CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

OKTÓBER 2025

TLP: WHITE

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

1 Vládna jednotka CSIRT spustila sériu špecializovaných školení pre policajných vyšetrovateľov

Vládna jednotka CSIRT, ktorá patrí pod Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky v spolupráci s odborom počítačovej kriminality a odborom kriminálnej polície Prezídia Policajného zboru, vzdeláva policajtov.

2 Skupina UAC-0245 šíri CABINETRAT cez Signal a škodlivé xll súbory

Ukrajinský CERT-UA zverejnil informácie o ďalšej cielenej kampani skupiny UAC-0245, ktorá prostredníctvom správ šíri na platforme Signal zadné vrátka CABINETRAT.

3 Skupina Scattered Lapsus$ Hunters exfiltrovala citlivé údaje používateľov Discordu

Platforma DISCORD potvrdila, že sa 20. septembra 2025 stala obeťou kybernetického útoku, v rámci ktorého došlo ku kompromitácii a exfiltrácii údajov zo systémov dodávateľa zákazníckej podpory.

4 Z portálu MySonicWall unikli cloudové zálohy konfigurácie firewallov používateľov

Spoločnosť SonicWall 17. septembra 2025 oznámila, že útočníci prenikli do jej cloudovej služby mysonicwall.com a získali zálohy konfigurácií firewallov všetkých používateľov, ktorí využívali funkciu Cloud Backup.

5 Phishingová kampaň cielená na používateľov manažérov hesiel LastPass a Bitwarden

Prebiehajúca phishingová kampaň cieli na používateľov správcu hesiel LastPass a Bitwarden. Útočníci rozosielajú falošné e-maily, ktoré tvrdia, že spoločnosti boli hacknuté, a vyzývajú príjemcov, aby si stiahli údajne bezpečnejšiu desktopovú verziu správcu hesiel.

6 14-hodinový výpadok AWS spôsobila chyba DNS služby DynamoDB

Spoločnosť Amazon oznámila, že rozsiahly výpadok AWS (Amazon Web Services) v regióne US-EAST-1, ktorý trval viac než 14 hodín, bol spôsobený závažnou chybou DNS v službe DynamoDB.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

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

Rumunský kyberbezpečnostný tím DNSC informoval CSIRT.SK o kompromitovanom e-mailovom účte patriacemu slovenskej škole, ktorý bol zapojený do phishingového kybernetického incidentu a požiadal nás o pomoc pri riešení tohto incidentu. Jednotka po analýze poskytnutých dát kontaktovala zástupcu zasiahnutej školy a informovala ho o možnej kompromitácii. Poskytla tiež informácie potrebné pre vykonanie opatrení a krokov na zamedzenie ďalšej škodlivej aktivity.

Vládna jednotka zaznamenala rozsiahlu phishingovú kampaň imitujúcu Prima Banku. Podvodná správa informovala potenciálne obete o potrebe aktualizácie telefónneho čísla. Odkaz v e-maile smeroval na hosting AWS S3. Kampaň smerovala na cca 200 používateľských kont v rámci zasiahnutej organizácie. 90 percent škodlivých e-mailov však zachytili bezpečnostné systémy a neboli doručené. Jednotka o prebiehajúcej kampani informovala aj Prima Banku.

CSIRT.SK prijala od organizácie vo svojej konštituencii hlásenie detekcie komunikácie C&C a požiadavku o asistenciu pri incidente. Pri identifikácii zdrojového zariadenia sa zistilo, že škodlivá požiadavka bola zaznamenaná pri kliknutí na odkaz inej organizácie z verejného sektora. Na základe ďalšej analýzy sa preukázalo, že webstránka tejto organizácie bol kompromitovaná a priamo v kóde HTML obsahuje odkazy na problémový obsah.

CSIRT.SK v októbri prijala od partnera aj hlásenie DNS dopytu na doménu, ktorá mala súvis s ťažobným poolom Monera. Jednotka preverovala hlásenie a identifikovala zdroj komunikácie v príslušnej organizácii. Označenú organizáciu požiadala o vykonanie kontroly zariadenia na prítomnosť škodlivého kódu, aby sa zamedzilo potenciálnym bezpečnostným hrozbám.

Vládna jednotka CSIRT zachytila kompromitáciu malvérom Rhadamanthys vo viacerých organizáciách verejnej správy, ktoré o nálezoch informovala formou varovaní. Jedná sa o modulárny infostealer, ktorý sa špecializuje na exfiltráciu údajov z webových prehliadačov (heslá, cache...) a ďalších aplikácií (email, VPN, chat, password managers, 2FA...), krypto peňaženiek a dokumentov. Extrahované dáta a súbory posiela na C&C server. Malvér dokáže detegovať sandboxy a iné analytické prostredia, v ktorých svoju aktivitu limituje. Indikátory kompromitácie jednotka bezodkladne sprístupnila v službe Afrodita (MISP).

