CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

MÁJ 2026

TLP: CLEAR

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

1 Skupina TeamPCP kampaňou Mini Shai-Hulud kompromitovala viacero prominentných knižníc

Kampaň Shai-Hulud je pokračujúci kybernetický útok na softvérové dodávateľské reťazce v ekosystéme npm, pri ktorom útočníci kompromitovali legitímne knižnice a prostredníctvom oficiálnych kanálov distribuovali ich škodlivé verzie.

2 Spoločnosť OpenAI predstavila novú kyberbezpečnostnú platformu Daybreak

OpenAI predstavila novú kyberbezpečnostnú platformu Daybreak, ktorá integruje modely GPT-5.5 a agenta Codex Security. Jej hlavným cieľom je detegovať, analyzovať a opravovať zraniteľnosti v softvéri už počas vývoja.

3 Europol s partnermi rozložili First VPN zneužívanú na exfiltráciu dát v rámci ransomvérových útokov

Europol a viaceré európske policajné zložky rozložili VPN službu First VPN, ktorú kyberzločinci využívali na skrývanie identity pri ransomvérových útokoch a krádežiach dát.

4 CERT-In sprísňuje pravidlá aktualizácie verejných systémov s odvolaním sa na AI

Indická vládna agentúra CERT-In nariadila organizáciám opravovať aktívne zneužívané zraniteľnosti na kritických a do internetu vystavených systémoch do 12 hodín od ich odhalenia alebo detekcie útoku.

5 Anthropic sprístupní AI model Claude Mythos cez Claude Code

Anthropic pripravuje širšie sprístupnenie svojho kontroverzného AI modelu Claude Mythos cez nástroj Claude Code.

6 Ruská skupina GreyVibe využíva ChatGPT, Google Gemini a Ideogram AI na phishing a vývoj malvéru

Bezpečnostní výskumníci z WithSecure odhalili skupinu GreyVibe, ktorá od roku 2025 cieli hlavne na ukrajinské organizácie a pri útokoch používa ChatGPT, Gemini či Ideogram AI na generovanie realistických phishingových správ.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci máj 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 phishingových kampaní sa objavili e-maily, ktoré šírili malvér Agent Tesla, ktorý slúži ako trójsky kôň pre vytvorenie vzdialeného prístupu ku infikovanému zariadeniu. Tento malvér bol prvýkrát pozorovaný v roku 2014, no aj dnes sa teší obľube.

Ukázali sa tiež phishingové e-maily súvisiace s minulo-mesačnou kampaňou zneužívajúcou meno Všeobecnej zdravotnej poisťovne. Správy lákali potenciálne obete na preplatok na poistnom, pričom cieľom bolo zbierať osobné údaje a údaje z platobných kariet obetí.

V máji bola v rámci bezpečnostného monitoringu zaznamenaná zaujímavá phishingová kampaň, ktorá smerovala z kompromitovanej tureckej vládnej adresy na rôzne adresy v rámci siete Govnet. Zasiahnutých bolo 26 subjektov verejnej správy. Ani v jednom prípade nebola potvrdená interakcia používateľov s predmetným e-mailom.

Jednotke CSIRT.SK nahlásila v máji organizácia v jej konštituencii bezpečnostný incident týkajúci sa úniku prihlasovacích údajov a požiadala o usmernenie pri jeho riešení. Pod administrátorským účtom, slúžiacim primárne na zálohovanie, útočník hromadne pristupoval v krátkych časových odstupoch ku všetkým heslám uloženým v aplikácii pre manažment hesiel. Organizácia vykonala zmenu hesiel v predmetnej aplikácii pre všetky administrátorské účty, ako aj zmenu ďalších zasiahnutých hesiel a poskytla CSIRT.SK prístupy ku klonu virtuálneho stroja predmetnej aplikácie. Po jeho analýze poskytla jednotka zistenia kto pristupoval k heslám a aké kroky vykonával v predmetnej aplikácii. Poskytla tiež rad opatrení na zamedzenie podobných útokov, vrátane nasadenia MFA do predmetného systému.

V máji prijala jednotka CSIRT.SK od partnera hlásenie kompromitácie jedného zariadenia malvérom v rámci domény jednej slovenskej obce. Kompromitácia viedla k úniku prihlasovacích údajov do všetkých účtov a služieb používaných na infikovanom zariadení. Zoznam uniknutých údajov obsahoval tiež administrátorské prihlasovacie údaje k webovým portálom obce. Obec okamžite zmenila zasiahnuté prihlasovacie údaje, zariadenie preskenovala antimalvérovým riešením a následne preinštalovala operačný systém OS.

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 prebiehalo 5 penetračných testov webových aplikácií. V rámci služby Afrodita prebiehal pravidelný monitoring hrozieb v kybernetickom priestore a zdieľanie indikátorov kompromitácie zo známych kampaní na ochranu vládnej siete Govnet.

