OAuth tokenov, obmedzenia prístupových práv integrácií na nevyhnutné minimum, a potrebu monitorovania a okamžitej reakcie na neštandardnú aktivitu, aby sa minimalizovalo riziko úniku citlivých dát.

VÝZNAMNÉ UDALOSTI VO SVETE

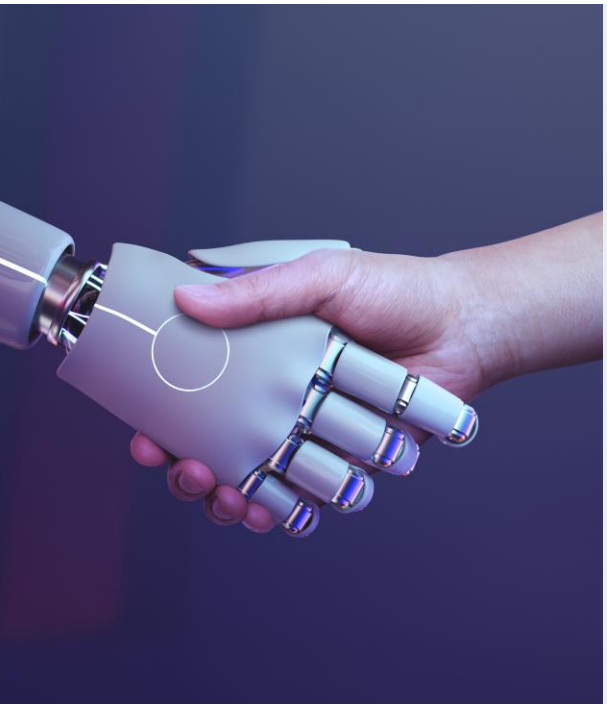


Rozsiahly útok na dodávateľský reťazec viedol ku kompromitácii NPM knižníc kryptodrainerom

Výskumníci z AIKIDO security zverejnili analýzu útoku na dodávateľský reťazec, v rámci ktorého došlo ku kompromitácii vyše 18 populárnych NPM knižníc. Vývojár Josh Junon vystupujúci pod aliasom QIX incident potvrdil a zároveň informoval, že útočníci jeho prihlasovacie údaje získali v rámci phishingovej kampane zneužívajúcej identitu NPM zameranej na vývojárov. Phishingové e-maily rozposielané z domény npmjs[.]help pod hrozbou pozastavenia účtu upozorňovali na potrebu aktualizácie 2FA a obete presmerovávali na phishingový obsah pre ich získanie. V prípade detekcie transakcií v kryptomenách malvér nahrádza cieľové adresy adresami útočníka. Útok postupne prerástol do kompromitácie stoviek ďalších knižníc NPM.

Nový malvér RatOn pre Android cieli na kryptopeňaženky a českú bankovú aplikáciu George

Malvér RatOn pre Android sa vyvinul z nástroja pre útoky typu NFC relay na sofistikovaný trojan s funkciami vzdialeného prístupu a automatizovaného prevodu peňazí. Ciele zahŕňajú používateľov kryptopeňaženiek ako MetaMask, Trust, Blockchain.com a Phantom, aj klientov českej bankovej aplikácie George Česko. Útočníci šíria malvér cez falošné stránky TikTok 18+. Po inštalácii získavajú administrátorské práva a prístup k službám prístupnosti, následne nasadia NFSkate pre útoky NFC relay. RatOn zobrazuje ransomvérové obrazovky a po zadaní PIN kódu získava prístup k citlivým údajom, ako seed frázy, ktoré umožňujú krádež kryptomien.



Slovenské školy sa pripravujú na AI

Ministerstvo školstva SR pripravuje zavedenie umelej inteligencie do školského systému tak, aby sa predišlo chybám z minulosti pri implementácii sociálnych sietí. Minister Tomáš Drucker zdôraznil potrebu dôkladnej prípravy učiteľov a žiakov, pričom nové kurikulum má zahŕňať výučbu AI od školského roku 2026/2027. Plánuje sa intenzívne školenie učiteľov, podpora medzinárodnej spolupráce a lokalizácia existujúcich AI nástrojov pre slovenské školy, vrátane chatbota Amos AI, ktorý bude pomáhať pri vyučovaní a implementácii AI technológií. Cieľom je pripraviť školstvo na rýchly technologický pokrok a zabezpečiť efektívne a zodpovedné využívanie umelej inteligencie. Výrazne to ovplyvní vzdelávanie v oblasti AI na školách v SR.