VJ CSIRT v rámci spolupráce s SK-CERT poskytla krátku analýzu hrozieb zachyteného kybernetického bezpečnostného incidentu v súkromnom sektore, s cieľom zabrániť presahu do sektora verejnej správy. Zasiahnutá spoločnosť sa stala obeťou ransomvérového útoku, za ktorým stála skupina Kairos. Táto sa zameriava na exfiltráciu citlivých dát a následné vydieranie obete pod hrozbou ich zverejnenia. Skupina tvrdí, že získala stovky GB citlivých údajov, vrátane obchodných, prevádzkových a osobných informácií. Tento incident zdôrazňuje rastúcu potrebu proaktívnej kybernetickej obrany, najmä v sektoroch s citlivými alebo regulovanými údajmi.

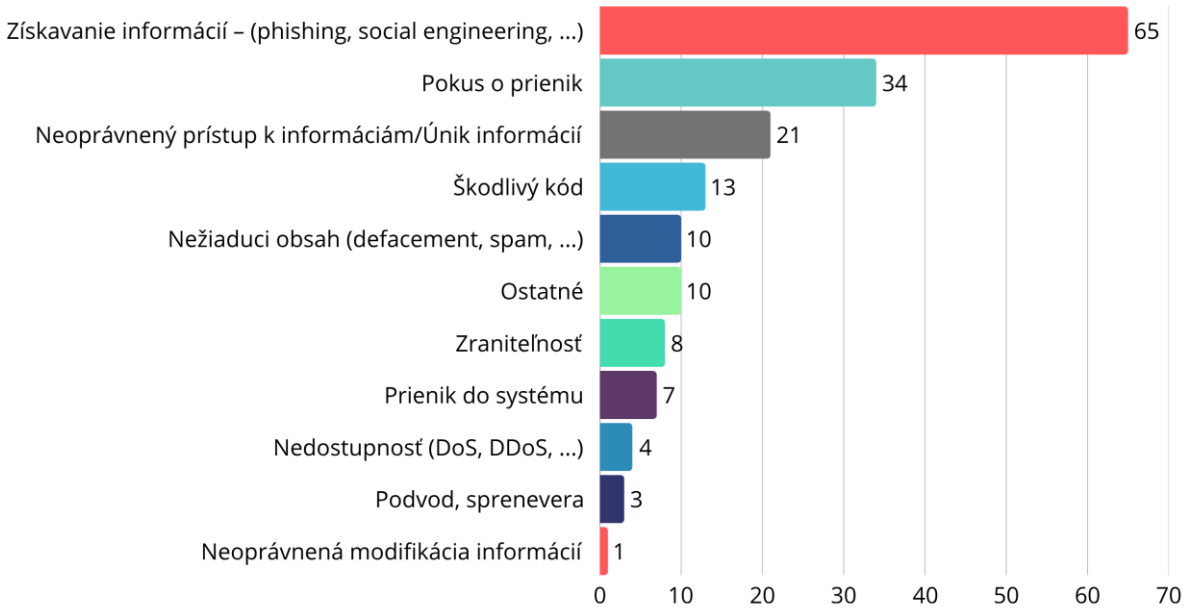
V rámci svojej proaktívnej činnosti jednotka CSIRT.SK vykonáva pravidelné skenovanie a overovanie zraniteľností v službách a zariadeniach IT infraštruktúr organizácií vo svojej konštituencii, ktoré sú vystavené do internetu. Využíva k tomu platformu Achilles, ktorú sama vyvíja a prevádzkuje. Systém Achilles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

V októbri CSIRT.SK plošne varovala svoju konštituenciu ohľadom zraniteľností produktov BIG-IP, F5OS, BIG-IP NEXT FOR KUBERNETES, BIG-IQ a APM klient spoločnosti F5. Informácie o zraniteľnostiach unikli spoločnosti po kompromitácii jej systémov a úniku citlivých interných informácií. O prípade sme písali tu. Jednotka varovala aj pre kampaňou šíriacou malvér Rhadamanthys, pričom poskytla indikátory kompromitácie.

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 októbri jednotka prezentovala rôzne témy z oblasti kybernetickej bezpečnosti pre zamestnancov Úradu jadrového dozoru SR a študentov SOŠ pedagogickej v Modre, SOŠ DSA v Trnave, Inštitútu pre pracovnú rehabilitáciu občanov so zdravotným postihnutím v Bratislave, Gymnázia Školská 7 v Spišskej Novej Vsi a Gymnázia Košických Mučeníkov v rámci akcie CyberSecurity Day. Pre žiakov 9. ročníka ZŠ prednášali členovia tímu CSIRT.SK na podujatí Knižnice Ružinov v Bratislave, organizovanom v rámci októbra, mesiaca kybernetickej bezpečnosti.

V októbri predstavili členovia VJ CSIRT proaktívne služby Achilles, Afrodita a Ares a výsledky, ktoré s ich pomocou jednotka dosahuje, na medzinárodnej konferencii HACK.LU v Luxemburgu. Stretli sa s veľmi pozitívnymi ohlasmi.