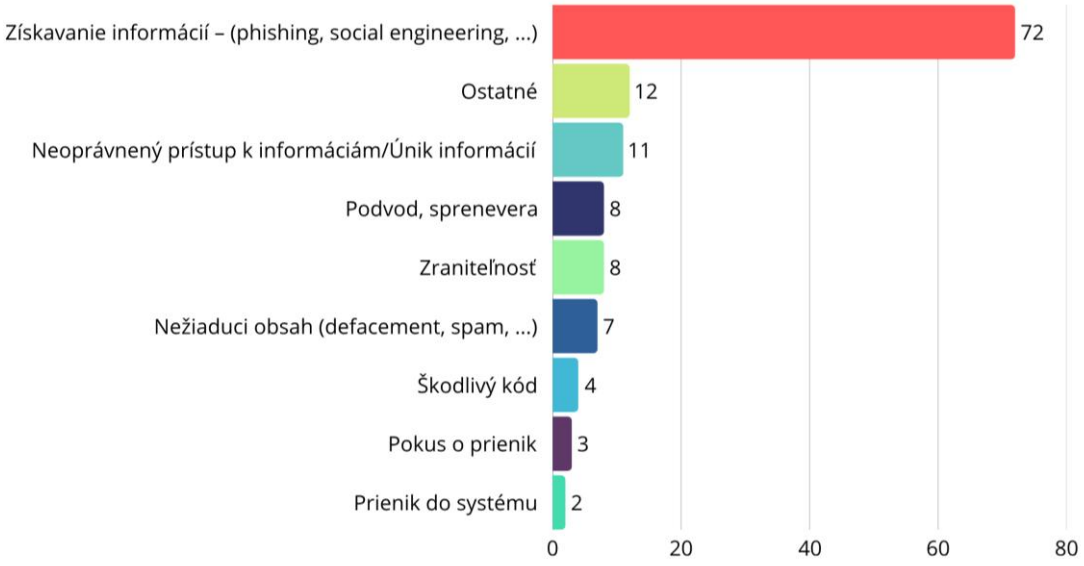
V máji CSIRT.SK plošne varoval svoju konštituenciu ohľadom zraniteľnosti CVE-2026-23918 v Apache HTTP Server, zneužiteľnej na spôsobenie nedostupnosti služby alebo získanie schopnosti vykonávať kód. Varoval aj ohľadne starej kritickej zraniteľnosti v NGINX s identifikátorom CVE-2026-42945. Do tretice informoval o aktívne zneužívanej zraniteľnosti servera Exchange Server 2016, 2019 a Subscription Edition s označením CVE-2026-42897. Jednotka upozornila aj na riziká nahrávania interných e-mailov a iných vzoriek do verejne dostupných online analytických nástrojov, a spôsoby ako tieto nástroje používať bez rizika úniku interných údajov.

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 máji jednotka prezentovala rôzne témy z oblasti kybernetickej bezpečnosti pre zamestnancov Štatistického úradu v Banskej Bystrici a Bratislave, Mestskej časti Petržalka Bratislava a zariadenia Senior Dom Svida vo Svidníku. Študentom prednášala na SOŠ hotelových služieb a obchodu vo Zvolene, Strednej priemyselnej školy v Považskej Bystrici, SOŠ obchodu a služieb J. Bocatia v Košiciach a Hotelovej akadémie v Liptovskom Mikuláši. Prednášku si vypočuli aj učitelia Základnej školy s materskou školou sv.Dominika Savia v Dubnici nad Váhom.

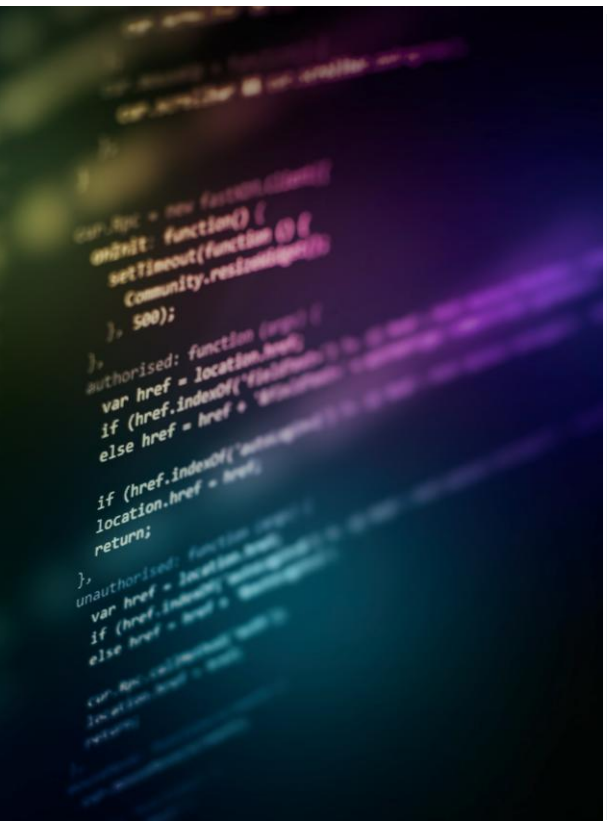
Členovia tímu CSIRT.SK sa v máji aktívne zúčastnili na niekoľkých medzinárodných konferenciách. V Prahe prezentovali služby CSIRT.SK na konferencii Qubit. Vo švédskom Göteborgu sa zúčastnili konferencie Security Fest 2026, kde úspešne prezentovali službu Afrodita MISP. Z konferencie je dostupný záznam. Služba Afrodita vytvára dôveryhodné prostredie pre výmenu informácií o hrozbách v organizovanom formáte. Prácu jednotky CSIRT.SK v rámci Afrodity overili aj tvorcovia nástroja MISP, vývojári z CIRCL.LU, ktorí preverili štruktúru udalostí tvorených pre komunitu prepojených MISPov a potvrdili ich korektnosť a prehľadnosť. MISPovú komunitu CSIRT.SK nájdete na webe https://www.misp-project.org/communities/.

CSIRT.SK však nevynechal ani domáci priestor. Na seminári obcí v Dolnom Kubíne prezentoval informácie o aktuálnych trendoch kybernetických útokov a svoje služby, ktoré môžu organizácie verejnej správy využiť pre pomoc s minimalizáciou rizika alebo odstraňovania ich následkov.

