CSIRT.SK

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

MESAČNÁ SPRÁVA

DECEMBER 2024

TLP: CLEAR

Kybernetickým priestorom v decembri 2024 rezonovalo hneď niekoľko kľúčových udalostí a útokov. Doplňujúce informácie môžete nájsť v časti Významné udalosti vo svete.

1 Čínske hackerské skupiny aktívne zneužívajú funkcionality Visual Studio Code injekciu

Bezpečnostní výskumníci zverejnili informácie o kampani, v rámci ktorej čínski hackeri na vytvorenie perzistentného prístupu ku kompromitovaným systémom zneužívajú tunely vo Visual Studio Code

2 Útočníci v rámci útokov čoraz častejšie zneužívajú služby Cloudflare

Zneužitie platforiem Pages, Workers a Tunnels od spoločnosti Cloudflare predstavuje efektívny mechanizmus maskovania škodlivej činnosti a zjednodušuje obchádzanie bezpečnostných prvkov.

3 Nový typ phishingu zneužíva funkciu MS Word pre obnovu poškodených súborov

Výskumníci zachytili nový typ phishingových útokov, ktorý na obchádzanie bezpečnostných prvkov zneužíva zabudovanú funkcionalitu pre obnovu poškodených Microsoft Word dokumentov.

4 Nová phishing-as-a-service služba Rockstar 2FA je schopná obísť MFA ochranu

Nová phishing-as-a-service služba, ktorá sa primárne zameriava na získavanie prihlasovacích údajov do Microsoft 365 a ďalších SSO služieb je schopná obchádzať aj mechanizmy viacfaktorovej autentifikácie.

5 Password-spraying útoky zamerané na sieťové zariadenia Citrix Netscaler

Spoločnosť CITRIX a nemecké BSI varovali pred intenzívnymi password-spraying útokmi zameranými na sieťové zariadenia Citrix Netscaler.

6 Srbská vláda údajne zneužíva malvér NOVISPY na sledovanie subjektov

AMNESTY INTERNATIONAL SECURITY LAB odhalila nový Android malvér NOVISPY, ktorý má srbská vláda zneužívať na sledovanie aktivistov, novinárov a účastníkov protestov.

RIEŠENÉ INCIDENTY NA SLOVENSKU A Z NAŠEJ ČINNOSTI

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

Zaujímavým prípadom phishingu boli v decembri dve kampane. V prvej odosielateľ falšoval totožnosť Všeobecnej zdravotnej poisťovne. Cieľom útočníkov bolo presvedčiť obete, že majú preplatok vo VšZP, ktorý môžu získať kliknutím na odkaz a ďalšou interakciou s podvodnou webstránkou. Druhá zneužívala meno Finančného riaditeľstva SR a portálu Slovensko.sk. Modus operandi bol podobný, pričom útočník sa snažil presvedčiť obeť, aby interagovala so škodlivým odkazom, pod zámienkou vrátenia daňového preplatku.

V inom prípade zamestnanec pristúpil na phishingovú stránku, kde zadal svoje prihlasovacie údaje do služby Microsoft 365, spolu s druhým faktorom pre overenie. Administrátori pristúpili k zrušeniu všetkých relácii dotknutého používateľa do 365 cloudu a resetovali jeho heslo. Zasiahnutej organizácii sme odporučili, aby informovala zamestnancov o obdobných kampaniach a o tom, aby si nepreposielali phishingové maily medzi sebou.

V decembri v rámci riešenia bezpečnostných incidentov zaregistrovala NASES podozrivú aktivitu smerujúcu na webovú stránku organizácie v konštituencii CSIRT.SK. Aktivita bola vyhodnotená ako pokus o SQL-injection. Organizácia následne preverila nahlásenú aktivitu v rámci svojich procesov.

December priniesol tiež kybernetický bezpečnostný incident medzinárodného európskeho rozsahu. VJ CSIRT prijala hlásenie o bezpečnostnom kybernetickom incidente v Rumunsku so žiadosťou o spoluprácu. Incident súvisel s publikovanou hybridnou vplyvovou kampaňou pred rumunskými prezidentskými voľbami. Do incidentu bola zapojená aj IP adresa, ktorá patrí do pôsobnosti VJ CSIRT. Zodpovednú organizáciu sme upozornili na možnú kompromitáciu. V rámci komunikácie so subjektom bolo zistené, že zariadenie má konfiguračnú chybu, ktorá umožňuje amplifikačný útok na externé ciele. Takáto aktivita sa následne potvrdila. Incident bol riešený v spolupráci s SK-CERT.

Ani v tomto mesiaci aktéri ransomvérových hrozieb neoddychovali. Zariadenie pre seniorov poslalo hlásenie o počítači, ktorý bol napadnutý ransomvérom. Toto zariadenie slúžilo ako osobný počítač a zároveň aj server s citlivými údajmi, vrátane osobných kariet pacientov danej organizácie. Organizácii navrhla CSIRT.SK potrebné bezodkladné opatrenia a vyžiadané dáta a vzorky následne analyzovala.