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



VÝZNAMNÉ UDALOSTI VO SVETE

VJ CSIRT spustila sériu špecializovaných školení pre policajných vyšetrovateľov: Spoločne posilňujeme obranu proti kyberkriminalite

Vládna jednotka CSIRT, ktorá patrí pod Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky v spolupráci s odborom počítačovej kriminality a odborom kriminálnej polície Prezídia Policajného zboru, vzdeláva policajtov. Zaisťovanie digitálnych stôp bolo prvou témou školenia pre policajných vyšetrovateľov a operatívcov z celého Slovenska, ktoré zorganizovala Vládna jednotka CSIRT súčasne v Bratislave a Košiciach.

Na podujatí sa celkovo zúčastnilo 30 príslušníkov Policajného zboru, ktorí čelia výzvam kybernetickej kriminality v prvej línii. Odborné školenie slávnostne otvoril štátny tajomník MIRRI SR pre informatizáciu Radoslav Štefánek, ktorý vo svojom príhovore zdôraznil kľúčový význam spolupráce a zdieľania informácií medzi štátom a bezpečnostnými zložkami. Vyzdvihol tiež ochotu a pripravenosť Vládnej jednotky CSIRT aktívne pomáhať orgánom činným v trestnom konaní, a to formou konzultácií, technickej súčinnosti pri zaisťovaní digitálnych dôkazov, OSINT analýz, forenzných šetrení či analýz hardvéru v našom špecializovanom chip-off laboratóriu.

Google zavádza povinné overovanie identity vývojárov a F-Droid upozorňuje že tým ohrozuje nezávislé repozitáre pre Android

Nezávislý katalóg aplikácií pre Android F-Droid má v súvislosti so zavedením nových bezpečnostných požiadaviek na vývojárov aplikácií pre Android obavy o svoju existenciu. Spoločnosť Google zavádza povinné overovanie identity vývojárov Android a na zariadeniach povolí inštaláciu aplikácií len od overených vývojárov. F-Droid distribuuje open source aplikácie vyvíjané priamo z oficiálnych repozitárov zdrojového kódu a implementuje viacero bezpečnostných mechanizmov. Vzhľadom na to, že uvedené zmeny môžu ovplyvniť viacero katalógov aplikácií Android, F-Droid vyzýva regulátorov a samotných vývojárov o preskúmanie právneho podkladu zavedenia povinného overovania identity. Google naopak argumentuje zvýšením bezpečnosti ekosystému Android.

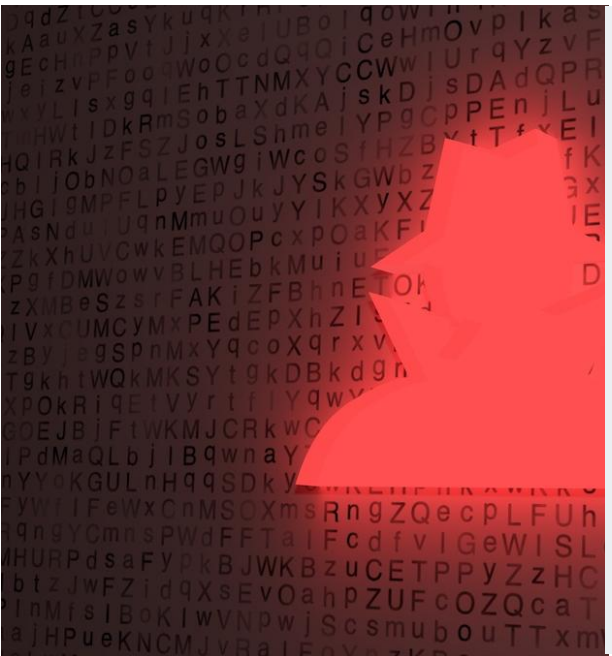
VÝZNAMNÉ UDALOSTI VO SVETE

Spoločnosti častejšie zatajujú, že sa stali obeťami kybernetických útokov

Spoločnosť Bitdefender zverejnila analýzu aktuálnych problémov v oblasti kybernetickej bezpečnosti. Zaujímavý je zvyšujúci sa trend snahy obetí o zatajenie kybernetického incidentu, ktorý môžeme pozorovať aj v rámci SR. Na základe opakovaných diskusií, ktoré Národný bezpečnostný úrad (NBU) realizoval s odbornou komunitou, majú regulované subjekty obavu z hlásenia kybernetických incidentov a odvolávajú sa na hrozbu udelenia pokút alebo poškodenia reputácie. Realita je však presne opačná a zatajenie kybernetického incidentu môže mať ešte významnejšie dopady ako samotný incident.

Skupina UAC-0245 šíri CABINETRAT cez Signal a škodlivé XLL súbory

Ukrajinský CERT-UA zverejnil informácie o ďalšej cielenej kampani skupiny UAC-0245, ktorá prostredníctvom správ šíri na platforme Signal zadné vrátka CABINETRAT. Komunikácia tematicky informuje o zadržaní osôb pokúšajúcich sa o prekročenie ukrajinských hraníc a útočníci v nej obetiam zasielajú archívy ZIP obsahujúce súbory XLL. Škodlivé XLL po spustení na zariadení obete vytvoria EXE súbor v priečinku Startup, ďalší súbor XLL a obrázok Office.png. Doplnok XLL z obrázka extrahuje shellkód CABINETRAT. Payload XLL aj shellkód obsahujú techniky pre detekciu spustenia vo virtualizovanom a detonačnom prostredí, ktoré kontrolujú počet procesorových jadier, veľkosť RAM a prítomnosť nástrojov VMware, VirtualBox, Xen, QEMU, Parallels a Hyper-V. Využitie týchto mechanizmov poukazuje na zvyšujúce sa kvalitatívne nároky na detonačné platformy, ktoré musia dokázať maskovať využitie virtualizácie.