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



VÝZNAMNÉ UDALOSTI VO SVETE



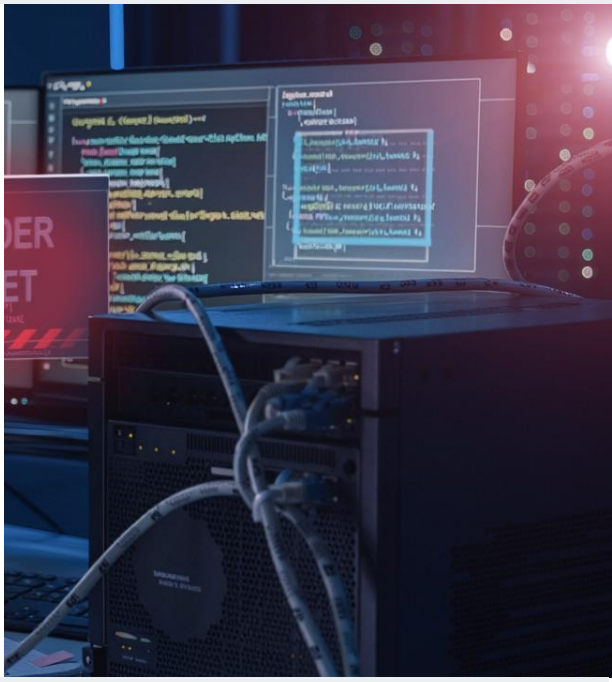
Skupina TeamPCP prostredníctvom kampane Mini Shai-Hulud kompromitovala viacero známych knižníc NPM a PyPI

Kampaň Shai-Hulud je pokračujúci kybernetický útok na softvérové dodávateľské reťazce v ekosystéme npm, pri ktorom útočníci kompromitovali legitímne knižnice a prostredníctvom oficiálnych kanálov distribuovali ich škodlivé verzie, ako napríklad *@tanstack/react-router* alebo balíky od Mistral AI.

Malvér sa šíri útokmi na CI/CD pipeline a zneužíva dôveryhodné publikačné procesy (napr. kompromitáciu identity OIDC a nástroje build runner), takže infikované verzie vyzerajú ako legitímne vydania. Po inštalácii dokáže kradnúť tokeny, poverenia GitHubu (heslá, prístupové tokeny, SSH kľúče, API tokeny), či cloudové kľúče a šíriť sa ďalej do ďalších balíkov. Tak vzniká reťazová infekcia naprieč celým ekosystémom. Celkovo bolo zasiahnutých viac než 170 npm balíkov a desiatky ďalších projektov. **VJ CSIRT vydala na svojom webe varovanie a naďalej sleduje pokračujúcu kyberkampaň.**

TeamPCP kompromituje modul Jenkins Checkmarx a rozširuje útoky na dodávateľský reťazec na CI/CD infraštruktúru

Skupina TeamPCP kompromitovala modul Jenkins Checkmarx a využila ho ako vstupný bod do prostredí CI/CD, čím ohrozila vývojové pipeline viacerých organizácií. Útočníci zneužili zraniteľnosť v integrácii na získanie prístupu k procesom vývoja softvéru (build process). To im umožnilo spustiť škodlivý kód v rámci úloh Jenkins a potenciálne získať prístup k citlivým údajom, ako sú zdrojové kódy, API kľúče či konfiguračné tajomstvá. Incident je klasifikovaný ako útok na dodávateľský reťazec, ktorý poukazuje na riziká dôvery v tretie strany v nástrojoch CI/CD a potrebu dôsledného overovania modulov, aktualizácií a izolácie vývojových prostredí.



Europol s partnermi rozložili First VPN zneužívanú na exfiltráciu dát v rámci ransomvérových útokov

Europol a viaceré európske policajné zložky rozložili VPN službu First VPN, ktorú kyberzločinci využívali na skrývanie identity pri ransomvérových útokoch a krádežiach dát. Počas koordinovanej operácie zaistili jej servery v rôznych krajinách a zadržali administrátora služby. Vyšetrovatelia spojili túto VPN infraštruktúru s viacerými prípadmi kyberkriminality a získané dáta môžu pomôcť identifikovať ďalších používateľov zapojených do útokov.