VÝZNAMNÉ UDALOSTI VO SVETE

Skupina Scattered Lapsus$ Hunters prenikla do systému Google LERS a oznámila koniec aktivity

Spoločnosť Google potvrdila, že útočník si založil falošný účet v portáli pre žiadosti orgánov činných v trestnom konaní (LERS), no rýchlo ho zrušil a nevykonal cez žiadnu aktivitu, ani nezískal dáta. Skupina Scattered Lapsus$ Hunters pritom tvrdí, že získala prístup aj do systému FBI eCheck, čo by umožnilo podvodníkom vydávať sa za políciu a získavať citlivé informácie. Google uisťuje, že žiadny únik dát nenastal a FBI sa k tvrdeniam zatiaľ nevyjadrila. V rámci svojho listu skupina oznámila ukončenie svojej aktivity: „We LAPSUS$, Trihash, Yurosh, yaxsh, WyTroZz, N3z0x, Nitroz, TOXIQUEROOT, Prosox, Pertinax, Kurosh, Clown, IntelBroker, Scattered Spider, Yukari, and among many others, have decided to go dark.“

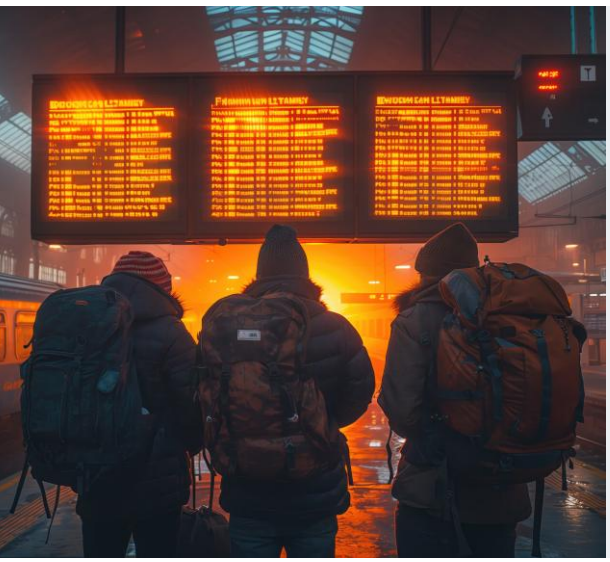
CISA plánuje väčšiu kontrolu nad programom CVE

CISA zverejnila dokument, v ktorom predstavila svoju víziu budúcnosti programu CVE (Common Vulnerabilities and Exposures). Podľa dokumentu CISA plánuje prevziať väčšiu kontrolu nad týmto globálnym štandardom pre identifikáciu zraniteľností. Tento krok prišiel potom, čo CISA takmer nepredĺžila zmluvu s MITRE, ktorá program spravuje. Tiež vyjadrila nesúhlas s návrhom CVE Foundation, neziskovej organizácie, ktorá navrhovala prechod programu na neziskovú entitu s medzinárodnou koordináciou a transparentným riadením. Privatizácia programu by mohla spôsobiť konflikty záujmov, ktoré by uprednostnili hodnotu pre akcionárov pred národnou bezpečnosťou.

Ruské ransomvérové skupiny zneužívajú nový loader COUNTLOADER

Ruské ransomvérové skupiny LockBit, Black Basta, Qilin a ďalšie používajú nový loader CountLoader na nasadzovanie post-exploitačných nástrojov, napríklad Cobalt Strike, AdaptixC2 a trojana PureHVNC RAT. CountLoader existuje v troch verziách, pričom najrozvinutejšia verzia v JavaScripte podporuje šesť metód sťahovania súborov a tri spôsoby spúšťania binárie. Útočníci sa zameriavajú na obete na Ukrajine cez phishingové PDF dokumenty vydávajúce sa za ukrajinskú políciu, nasadzujú implantát BrowserVenom, ktorý presmerováva sieťovú prevádzku cez ich proxy a zbierajú informácie. Loader využíva legitímne nástroje pre Windows ako certutil.exe a bitsadmin, dočasne ukladá škodlivé súbory do priečinka MUSIC (HUDBA) a komunikuje cez viac než 20 unikátnych domén.

VÝZNAMNÉ UDALOSTI VO SVETE



Ransomvérový útok na COLLINS AEROSPACE ochromil viaceré letiska v Európe

Ransomvérový útok na spoločnosť COLLINS AEROSPACE negatívne ovplyvnil viaceré letiská, ktoré využívali ich informačný systém na check-in cestujúcich, tlač boarding passov a označovanie batožiny. Viacero letov na letiskách v Bruseli, Berlíne a Londýne sa oneskorilo alebo bolo zrušených. Najhoršie dopady zaznamenalo letisko Brussels Airport, ktoré muselo zrušiť 25 odletov v sobotu, 50 odletov v nedeľu a 140 odletov v pondelok.