Spoločnosť RED HAT sa stala obeťou kybernetického útoku

Spoločnosť Red Hat potvrdila, že sa stala obeťou kybernetického útoku, pri ktorom útočníci exfiltrovali 570 GB dát z jednej z inštancií GitLab patriacej Red Hat Consulting. Dáta obsahujú približne 28 000 interných repozitárov a okolo 800 CER (Customer Engagement Reports), ktoré môžu obsahovať citlivé údaje ako prihlasovacie údaje alebo schémy infraštruktúry. K útoku sa pred dvoma týždňami prihlásila skupina Crimson Collective. Zoznam súborov zahŕňa názvy veľkých spoločností ako Bank of America, T Mobile, AT&T či US Navy Naval Surface Warfare Center. Útočníci mali z CER získať aj autentifikačné tokeny a URI, ktoré zneužili na kompromitáciu infraštruktúry jedného zo zákazníkov. Skupina sa prihlásila aj k defacementu stránky Nintendo.

VÝZNAMNÉ UDALOSTI VO SVETE

Skupina SCATTERED LAPSUS$ HUNTERS exfiltrovala citlivé údaje používateľov Discordu

Platforma DISCORD potvrdila, že sa stala obeťou kybernetického útoku, v rámci ktorého došlo ku kompromitácii a exfiltrácii údajov zo systémov dodávateľa zákazníckej podpory. Tikety z komunikácie so zákazníckou podporou alebo Trust and Safety tímom obsahujú aj citlivé osobné údaje, platobné údaje či fotokópie oficiálnych dokladov totožnosti. K útoku sa prihlásila skupina SCATTERED LAPSUS$ HUNTERS, ktorá potvrdila kompromitáciu inštancie Zendesk a pod hrozbou zverejnenia dát vyžadovala výkupné. Zverejnený bol screenshot ukazujúci access list zo služby Kolide, ktorý obsahuje zoznam zamestnancov Discord s prístupom k administrátorskej konzole. Výskumníci z Hudson Rock poukazujú, že vzhľadom na nízku úroveň operatívneho zabezpečenia viacerých hackerov zneužívajúcich Discord by tento únik mohol mať aj vysokú analytickú hodnotu z hľadiska identifikácie útočníkov.

Nový variant ClickFix zneužíva na doručenie malvéru Cache Smuggling v prehliadači

Útočníci vyvinuli novú variantu ClickFix, ktorá pomocou techniky Cache Smuggling maskuje škodlivý ZIP ako obrázok v pamäti cache prehliadača, a potom donúti používateľa vložiť upravenú cestu do panela Prieskumníka, pričom skrytý príkaz PowerShell automaticky skopíruje cache Chrome do lokálneho priečinka, vyextrahuje ZIP a spustí škodlivý spustiteľný súbor. Tým obchádza bežné kontroly, lebo nesťahuje žiaden obsah priamo cez skript. Výskumník P4nd3m1cb0y a správa spoločnosti Expel popisujú, že útok sa vydáva napr. za Fortinet VPN Compliance Checker. Techniku rýchlo začali využívať ransomvérové skupiny a autori ClickFix zautomatizovali tvorbu týchto podvodných stránok.

Z portálu MySonicWall unikli cloudové zálohy konfigurácie firewallov všetkých používateľov

Spoločnosť SonicWall 17. septembra 2025 oznámila, že útočníci prenikli do jej cloudovej služby mysonicwall.com a získali zálohy konfigurácií firewallov všetkých používateľov, ktorí využívali funkciu Cloud Backup. Tieto súbory obsahujú šifrované poverenia a konfiguračné údaje, ktoré môžu výrazne uľahčiť zneužitie firewallov. SonicWall odporúča administrátorom zmeniť všetky poverenia vrátane hesiel lokálnych používateľov, API kľúčov, autentifikačných tokenov, VPN účtov a služieb. Zákazníci môžu skontrolovať, či sú ich zariadenia ovplyvnené, prihlásením na portál MySonicWall a prechodom do sekcie 'Product Management → Issue List'.