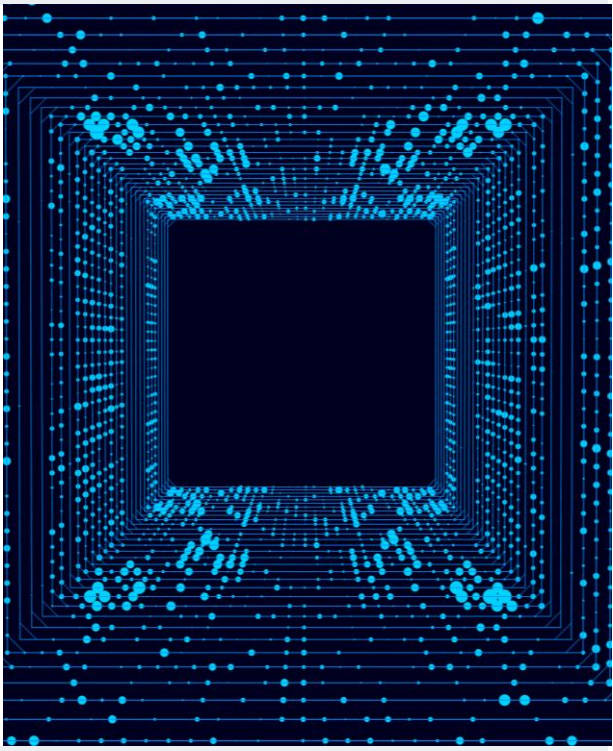
VÝZNAMNÉ UDALOSTI VO SVETE

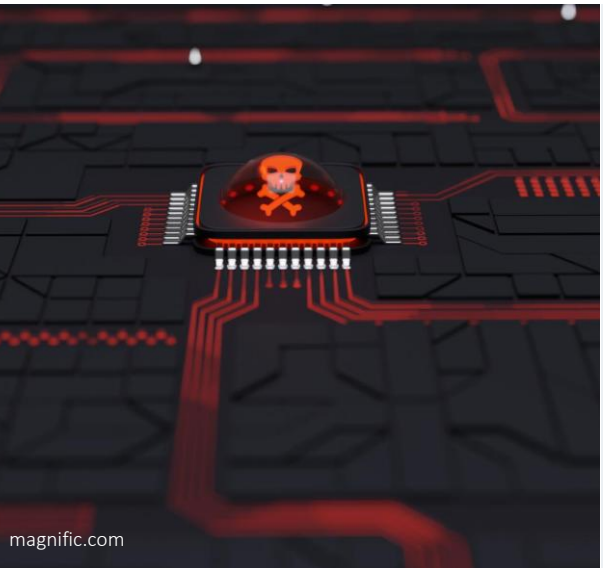
Grafana bola zasiahnutá útokom na dodávateľský reťazec, ktorý realizovala skupina TeamPCP cez NPM knižnicu TanStack

Grafana Labs potvrdila, že nedávny únik z jej prostredia GitHub vznikol kvôli jedinému tokenu GitHub workflow, ktorý nebol správne zrotovaný po známom útoku na dodávateľský reťazec TanStack. Útočníci zo skupiny TeamPCP kompromitovali škodlivé npm balíčky TanStack obsahujúce malvér typu infostealer, ktorý sa spustil v CI/CD prostredí Grafany a ukradol tokeny workflow používané v GitHub Actions. Hoci spoločnosť po odhalení incidentu väčšinu tokenov okamžite zneplatnila, jeden kompromitovaný token zostal aktívny, čo hackerom umožnilo prístup k súkromným repozitárom a stiahnutie časti zdrojového kódu a interných dát.

Útočníci kompromitovali balík pytorch-lightning a zneužili ho v rámci útoku na dodávateľský reťazec na získavanie prihlasovacích údajov

Výskumníci zdokumentovali útok na dodávateľský reťazec populárneho AI frameworku PyTorch Lightning, pri ktorom útočníci kompromitovali jeho balík na PyPI a publikovali škodlivé verzie obsahujúce skrytý kód na krádež prihlasovacích údajov. Nainštalovaný balík automaticky spustí obfuskovaný obsah JavaScript, ktorý zbiera dáta z prehliadačov, premenných prostredia či cloudových služieb a môže zneužiť ukradnuté tokeny pre ďalšie útoky, napríklad cez repozitáre GitHub. Incident odhalený koncom apríla 2026 zasiahol široké spektrum vývojárov, keďže ide o veľmi populárnu knižnicu s miliónmi stiahnutí. Útok potvrdzuje rastúci trend sofistikovaných útokov na open-source ekosystém. Odporúča sa nepoužívať infikované verzie, prejsť na bezpečné vydania a bezodkladne rotovať všetky kompromitované prihlasovacie údaje.





Nové zadné vrátka PamDOORa pre Linux umožňujú perzistentný SSH prístup a exfiltráciu prihlasovacích údajov

Výskumníci odhalili podrobnosti o novom malvéri PamDOORa, ktorý vytvára zadné vrátka v systémoch Linux. Útočníci ho integrujú priamo do Pluggable Authentication Modules (PAM), aby získali skrytý a trvalý prístup cez SSH. Malvér sa spúšťa počas prihlasovania, umožňuje obísť štandardnú autentifikáciu pomocou hesla a zároveň zachytáva prihlasovacie údaje všetkých používateľov, ktorí sa na kompromitovaný systém pripájajú. Aktér vystupujúci pod aliasom Darkworm ho ponúka na predaj na ruskom fóre Rehub.

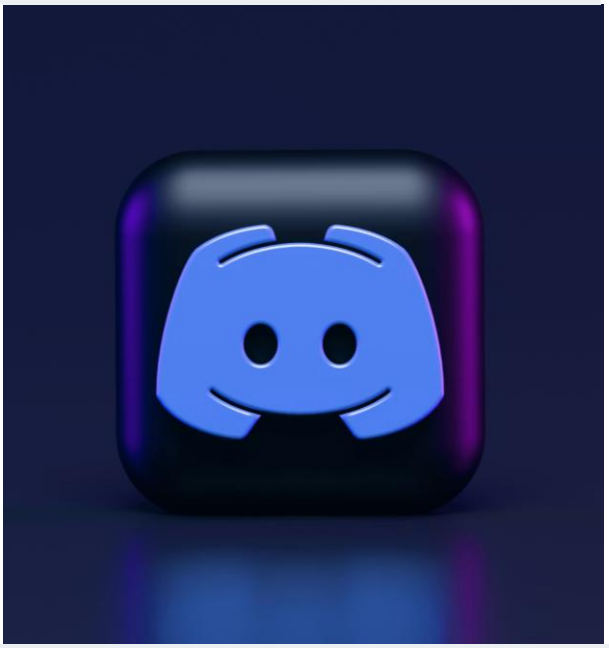
VÝZNAMNÉ UDALOSTI VO SVETE

Výbor pre vnútornú bezpečnosť USA žiada spoločnosť Instructure Holdings o svedectvo v súvislosti s kyberútokmi na platformu Canvas

Americký výbor pre vnútornú bezpečnosť vyzýva vedúcich predstaviteľov spoločnosti Instructure Holdings, Inc. o podanie svedectva k masívnym útokom na platformu Canvas, pri ktorých útočníci zo skupiny ShinyHunters získali prístup k dátam mnohých škôl a univerzít. Vyšetrovatelia sa zameriavajú na spôsob kompromitácie systémov, rozsah úniku dát a reakciu spoločnosti na incident, ktorý ovplyvnil tisíce vzdelávacích inštitúcií a spôsobil výpadky služieb počas skúškového obdobia.