Agentúra ENISA vo vyhlásení pre portál Guardian potvrdila, že za narušením činnosti letísk bol ransomvérový útok na dodávateľa check-in a boarding systémov COLLINS AEROSPACE. Útok ovplyvnil činnosť systému MISE (Multi-User System Environment), ktorý letecké spoločnosti využívajú na zdieľanie informácií o check-in pracoviskách a boarding bránach. Collins Aerospace incident rieši v spolupráci s NCSC UK a príslušnými OČTK.

V nasledujúcich dňoch anglická NCA (National Crime Agency) zadržala osobu podozrivú zo zapojenia do ransomvérového útoku na COLLINS AEROSPACE. Výskumník GOSSITHEDOG na sociálnej sieti informoval, že sa jednalo o ransomvér HARDBIT, zatiaľ čo iné zdroje uvádzajú ransomvér LOKI.

Výskumníci zverejnili analýzu platforiem phishing-as-a-service LUCID a LIGHTHOUSE

Skupina XinXin, známa aj ako LARVA-241, spustila rozsiahlu kampaň phishing-as-a-service (PhaaS) s názvom Lucid, ktorá zahŕňa viac ako 17 500 phishingových domén cieliacich na 316 značiek v 74 krajinách. Tieto domény napodobňujú webové stránky vládnych inštitúcií, finančných a poštových spoločností, ako aj e-commerce platforiem. Lucid umožňuje útočníkom prispôsobiť šablóny phishingových stránok a cieliť na špecifické skupiny používateľov podľa parametrov ako mobilný User-Agent alebo proxy krajina. Skupina Lucid a ďalší PhaaS nástroj Lighthouse, ktorý tiež vyvinula skupina LARVA-241, ponúkajú funkcie sledovania obetí v reálnom čase a prispôsobiteľné šablóny pre viac ako 200 platforiem. Tieto nástroje sa predávajú za ceny od 88 USD na týždeň do 1 588 USD ročne.

VÝZNAMNÉ UDALOSTI VO SVETE

Útočníci integrujú LLM-modely na podporu činnosti malvéru

Výskumníci zo SentinelOne objavili malvér MalTerminal, ktorý využíva schopnosti GPT-4 na generovanie kódu ransomvéru alebo reverzného shellu priamo na zariadení obete. Hoci ho zatiaľ nasadili len v testoch, jeho existencia ukazuje vznik novej kategórie malvéru, LLM-embedded malware. Podobné nástroje ako LameHug (aka PromptSteal) a PromptLock generujú škodlivé príkazy v reálnom čase pomocou LLM. MalTerminal obsahuje zastarané OpenAI API z novembra 2023, binárny súbor pre Windows a skripty v jazyku Python, ktoré používateľovi umožňujú spustiť ransomvér alebo reverzný shellu. Výskumníci tiež vytvorili nástroj FalconShield, ktorý kontroluje skripty v Python a používa GPT na detekciu škodlivého kódu a tvorbu správ o analýze malvéru. Tento výskum prezentovali na konferencii LABScon 2025.

Nová phishingová kampaň zameraná na PyPI kradne prihlasovacie údaje

Spoločnosť Python Software Foundation (PSF) upozornila vývojárov na novú vlnu phishingových útokov, ktoré používajú falošnú webovú stránku imitujúcu Python Package Index (PyPI) na krádež prihlasovacích údajov. Útočníci posielajú e-maily, v ktorých žiadajú používateľov o overenie e-mailovej adresy kvôli údržbe účtu a bezpečnostným procedúram, a hrozia pozastavením účtu, pričom odkazujú na phishingovú stránku na doméne pypi-mirror[.]org. PSF odporúča okamžite zmeniť heslo na PyPI a skontrolovať aktivitu účtu, ak používatelia klikli na odkaz a zadali svoje údaje. Útočníci môžu tieto prihlasovacie údaje použiť na kompromitovanie existujúcich balíčkov Python.

Hackerská skupina zasiahla ministerstvá a sektor obrany na všetkých kontinentoch

Čínska hackerská skupina RedNovember (známa aj ako Storm-2077) od júna 2024 do júla 2025 cielila na vládne a súkromné organizácie po celom svete, vrátane Afriky, Ázie, Severnej a Južnej Ameriky a Oceánie. Útočníci využívali známe zraniteľnosti v internetových zariadeniach ako VPN, firewally a load balancery od firiem Check Point, Cisco, Citrix, F5, Fortinet, Ivanti, Palo Alto Networks a SonicWall na získanie prvotného prístupu. Po infiltrácii nasadili nástroje, ktoré im umožnili udržať prístup a exfiltrovať citlivé údaje. Útoky zasiahli ministerstvá zahraničných vecí v strednej Ázii, štátne bezpečnostné organizácie v Afrike, vládne agentúry v Európe a juhovýchodnej Ázii, ako aj obranných a leteckých dodávateľov v USA.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zero-day zraniteľnosť vo FreePBX bola opravená

Bezpečnostní výskumníci zo Sangoma FreePBX Security Team informovali o kritickej zero-day zraniteľnosti v rozšírenom open-source komunikačnom softvéri FreePBX, využívanom najmä v call centrách. Zraniteľnosť bola označená ako aktívne zneužívaná.