VÝZNAMNÉ UDALOSTI VO SVETE

OpenAI zablokovala kontá ChatGPT asociované s činnosťou hackerských skupín

OpenAI deaktivovala používateľské kontá ChatGPT, ktoré boli zneužívané ruskými, severokórejskými a čínskymi hackermi. Ruské skupiny AI zneužívali na vývoj a vylepšovanie škodlivých nástrojov RAT, infostealerov a komponentov pre post-exploitatívne operácie a exfiltráciu citlivých údajov. Analýza promptov odhalila, že sa v skupine nachádzajú útočníci s rôznou úrovňou technických vedomostí. Severokórejské skupiny ChatGPT zneužívali na vývoj riadiacej infraštruktúry, rozšírenia macOS Finder, konfiguračné súbory pre Windows Server VPN, konverziu rozšírení pre Chrome na Safari, tvorbu phishingových e-mailov a vyhľadávanie nových techník distribúcie malvéru. Čínski hackeri AI zneužívali na generovanie obsahu v rôznych jazykoch, zefektívňovanie používaných nástrojov, inštaláciu skenovacích nástrojov Nuclei a FScan. Ďalšie skupiny zneužívali AI na identifikáciu ľudí, vývoj nástrojov pre sledovanie ľudí, generovanie deepfake obsahu a príspevkov na šírenie dezinformácií. OpenAI upozornila na nový trend, kedy útočníci začínajú odstraňovať dôkazy implikujúce, že ide o výstupy AI. Zaujímavé je, že OpenAI dokáže pristupovať k používateľským promptom.

Španielske OČTK rozložili hackerskú skupinu GXC TEAM

Španielska Guardia Civil rozložila kyberzločineckú skupinu GXC TEAM a zatkla jej vodcu, 25-ročného Brazílčana prezývaného GoogleXcoder. Skupina ponúkala služby typu crime-as-a-service – predávala phishingové nástroje s podporou umelej inteligencie, malvér pre Android a systémy na hlasové podvody, ktoré používali útočníci v krajinách vrátane Španielska, Slovenska, USA či Brazílie. Polícia zaistila zariadenia so zdrojovým kódom týchto nástrojov, komunikáciu s klientmi aj ukradnuté kryptomeny, a zároveň odstránila Telegramové kanály, cez ktoré GXC Team propagovala svoje služby.

Taiwan zaznamenal nárast aktivít Číny v kybernetickom priestore

Taiwanský úrad pre národnú bezpečnosť NSB (National Security Bureau) upozornil na nárast kybernetických útokov na vládny sektor zo strany ČÍNY. Rovnako upozornil aj na vplyvové operácie a aktivity súvisiace so šírením dezinformácií, ktorých cieľom je narušiť dôveru obyvateľov vo vládu a naštrbiť diplomatické vzťahy s USA.

VÝZNAMNÉ UDALOSTI VO SVETE

Phishingová kampaň cielená na používateľov manažérov hesiel LastPass a BitWarden

Prebiehajúca phishingová kampaň cieli na používateľov správcu hesiel LastPass a Bitwarden. Útočníci rozosielajú falošné e-maily, ktoré tvrdia, že spoločnosti boli hacknuté, a vyzývajú príjemcov, aby si stiahli údajne bezpečnejšiu desktopovú verziu. Tieto správy obsahujú odkazy na škodlivé súbory, ktoré po stiahnutí inštalujú nástroj Syncro, používaný poskytovateľmi správy IT služieb. Syncro následne nasadzuje vzdialený prístupový nástroj ScreenConnect, čo útočníkom umožňuje prevziať kontrolu nad zariadením obete. Spoločnosti LastPass a Bitwarden potvrdili, že neboli obeťami kybernetického útoku a že tieto e-maily sú pokusom o sociálne inžinierstvo. Používatelia manažérov hesiel by mali byť obozretní, podobné upozornenia vždy overovať na legitímnych stránkach výrobcu a nikdy neposkytovať kritické heslá a tajné hodnoty.

Microsoft zakázal automatické náhľady stiahnutých súborov v aplikácii File Explorer

Microsoft v rámci zvyšovania bezpečnosti svojich používateľov zakázal zobrazovanie automatických náhľadov stiahnutých súborov vo File Explorer. V prípade pokusu o zobrazenie náhľadu súborov zobrazovaných na Internet Zone a súborov s príznakom MotW (Mark of the Web) aplikácia zobrazí upozornenie na možnú prítomnosť škodlivého obsahu. Uvedený krok má primárne mitigovať zneužitie zraniteľností slúžiacich na získavanie NTLM hashov, ktoré zneužívali špeciálne HTML tagy vykresľované pri náhľade. Funkciu je na dôveryhodných súboroch možné opätovne spustiť kliknutím na tlačidlo Unblock vo vlastnostiach súboru zobrazených po pravom kliknutí myšou.

Zlyhanie DNS spôsobilo masívnu nedostupnosť Microsoft Azure, 365, Purview a Intune

Spoločnosť Microsoft zaznamenala zlyhanie DNS služieb, ktoré spôsobilo nedostupnosť služieb na báze Microsoft Azure, Microsoft 365, Microsoft Purview a Microsoft Intune. Pretože je Azure základom virtuálnej infraštruktúry viacerých projektov a spoločností, výpadky mali negatívne dopady na fungovanie základných služieb až po služby kritickej infraštruktúry. Problémy s prihlasovaním do podnikových sietí a online platforiem hlásili subjekty zo sektorov ako zdravotníctvo alebo doprava. Príčinou problému bola nesprávna konfigurácia AFD (Azure Front Door), ktorá bola odstránená spätnou migráciou na poslednú správnu konfiguráciu. Microsoft zaviedol dodatočné bezpečnostné opatrenia.