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.

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 decembri prezentovala rôzne témy z oblasti kybernetickej bezpečnosti pre zamestnancov Kancelárie najvyššieho súdu SR a študentom SPŠ chemickej v Bratislave, SOŠ Šaca, Obchodnej akadémie Polárna v Košiciach a Gymnázia Trebišovská v Košiciach.

Členovia tímu CSIRT.SK sa v decembri zúčastnili 16. ročníka odbornej pedagogickej konferencie Škola 2024/2025 organizovanej odborným nakladateľstvom Dr. Josef Raabe Slovensko, kde predstavila niektoré témy z kybernetickej bezpečnosti.

V rámci tréningu svojich zručností sa členovia VJ CSIRT zúčastnili na medzinárodnom cvičení Cyber Coalition 2024 pod záštitou NATO. Aktívne spolupracovali v súčinnosti s SK-CERT so všetkými zúčastnenými krajinami a orgánmi. CyberCoalition je každoročne organizované cvičenie kybernetickej obrany, ktoré riadi a plánuje Allied Command Transformation (ACT) pod velením Military Commitee (MC). Zameriava sa na rozhodovacie procesy, technické a prevádzkové postupy a spoluprácu pre posilnenie schopnosti NATO a spojencov chrániť a brániť Alianciu v doméne kyberpriestoru.

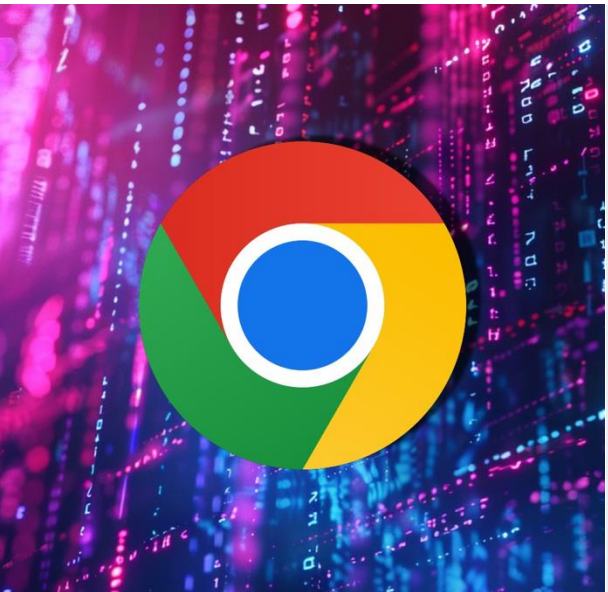
VÝZNAMNÉ UDALOSTI VO SVETE

Nový typ phishingu zneužíva funkciu MS Word pre obnovu poškodených súborov

Bezpečnostní výskumníci zachytili nový typ phishingových útokov, ktorý na obchádzanie bezpečnostných prvkov zneužíva zabudovanú funkcionalitu pre obnovu poškodených MICROSOFT WORD dokumentov. E-maily rozposielané v mene pracovníkov oddelenia miezd a ľudských zdrojov obsahujú úmyselne poškodené súbory, ktoré po obnove obsahujú personalizovaný obsah a QR kód slúžiaci na presmerovanie obete na falošnú prihlasovaciu stránku do Microsoft 365. Používatelia by mali byť obozretní pri otváraní správ a príloh z neoverených a nedôveryhodných zdrojov. S narastajúcou popularitou QR kódov je potrebné venovať zvýšenú pozornosť aj v prípade ich načítavania.

Spoločnosť Trustwave zverejnila analýzu phishing-as-a-service platformy Rockstar 2FA

Spoločnosť TRUSTWAVE zverejnila informácie o novej phishing-as-a-service službe ROCKSTAR 2FA, ktorá sa primárne zameriava na získavanie prihlasovacích údajov do Microsoft 365, Hotmail, Godaddy a ďalších SSO služieb. Využitím populárneho princípu adversary-in-the-middle sú útočníci zachytávaním platných session cookies schopní obchádzať aj mechanizmy viacfaktorovej autentifikácie. Framework prostredníctvom CLOUDFLARE TURNSTILE CAPTCHA filtruje návštevníkov, pričom podozrivé návštevy presmerováva na neškodné stránky s auto-moto tematikou. Útočníci na šírenie zneužívajú e-mailové správy rozposielané z kompromitovaných účtov a prostredníctvom legitímnych marketingových nástrojov. Na obídenie detekčných mechanizmov využívajú URL skracovače, QR kódy, PDF prílohy a ďalšie metódy.