Platforma Discord úspešne dokončila implementáciu end-to-end šifrovania hovorov

Platforma Discord dokončila zavádzanie koncového (end-to-end) šifrovania pre všetky hlasové a videohovory. Výnimkou sú len Stage Channels určené pre verejné vysielanie. Od marca 2026 sú všetky DM hovory, skupinové hovory, hlasové kanály aj streamy Go Live automaticky chránené protokolom DAVE. Vďaka end-to-end šifrovaniu nemá k obsahu komunikácie prístup ani samotný Discord. DAVE je otvorený a auditovaný protokol vyvinutý špeciálne pre multiplatformové prostredie Discordu vrátane desktopu, mobilov, webu, PlayStation, Xboxu a botov. Discord zároveň potvrdil, že zatiaľ neplánuje zaviesť podobné šifrovanie pre textové správy, pretože by to výrazne komplikovalo existujúce funkcie platformy.



Skupina Ghostwriter cieli na ukrajinské vládne inštitúcie cez phishing

Phishingová kyberšpionážna kampaň skupiny Ghostwriter, známej aj ako UNC1151/UAC-0057, cieli na ukrajinské vládne organizácie formou falošných e-mailov a príloh PDF maskovaných ako komunikácia z ukrajinskej online vzdelávacej platformy Prometheus. Po otvorení prílohy obeť stiahne archív ZIP obsahujúci malvér v JavaScript, ktorý vykonáva viacstupňovú infekciu. Zobrazí návnadu, uloží šifrované dáta do registra a stiahne ďalšie komponenty schopné zbierať systémové informácie a komunikovať s riadiacim serverom. Finálnou fázou útoku býva nasadenie nástroja Cobalt Strike. Kampaň je aktívna od jari 2026 a využíva kompromitované účty na zvýšenie dôveryhodnosti. Podľa CERT-UA sa zameriava najmä na vládne, vojenské a ďalšie citlivé inštitúcie v regióne.

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
CSIRT.SK

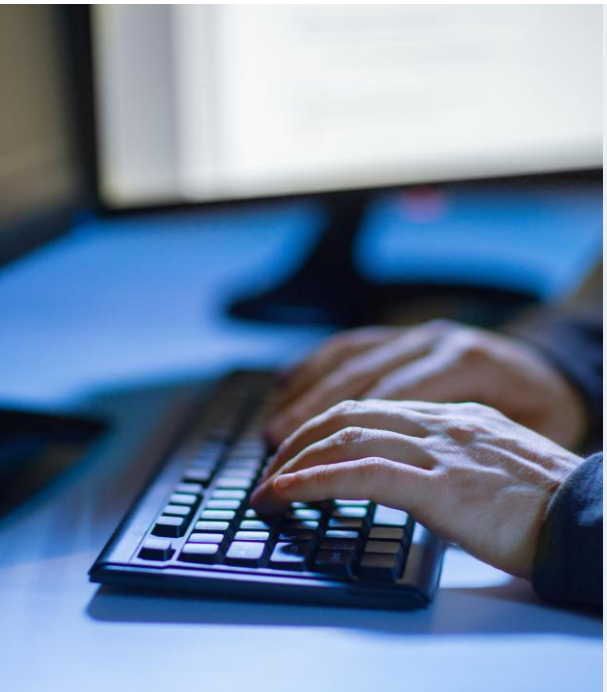
VÝZNAMNÉ UDALOSTI VO SVETE

Spoločnosť OpenAI predstavila model DayBreak špecializovaný na kybernetickú bezpečnosť

OpenAI predstavila novú kyberbezpečnostnú platformu Daybreak, ktorá integruje modely GPT-5.5 a agenta Codex Security, a ktorej hlavným cieľom je detegovať, analyzovať a opravovať zraniteľnosti v softvéri už počas vývoja. Systém automaticky vykonáva modelovanie hrozieb, kontrolu kódu, validáciu opráv a testovanie záplat v izolovaných prostrediach, čím skracuje čas medzi odhalením chyby a jej odstránením. Zároveň zavádza viacúrovňový prístup k modelom, vrátane špecializovaného GPT-5.5-Cyber. Je tak súčasťou širšej iniciatívy OpenAI integrovať umelú inteligenciu priamo do bezpečnostných procesov a konkurovať podobným iniciatívam ako Anthropic Project Glasswing.

Výrobca automobilov Škoda potvrdil kompromitáciu svojho online obchodu a únik citlivých údajov zákazníkov

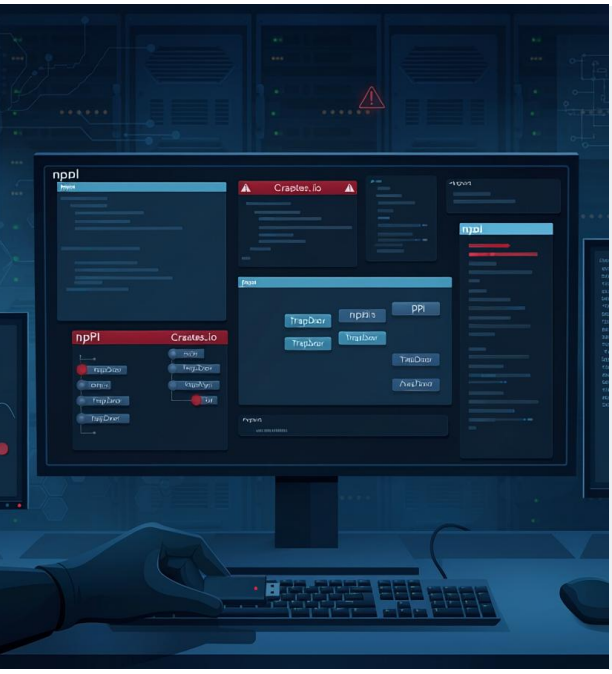
Spoločnosť Škoda Auto potvrdila únik dát zo svojho online obchodu, ktorý sa stal terčom kybernetického útoku. Útočníci zneužili zraniteľnosť softvéru a dostali sa k osobným údajom zákazníkov, predovšetkým k ich menám, adresám, e-mailom, telefónnym kontaktom a detailom objednávok. Spoločnosť informovala, že chybu už odstránila a e-shop dočasne odstavila. Zatiaľ však nie je potvrdené, v akom rozsahu dáta unikli a koľko ľudí bolo zasiahnutých, no spoločnosť varuje pred rizikom phishingu a odporúča zvýšenú obozretnosť.