VÝZNAMNÉ UDALOSTI VO SVETE

Výskumníci zaznamenali masívny nárast výskytu malvéru pre NFC relay na Android

Spoločnosť Zimperium odhalila vyše 760 škodlivých aplikácií pre Android, ktoré šíria malvér spojený s útokmi typu NFC relay. Kampaň odhaľuje masívne rozšírenie tohto typu mobilného malvéru v Rusku, Bielorusku, Poľsku, Česku, Slovensku, Holandsku, Brazílii a USA. NFC a Android HCE (Host Card Emulation) zneužívajú na emuláciu a exfiltráciu bezkontaktných kreditných kariet a platobných dát a vyskytujú sa v mnohých formách. Niektoré zaznamenávajú EMV polia, ktoré preposielajú do Telegramových kanálov, sady „relay toolkit“ preposielajú APDU príkazy POS terminálov na vzdialené spárované zariadenia, technikou ghost-tap manipulujú HCE odpovede na autorizáciu transakcií cez POS. Špecifické postavenie majú progresívne webové aplikácie (PWA) a falošné bankové aplikácie, ktoré sa registrujú ako predvolená platobná aplikácia. Výskumníci identifikovali vyše 70 riadiacich serverov, centier pre distribúciu škodlivých aplikácií a veľké množstvo telegramových botov a kanálov. Používatelia zariadení Android by mali inštalovať výhradne aplikácie z oficiálnych obchodov ako Google Play a pri inštalácii aplikáciám udeľovať minimálne oprávnenia potrebné pre ich fungovanie.

Spearphishingová kampaň cielená na vládne organizácie a poskytovateľov humanitárnej pomoci na Ukrajine

Sentinellabs zverejnili informácie o spearphishingovej kampani cielené na ukrajinskú štátnu správu a humanitárne organizácie ako Červený Kríž, UNICEF a ďalšie neziskové organizácie vykonávajúce aktivity na zmiernenie dopadov vojny. E-mailové správy v rámci kampane PhantomCAPTCHA zneužívali identitu úradu prezidenta a obsahovali PDF dokumenty s URL odkazom napodobňujúcim komunikačnú platformu Zoom. Phishingová stránka imitovala overovanie Cloudflare CAPTCHA a prostredníctvom techniky ClickFix sa snažili zariadenia obete infikovať malvérom typu RAT (Remote Access Trojan). Cez WebSocket vykonávala identifikáciu návštevníkov. Jednu skupinu presmerovávala na stiahnutie legitímneho inštalátora Zoom a ďalšie na inštrukcie ClickFix pre spustenie príkazu PowerShell. Skripty sťahovali payload pre fingerprinting zariadenia obete, zber systémových údajov a inštaláciu RAT, ktorý taktiež komunikoval cez WebSocket, umožňoval vzdialené vykonávanie príkazov a exfiltráciu dát. Útok mal súvisieť aj s kampaňou cielenou na obyvateľov Ľviva, ktorej cieľom bolo šírenie spyvéru pre Android. Škodlivá PDF príloha bola podľa telemetrie služby Virustotal nahratá z Ukrajiny, Indie, Talianska a Slovenska, čo môže indikovať širšie cielenie kampane.

VÝZNAMNÉ UDALOSTI VO SVETE

14-hodinový výpadok AWS spôsobila chyba DNS služby DynamoDB

Amazon oznámila, že rozsiahly výpadok AWS (Amazon Web Services) v regióne US-EAST-1, ktorý trval viac než 14 hodín, bol spôsobený závažnou chybou DNS v službe DynamoDB. Chyba súbehu vymazala všetky IP adresy koncového bodu, čo znemožnilo pripojenie zákazníkov aj interných AWS služieb. Obnova si vyžiadala manuálny zásah, pretože automatické mechanizmy zlyhali, a spoločnosť Amazon následne zaviedla ochranné kontroly a zlepšila testovanie, aby zabránila podobným incidentom v budúcnosti.

VÝZNAMNÉ UDALOSTI VO SVETE

- Výskumníci z Okta zverejnili svoju analýzu kampaní severokórejských štátnych aktérov, v ktorých sa uchádzajú o vzdialené pracovné pozície pod falošnou identitou.
- Hackerská skupina ShinyHunters spustila webstránku s uniknutými dátami venovanú obetiam útokov na inštancie SalesForce, na ktorej boli za účelom vydierania zverejnené vzorky exfiltrovaných dát.
- Výskumníci z ReliaQuest a ZeroFox zverejnili analýzu ransomvérových útokov za Q3 2025.
- Ukrajinská tajná služba SSSCIP zverejnila prehľad aktivít ruských aktérov za H1 2025.
- Malvér STEALIT zneužíva novú funkciu Node.js s názvom Single Executable Application (SEA), ktorá umožňuje distribuovať škodlivý kód ako samostatný spustiteľný súbor bez potreby inštalácie Node.js.
- Spoločnosť Symantec zverejnila informácie o útokoch čínskej skupiny Jewelbug na systémy ruského poskytovateľa IT služieb.
- Výskumníci z GTIG zaznamenali prvý prípad zneužitia techniky Etherhiding zo strany štátom sponzorovaných aktérov. Severokórejská APT skupina UNC5342 od februára 2025 túto techniku zneužíva v rámci kampane Contagious Interview na šírenie malvéru slúžiaceho na krádež kryptomien.
- Kampaň DreamJob severokórejskej skupiny Lazarus cieli na výrobcov dronov v Európe.
- Palo Alto zverejnila detailnú analýzu dlhodobej phishingovej kampane Smishing Triad.
- CISA a NSA zverejnili odporúčania pre hardening serverov Microsoft Exchange.
- Avast zverejnila dekryptor ransomvéru Midnight.
- Europol vyzýva na koordinované zavedenie opatrení voči útokom falšujúcim službu Caller ID.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