Microsoft v rámci Patch Tuesday opravil dve aktívne zneužívané zraniteľnosti

Spoločnosť Microsoft vydala v septembri 2025 balík opráv pre portfólio svojich produktov opravujúci 81 zraniteľností, z ktorých 8 spoločnosť označila ako kritické. Tieto umožňujú vzdialene vykonávať kód, eskalovať oprávnenia a získať citlivé informácie. Dve zraniteľnosti sú typu zero-day.

Kritická zraniteľnosť v operačnom systéme firewallov WatchGuard Firebox

Spoločnosť WatchGuard vydala bezpečnostné aktualizácie svojich firewallov Firebox, ktoré opravujú kritickú zraniteľnosť operačného systému Fireware OS. CVE-2025-9242 by vzdialený neautentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu.

Google opravil aktívne zneužívanú zero-day zraniteľnosť v prehliadači Chrome

Spoločnosť Google vydala bezpečnostné aktualizácie pre svoj webový prehliadač Chrome, ktoré opravujú 4 vysoko závažné zraniteľnosti, z čoho 1 je označená ako aktívne zneužívaná zero-day. CVE-2025-10585 by vzdialený neautentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritická zraniteľnosť v platforme pre prenos súborov Fortra GoAnyWhere MFT

Spoločnosť Fortra vydala bezpečnostné aktualizácie webového nástroja pre prenos súborov GoAnywhere MFT (Managed File Transfer), ktoré opravujú kritickú zraniteľnosť. CVE-2025-10035 by vzdialený neautentifikovaný útočník mohol zneužiť na injekciu príkazov a získanie úplnej kontroly nad systémom. Zraniteľnosť je aktívne zneužívaná.

Kompromitované balíčky v knižnici NPM šíria malvér

Bezpečnostní výskumníci odhalili nový útok na dodávateľský reťazec v npm registri, ktorý zasiahol stovky balíčkov od rôznych udržiavateľov. Tieto balíčky sa používajú ako súčasti softvéru a webových stránok, od komerčných aplikácií až po open-source projekty, čo znamená, že počet ohrozených produktov nie je možné presne určiť.

Cisco v súvislosti so zero-day zraniteľnosťami odporúča bezodkladnú aktualizáciu firewallov ASA a FTD

Spoločnosť CISCO vydala bezpečnostné aktualizácie, ktoré okrem iného opravujú dve aktívne zneužívané zero-day zraniteľnosti vo firewalloch ASA a FTD. CVE-2025-20362 možno zneužiť na obídenie mechanizmov autentifikácie a CVE-2025-20333 na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom.

SolarWinds vydáva už tretiu aktualizáciu na opravu kritickej zraniteľnosti v Web Help Desk

Spoločnosť SolarWinds vydala bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť v produkte Web Help Desk. CVE-2025-26399 možno zneužiť na vzdialené vykonanie príkazov a získanie úplnej kontroly nad systémom.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Nový firmvér pre zariadenia SonicWall SMA 100 dokáže odstrániť známe rootkity

Spoločnosť SonicWall vydala aktualizáciu firmwaru pre svoje zariadenia série SMA 100, ktorá zavádza pokročilú kontrolu integrity súborov a dokáže identifikovať a odstrániť známe rootkity. Hackerská skupina UNC6148 zneužívala zraniteľnosti webového servera Apache CVE-2024-38475 a SMA 100 CVE-2025-40599 na šírenie rootkitu OVERSTEP.

Zraniteľnosti v Supermicro BMC možno zneužiť na modifikáciu firmvéru

Spoločnosť Supermicro vydala bezpečnostné aktualizácie firmvéru BMC (Baseboard Management Controller), ktoré opravujú dve zraniteľnosti vysokej závažnosti. CVE-2025-7937 a CVE-2025-6198 by vzdialený útočník mohol zneužiť na modifikáciu firmvéru zariadenia a získanie úplnej kontroly nad systémom.

Cisco opravilo aktívne zneužívanú zraniteľnosť operačných systémov IOS a IOS XE

Spoločnosť Cisco vydala bezpečnostné aktualizácie, ktoré opravujú 14 zraniteľností operačných systémov Cisco IOS a IOS XE, z čoho jedna je označená ako aktívne zneužívaná zero-day. CVE-2025-20352 by vzdialený útočník mohol zneužiť na zneprístupnenie služby, vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom.

MESAČNÍK ZRANITEĽNOSTÍ SEPTEMBER 2025

VJ CSIRT pravidelne vydáva mesačný prehľad kritických zraniteľností.

https://csirt.sk/posts/2838.html