FBI varuje pred službou Kali365 kradnúcou prístup k účtom Microsoft 365 aj s MFA

FBI varuje pred službou Kali365, ktorá útočníkom umožňuje kradnúť prístup k účtom Microsoft 365 a obchádzať MFA bez potreby získania hesla. Útočníci zneužívajú legitímne overovanie pomocou kódu zariadenia, čo je proces Microsoftu určený pre smart TV a zariadenia IoT. Obeť zadá prihlasovací kód na oficiálnej webovej stránke Microsoftu, kde útočníci následne získajú tokeny Oauth a prístupy k aplikáciám Outlook, Teams, OneDrive či SharePoint. Kali365 ponúka phishingové kampane generované AI, portál na správu útokov aj režim AiTM na kradnutie relačných cookies po MFA autentifikácii. FBI odporúča obmedziť odosielanie prihlasovacích kódov, monitorovať prihlásenia cez OAuth a školiť používateľov o tomto type phishingu.

VÝZNAMNÉ UDALOSTI VO SVETE



Útočníci infikujú balíčky npm, PyPI a Crates.io malvérom TrapDoor na krádež prístupov

Útočníci spustili rozsiahly útok na dodávateľský reťazec, pri ktorom infikujú softvérové balíčky malvérom TrapDoor. Publikovali viac než 34 škodlivých balíčkov naprieč ekosystémami npm, PyPI a Crates.io, s cieľom krádeže cloudových hesiel, SSH kľúčov, kryptopeňaženiek a ďalších developerských tajomstiev. Kampaň cieli najmä na komunity krypto, DeFi, Solana a AI, pričom škodlivé balíčky používajú post-inštalačné skripty, vzdialený obsah a vývojové mechanizmy na spustenie malvéru „trap-core.js“. Tento overuje platnosť tokenov AWS a GitHub, šíri sa cez pripojenia SSH a vytvára perzistenciu pomocou cron jobov, systemd či Git hookov. Útočníci maskujú balíčky za legitímne developerské nástroje a publikujú ich vo vlnách z viacerých účtov, aby zvýšili šancu na ich stiahnutie a znížili detekciu.

Anthropic sprístupní AI model Claude Mythos cez Claude Code

Anthropic pripravuje širšie sprístupnenie svojho kontroverzného AI modelu Claude Mythos cez nástroj Claude Code. Výskumníci objavili v zdrojových kódoch a konfiguráciách Claude Code zmienky o modeli Mythos a prepínače, ktoré naznačujú integráciu tejto doteraz striktne obmedzenej AI. Anthropic predstavil Mythos v apríli 2026 v rámci iniciatívy Project Glasswing ako model špecializovaný na kybernetickú bezpečnosť a vyhľadávanie zraniteľností, pričom spoločnosť upozornila, že model dokáže autonómne vykonávať sofistikované kybernetické útoky a identifikovať kritické chyby v operačných systémoch a webových prehliadačoch.

Ruská skupina GreyVibe zneužíva ChatGPT, Gemini a Ideogram AI na phishing a vývoj malvéru

Bezpečnostní výskumníci z WithSecure odhalili skupinu GreyVibe, ktorá od roku 2025 cieli hlavne na ukrajinské organizácie a pri útokoch využíva ChatGPT, Gemini či Ideogram AI na generovanie realistických phishingových správ, falošných stránok CAPTCHA a podvodných konferencií Zoom. Útočníci pomocou LLM nástrojov vytvorili vlastné obfuskátory a malvér ako LegionRelay či PhantomRelay, ktoré kradnú heslá, súbory, dáta z platforiem Telegram a WhatsApp a vytvárajú vzdialený prístup cez RDP. Výskumníci upozorňujú, že AI zatiaľ nevytvára nové typy útokov. Výrazne však zrýchľuje phishing, vývoj škodlivého kódu a automatizáciu existujúcich techník. Potvrdili to spoločnosti Google a Microsoft vo vlastných správach o zneužívaní Gemini pri štátom sponzorovaných útokoch z Ruska, Číny, Iránu a Severnej Kórey.

VÝZNAMNÉ UDALOSTI VO SVETE

Skupina JINX-0164 útočí na kryptofirmy cez falošných recruiterov a malvér pre macOS

Bezpečnostní výskumníci z Wiz odhalili novú hackerskú skupinu JINX-0164, ktorá od polovice roka 2025 cieli na kryptoburzy, DeFi firmy a vývojárov blockchainových technológií. Využíva pri tom falošných recruiterov na sieti LinkedIn, podvodných videohovorov a vlastného malvéru AUDIOFIX a MiniRAT pre macOS. Útočníci presmerujú obete na klonované stránky pripomínajúce Microsoft Teams alebo Slack, presvedčia ich, aby stiahli falošnú opravu ovládača pre audio a následne kradnú SSH kľúče, heslá, relačné tokeny, kryptopeňaženky a dáta z Discordu, Slacku či Telegramu. Skupina zároveň kompromitovala npm balík @velora-dex/sdk a použila ho pri útoku na dodávateľský reťazec v rámci CI/CD infraštruktúry vývojárov. Wiz upozorňuje, že techniky skupiny pripomínajú severokórejské kampane BlueNoroff alebo UNC1069, no zatiaľ nenašla priame infraštruktúrne prepojenie.