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.

Novirmvér 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.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Keď sa uniknutý SECRET_KEY platformy Django stane horším: prípadová štúdia Wagtail

V ekosystéme Django je SECRET_KEY sama o sebe veľmi citlivá hodnota. Jej únik zvyčajne umožňuje útočníkom falšovať tokeny, resetovať heslá alebo kradnúť relácie v určitých konfiguráciách. Pri skúmaní modulu redirects aplikácie Wagtail však náš kolega objavil prípad, keď by únik hodnoty SECRET_KEY mohol eskalovať nad rámec zneužitia používateľa/relácie a umožniť čítanie súborov na strane servera. Python skript na zneužitie tejto zraniteľnosti je k dispozícii na repozitári Github nášho kolegu..

Končí podpora pre Windows 10. Čo ďalej?

Spoločnosť Microsoft tento rok plánovane ukončí podporu pre všetky verzie Windows 10. Po 14. októbri 2025 už tieto produkty nebudú dostávať aktualizácie zabezpečenia, aktualizácie nesúvisiace so zabezpečením, opravy chýb, technickú podporu a ani aktualizácie technického obsahu online. Po rokovaní s organizáciou Euroconsumers však v Európskom hospodárskom priestore predĺži pre nekomerčných používateľov bezplatnú podporu systémov Windows 10 o jeden rok, teda do októbra 2026. Spoločnosť to uskutoční poskytnutím svojho programu predĺženej podpory ESU (Extended Security Updates) pre spotrebiteľov zdarma.

DrayTek opravil závažnú zraniteľnosť vo webovom rozhraní routerov Vigor

Spoločnosť DrayTek vydala bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú zraniteľnosť viacerých routerov Vigor. CVE-2025-10547 možno zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom.

Kritická zraniteľnosť v Redis umožňuje vzdialené vykonanie kódu

Vývojári in-memory NoSQL úložiska Redis vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú kritickú zraniteľnosť. CVE-2025-49844 by vzdialený autentifikovaný útočník mohol zneužiť na vykonanie kódu a získanie úplnej kontroly nad systémom.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kampaň zneužívajúca kritickú zraniteľnosť Grafana

Dňa 28. septembra 2025 zaznamenala spoločnosť GreyNoise výrazný nárast pokusov o zneužitie zero-day zraniteľnosti CVE-2021-43798 v nástroji Grafana, ktorý umožňuje útočníkovi využívať možnosť prechádzania adresárovej štruktúry (path traversal). Celkom 110 unikátnych IP adries sa v ten deň pokúsilo o útok voči monitorovaným inštanciám. Všetky identifikované IP adresy sú klasifikované ako škodlivé.

Zraniteľnosť riešenia OneLogin IAM možno zneužiť na extrakciu tajných hodnôt OIDC

Spoločnosť One Identity vydala bezpečnostné aktualizácie svojho IAM (Identity and Access Management) riešenia OneLogin, ktoré opravujú zraniteľnosť vysokej závažnosti. CVE-2025-59363 umožňuje enumeráciu aplikácií a získanie tajných hodnôt OIDC (OpenID Connect). Tie možno následne zneužiť na získanie neoprávneného prístupu do systému.

Závažné zraniteľnosti vo VMware NSX a vCenter umožňujú enumeráciu používateľov a injekciu SMTP

Spoločnosť Broadcom vydala bezpečnostné aktualizácie VMware NSX a VMware vCenter, ktoré opravujú 3 vysoko závažné zraniteľnosti. Zraniteľnosti v NSX možno zneužiť na enumeráciu používateľov a následnú realizáciu brute-force alebo slovníkových útokov. Zraniteľnosť vo VMware vCenter umožňuje injektovať hlavičky SMTP.

Kritická zraniteľnosť v sieťových úložiskách WD My Cloud umožňuje vzdialené vykonanie kódu

Spoločnosť Western Digital vydala aktualizácie firmvéru viacerých modelov zariadení NAS (Network Attached Storage) série My Cloud, ktoré opravujú kritickú zraniteľnosť. CVE-2025-30247 možno zneužiť na vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Zraniteľnosť v Oracle E-Business Suite

Spoločnosť Oracle vydala bezpečnostnú aktualizáciu na svoj produkt E-Business Suite, ktorá opravuje vysoko závažnú zraniteľnosť. CVE-2025-61884 by vzdialený neautentifikovaný útočník zaslaním špeciálne vytvorených HTTP požiadaviek mohol zneužiť na kompromitáciu Oracle Configurator a získanie neoprávneného prístupu k citlivým údajom.