CERT-In sprísňuje pravidlá aktualizácie verejne dostupných systémov do 12 hodín s odvolaním sa na aktuálny stav AI

Indická vládna agentúra CERT-In nariadila organizáciám opravovať aktívne zneužívané zraniteľnosti na kritických a do internetu vystavených systémoch do 12 hodín od ich odhalenia alebo detekcie útoku. Nové pravidlá reagujú na rastúci trend využívania umelej inteligencie pri kyberútokoch, kde útočníci pomocou AI automatizujú vyhľadávanie zraniteľností, tvorbu exploitov aj phishingové kampane. Tým výrazne skracujú čas potrebný na úspešné zneužitie chýb zabezpečenia. CERT-In upozornila najmä na riziká pre štátnu správu, finančný sektor, telekomunikácie, zdravotníctvo a kritickú infraštruktúru.

VÝZNAMNÉ UDALOSTI VO SVETE

- Čínska skupina Silver Fox v rámci phishingovej kampane cielenej na Rusko a Indiu šíri nový malvér ABCDoor.
- Microsoft varuje pred masívnou phishingovou kampaňou zameranou na získavanie prihlasovacích údajov do MS365.
- Iránska APT skupina MuddyWater (Seedworm) nasadzuje ransomvér Chaos za účelom maskovania špionážnych aktivít a sťaženia atribúcie.
- Iránska APT skupina MuddyWater zneužíva legitímne aplikácie Fortemedia a SentinelOne pri nasadzovaní malvéru technikou DLL side-loadingu.
- Nemecká polícia rozložila opätovne spustený kyberkriminálny obchod Crimenetwork.
- Nová verzia iOS 26.5 prináša podporu end-to-end šifrovania RCS správ medzi iOS a Android.
- Špionážna kampaň iránskej APT MuddyWater sa zameriava na vysoko postavené organizácie.
- Grafana potvrdila útok skupiny CoinBaseCartel vedúci k exfiltrácii zdrojového kódu z prostredia GitHub.
- Výskumníci zdokumentovali infraštruktúru Android malvertisingovej kampane Trapdoor.
- Microsoft sprístupnil open-source nástroje RAMPART a Clarity slúžiace na testovanie bezpečnosti AI agentových systémov.
- Čínska skupina Calypso (Red Lamassu) nasadzovala nový malvér Showboat a JFMBackdoor v rámci špionážnej kampane zameranej na telekomunikačných operátorov.
- Spoločnosť Apple zverejnila štatistiky sumarizujúce zneužitie a ochranu App Store za rok 2025.
- Talianska polícia rozložila sieť okolo aplikácie CINEMAGOAL, poskytujúcej prístup na streamovacie platformy.
- Masívny útok na CI/CD Megalodon zasiahol tisíce projektov GitHub.
- Skupina Lazarus nasadila nový fileless malvér RemotePE proti bankám a firmám venujúcim sa kryptomenám.
- Holandská polícia zatkla podozrivého z kompromitácie systémov futbalového klubu AFC Ajax.

- FBI varuje pred ransomvérovou skupinou Silent Ransom Group kombinujúcou phishing s fyzickými návštevami.
- Útočníci zneužívajú AI chatboty na distribúciu cryptojackingového malvéru.
- Rumunský hacker dostal takmer 5 rokov väzenia za predaj prístupu do siete vlády štátu Oregon.
- Microsoft kritizuje zverejňovanie zero-day exploitov po spore s bezpečnostným výskumníkom.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Copy Fail: aktívne zneužívaná zraniteľnosť Linuxového jadra

Jadro operačných systémov Linux obsahuje od roku 2017 vysoko závažnú zraniteľnosť, ktorá umožňuje neprivilegovanému používateľovi zapisovať do pamäte v rámci page cache súborov. Môže tak prepisovať bajty, ktoré definujú jeho oprávnenia, čím môže získať oprávnenia používateľa root. Zraniteľnosť je aktívne zneužívaná.

Zraniteľnosti v Progress MOVEit Automation umožňujú získanie administrátorského prístupu

Spoločnosť Progress Software vydala bezpečnostné aktualizácie nástroja pre spravovaný prenos súborov (MFT), MOVEit Automation, ktoré opravujú jednu kritickú a jednu vysoko závažnú zraniteľnosť. Zraniteľnosti sa nachádzajú v backendových príkazových rozhraniach a umožňujú obídenie autentifikácie a eskaláciu privilégií.

Zraniteľnosť v Apache HTTP Server umožňuje zneprístupnenie služby a vzdialené vykonanie kódu

Apache Software Foundation vydala bezpečnostné aktualizácie, ktoré riešia niekoľko bezpečnostných zraniteľností v Apache HTTP Server, vrátane závažnej zraniteľnosti, ktorá by mohla viesť k vzdialenému vykonaniu kódu.

Zraniteľnosť Cisco CNC a NSO spôsobuje nedostupnosť služby

Spoločnosť Cisco opravila vysoko závažnú zraniteľnosť zariadení Crosswork Network Controller (CNC) a Network Services Orchestrator (NSO), ktorá umožňuje vyčerpať kapacitu sieťových spojení a vyvolať nedostupnosť služby na zraniteľnom zariadení.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritické zraniteľnosti vm2 umožňujú unikať zo sandboxu

Vývojári knižnice vm2 pre Node.js opravili sady kritických zraniteľností, ktoré umožňujú vzdialeným neautorizovaným útočníkom uniknúť zo sandboxu a vykonávať kód v hostiteľskom prostredí.

Aktívne zneužívaná kritická zraniteľnosť Palo Alto Networks PAN-OS umožňuje vykonávať kód ako root

Spoločnosť Palo Alto Networks opravila kritickú aktívne zneužívanú zraniteľnosť v PAN-OS firewallov sérií PA a VM, nakonfigurovaných ako User-ID Authentication Portal. Vzdialený útočník ju môže zneužiť na vykonanie škodlivého kódu s oprávneniami používateľa root.

NGINX Rift: 18 rokov stará zraniteľnosť umožňuje DoS a vzdialené vykonávanie kódu

Vývojári webového servera NGINX opravili 18 rokov starú zraniteľnosť NGINX Rift, ktorá umožňuje vzdialenému neautentifikovanému útočníkovi zaslaním HTTP požiadavky spôsobiť nedostupnosť servera, a tiež mu umožňuje vykonávať kód. Zraniteľnosť je aktívne zneužívaná.

Kritické zraniteľnosti vo Fortinet FortiAuthenticator a FortiSandbox umožňujú vzdialené vykonanie kódu

Spoločnosť Fortinet vydala bezpečnostné aktualizácie, ktoré opravujú dve kritické zraniteľnosti v platformách FortiSandbox a FortiAuthenticator umožňujúce spúšťať príkazy alebo ľubovoľný kód na neopravených systémoch.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritická zraniteľnosť mailových serverov Exim umožňuje poškodenie obsahu pamäte

Spoločnosť Exim vydala bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť v mail serveroch Exim, ktoré využívajú knižnicu GnuTLS. Jej zneužitie môže spôsobiť poškodenie pamäte a umožniť vzdialené vykonanie kódu.

SAP opravili viaceré kritické a vysoko závažné zraniteľnosti

Vývojári Spoločnosť SAP vydala sadu opráv zraniteľností vo viacerých svojich produktoch. Dve z nich sú klasifikované ako kritické a jedna ako vysoko závažná. Umožňujú vzdialene vykonávať kód a príkazy operačného systému, získať prístup k citlivým údajom, alebo spôsobiť nedostupnosť aplikácie.

Kritická zraniteľnosť Drupal umožňuje injektovať príkazy SQL

Vývojári platformy Drupal vydali opravné aktualizácie pre zraniteľnosť, ktorú označili ako vysoko kritickú. Táto chyba zabezpečenia umožňuje neautorizovaným vzdialeným útočníkom zasielať špeciálne vytvorené požiadavky, ktoré zneužívajú nevhodnú sanitizáciu a umožňujú injektovať príkazy SQL.

HP Linux Imaging and Printing Software má dve závažné zraniteľnosti

Vývojári spoločnosti HP opravili jednu kritickú a jednu vysoko závažnú zraniteľnosť v aplikácii HP Linux Imaging and Printing Software. Chyby zabezpečenia umožňujú eskalovať oprávnenia a vykonávať príkazy na hostiteľskom operačnom systéme.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Stará zraniteľnosť jadra Linux umožňuje prevziať kontrolu nad systémom

Jadro operačných systémov Linux obsahuje od roku 2017 vysoko závažnú zraniteľnosť, ktorá umožňuje neprivilegovanému používateľovi zapisovať do pamäte v rámci page cache súborov. Môže tak prepisovať bajty, ktoré definujú jeho oprávnenia, čím môže získať oprávnenia používateľa root. Zraniteľnosť je aktívne zneužívaná.

Cisco Secure Workload má kritickú zraniteľnosť v REST API

Spoločnosť Cisco opravila kritickú zraniteľnosť v produkte Secure Workload, ktorá dovoľuje vzdialeným neautentifikovaným útočníkom prostredníctvom rozhrania REST API získať oprávnenia Site Admin. Útočníci môžu pristupovať k citlivým informáciám a meniť konfiguračné nastavenia.

Aktívne zneužívané zraniteľnosti Microsoft Defender

Spoločnosť Microsoft opravila dve aktívne zneužívané zraniteľnosti vo svojom bezpečnostnom produkte Microsoft Defender. Zraniteľnosti umožňujú lokálnym útočníkom získať oprávnenia na úrovni SYSTEM a spôsobiť nedostupnosť nástroja.

Kritické zraniteľnosti Ubiquiti UniFi OS

Spoločnosť Ubiquiti vydala bezpečnostné aktualizácie pre UniFi OS, ktoré opravujú tri kritické zraniteľnosti CVE-2026-34908, CVE-2026-34909 a CVE-2026-34910. Tieto umožňujú vzdialeným útočníkom bez oprávnení vykonávať neautorizované zmeny v systéme, získať prístup k súborom alebo vykonávať príkazy. Zraniteľnosti ovplyvňujú široké spektrum zariadení vrátane UDM Pro, UDR, UNVR či UniFi OS Server.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľnosť Microsoft SharePoint umožňuje vykonávať kód

Spoločnosť Microsoft vydala bezpečnostné aktualizácie pre vysoko závažnú zraniteľnosť v platforme Microsoft SharePoint, ktorá umožňuje autentifikovaným útočníkom vzdialene vykonávať kód prostredníctvom deserializácie nedôveryhodných dát. Na jej úspešné zneužitie útočníkovi stačí konto s minimálnymi oprávneniami používateľa Site Member.

Zraniteľnosť Gitea umožňuje voľne pristupovať k privátnym kontajnerom

Vysoko závažná zraniteľnosť v open-source platforme Gitea umožňuje neautentifikovaným vzdialeným útočníkom získať prístup k súkromným kontajnerom a obsahu privátnych projektov bez platných oprávnení alebo vytvoreného účtu na platforme.

MESAČNÍK ZRANITEĽNOSTÍ MÁJ 2026

VJ CSIRT pravidelne vydáva mesačný prehľad kritických zraniteľností.

https://csirt.sk/posts/3614.html