Microsoft v októbrovom balíku aktualizácií Patch Tuesday opravil 6 aktívne zneužívaných zraniteľností

Spoločnosť Microsoft vydala v októbri 2025 balík opráv pre portfólio svojich produktov opravujúci 172 zraniteľností, z ktorých 8 spoločnosť označila ako kritické. Tieto umožňujú vzdialene vykonávať kód a eskalovať oprávnenia. Šesť zraniteľností je aktívne zneužívaných.

Októbrová aktualizácia Windows 11 znemožňuje aplikáciám prístup na localhost

Kumulatívna aktualizácia 2025-10, 64-bitového operačného systému WINDOWS 11 znemožňuje vytvorenie HTTP spojenia s LOCALHOST adresou 127.0.0.1, čo narúša činnosť viacerých aplikácií. Nie je možné napríklad lokálne ladenie v nástroji Visual Studio, autentifikovať sa prostredníctvom SSMS Entra ID a Cisco Duo Desktop, ktoré počas svojej činnosti vyžadujú komunikáciu s komponentmi dostupnými prostredníctvom LOCALHOST.

Kritická zraniteľnosť Cisco Secure Firewall Management Center dovoľuje vykonávať systémové príkazy

Spoločnosť Cisco opravila kritickú zraniteľnosť v Cisco Secure Firewall Management Center, ktorá z dôvodu nevhodnej validácie používateľských vstupov dovoľuje vzdialenému útočníkovi pri prihlasovaní odoslať požiadavku obsahujúcu príkaz Shell. Ten zraniteľné zariadenie vykoná.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Juniper Networks vydáva veľký balík bezpečnostných opráv

Spoločnosť Juniper Networks opravila zhruba 220 zraniteľností vo svojich produktoch Junos OS, Junos Space a Junos Space Security Director. 9 z nich je kritických.

Útočníci ukradli zdrojový kód a popisy zraniteľností F5 BIG-IP

Spoločnosť F5 potvrdila, že sa stala obeťou kybernetického útoku, v rámci ktorého sa bližšie nešpecifikovanej štátom sponzorovanej skupine podarilo získať dlhodobý prístup do ich systémov a exfiltrovať citlivé údaje, vrátane zdrojového kódu a konfigurácií časti zákazníkov.

Automatický vytáčací systém ICTBroadcast obsahuje aktívne zneužívanú zraniteľnosť

Výskumníci z VulnCheck zverejnili informácie o aktívne zneužívanej kritickej zraniteľnosti v softvéri ICTBroadcast spoločnosti ICT Innovations, ktorý slúži na správu call centier a automatické vytáčanie hovorov. CVE-2025-2611 možno zneužiť na injekciu shellových príkazov a získanie úplnej kontroly nad systémom.

Zraniteľnosť v UEFI modulárnych počítačov Framework umožňuje inštaláciu bootkitov

Výrobca modulárnych notebookov a desktopov Framework vydal bezpečnostné aktualizácie firmvéru svojich produktov, ktoré opravujú zraniteľnosť zneužiteľnú na inštaláciu bootkitov a získanie úplnej kontroly nad systémom.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Prostredia Cursor a Windsurf obsahujú desiatky zraniteľností

Bezpečnostní výskumníci spoločnosti Ox Security upozornili na prítomnosť veľkého množstva známych zraniteľností v aktuálnych verziách vývojových prostredí Cursor a Windsurf, z dôvodu implementácie starých verzií nástrojov Chromium a V8. Výskumníci varujú, že ignorovanie či neaktualizovanie takýchto chýb predstavuje vážnu bezpečnostnú hrozbu.

Kritické zraniteľnosti v bránach TP-Link Omada

Spoločnosť TP-Link vydala bezpečnostné aktualizácie svojich brán Omada, ktoré opravujú 4 zraniteľnosti, z čoho 2 sú označené ako kritické. Kritické zraniteľnosti s identifikátormi CVE-2025-6542 a CVE-2025-7850 možno zneužiť na vzdialené vykonanie príkazov operačného systému a získanie úplnej kontroly nad systémom.

Microsoft WSUS má kritickú aktívne zneužívanú zraniteľnosť

Služba Windows Server Update Services obsahuje kritickú zraniteľnosť umožňujúcu vzdialene vykonávať kód. Útočníci posielajú upravené požiadavky na porty 8530 a 8531 služby WSUS, čím získavajú kontrolu nad serverom. Microsoft vydal núdzovú aktualizáciu a odporúča zakázať službu WSUS, pokiaľ opravná aktualizácia nie je možná.

MESAČNÍK ZRANITEĽNOSTÍ OKTÓBER 2025

VJ CSIRT pravidelne vydáva mesačný prehľad kritických zraniteľností.

https://csirt.sk/posts/2943.html