Spoločnosť Google pripravuje novú funkcionalitu Chrome na sumarizáciu hodnotení stránok

Spoločnosť GOOGLE vyvinula novú funkciu webového prehliadača CHROME, ktorá na základe nezávislých recenzií prostredníctvom umelej inteligencie vytvorí krátku sumarizáciu hodnotenia navštívenej stránky. Funkcia s označením „Store Reviews“ sa zobrazí po kliknutí na ikony zámku alebo informácií v lište pre zadávanie URL adresy. Algoritmus spracúva informácie z rôznych platforiem ako sú napríklad Trustpilot alebo ScamAdvisor. Google pokračuje v postupnom vývoji a integrácii nových AI prvkov pre zvýšenie bezpečnosti a používateľskej prívetivosti svojho internetového prehliadača.

VÝZNAMNÉ UDALOSTI VO SVETE

Útočníci v rámci útokov aktívne zneužívajú služby Cloudflare Pages a Cloudflare Workers

Spoločnosť FORTRA informovala o zvýšenej miere zneužívania vývojárskych platforiem CLOUDFLARE PAGES a WORKERS v rámci kybernetických útokov. Služba Pages umožňuje tvorbu webových stránok a ich distribúciu prostredníctvom CDN a je zneužívaná v rámci phishingových útokov. Serverless výpočtová platforma Workers umožňuje vytvorenie a prevádzku aplikácií a skriptov a je zneužívaná na realizáciu DDoS a brute-force útokov, hostovanie phishingového obsahu a injekciu skriptov. Zneužitie platforiem od spoločnosti Cloudflare predstavuje efektívny mechanizmus maskovania škodlivej činnosti a tiež zjednodušuje obchádzanie bezpečnostných prvkov.

Útočníci kompromitovali NPM knižnicu Solana web3.js

Spoločnosť SOCKET INC informovala supply chain útoku na NPM knižnicu SOLANA WEB3.JS, ktorú decentralizované aplikácie využívajú na pripojenie a interakciu s blockchainom SOLANA. Bližšie neidentifikovaný útočník získal prístup k tejto knižnici a injektoval do nej škodlivý kód, ktorého cieľom bolo získavanie a následná exfiltrácia citlivých údajov. Solana potvrdila kompromitáciu účtu jedného z vývojárov, ktorý útočníci zneužili v rámci útoku, odstránila škodlivé verzie a vývojárom odporučila preveriť integritu svojich aplikácií a vykonať zmenu hesiel a ďalšieho kryptografického materiálu (napr. certifikáty, kľúče, tokeny).

Ruská APT skupina BLUEALPHA na maskovanie činnosti zneužíva službu Cloudflare Tunnels

Ruská štátom sponzorovaná skupina BLUEALPHA v rámci kybernetických útokov šíriacich malvér GAMMADROP na maskovanie svojej činnosti zneužíva službu CLOUDFLARE TUNNELS. Služba umožňuje vytvorenie náhodne generovanej subdomény trycloudflare.com a preposielanie všetkých prichádzajúcich požiadaviek na cieľový webový server prostredníctvom infraštruktúry Cloudflare. Aktéri na šírenie malvéru zneužívajú HTML smuggling, sofistikované metódy obchádzania mechanizmov e-mailovej ochrany a DNS fast-flux metódu na maskovanie riadiacej infraštruktúry. Fast-Flux metóda spočíva v rýchlej a pravidelnej zmene IP adries domén, čo výrazne komplikuje analýzu a proces odstraňovania škodlivého obsahu.

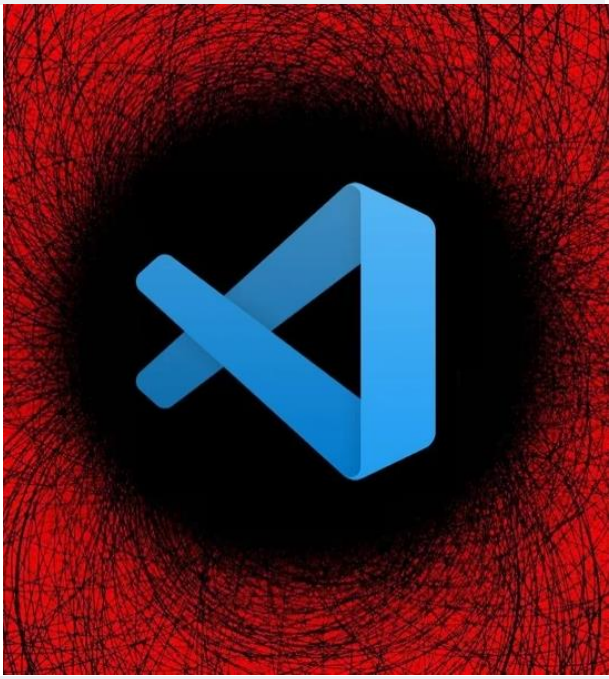
VÝZNAMNÉ UDALOSTI VO SVETE

Kampaň MEETEN distribuuje malvér pre získavanie kryptopeňaženiek a citlivých údajov

Spoločnosť CADO SECURITY LABS zverejnila informácie o malwaretisement kampani MEETEN, ktorá cieli na WEB3 komunitu. Obete sú oslovované s ponukou spolupráce a následne navádzané na stiahnutie videokonferenčných nástrojov, ktoré v skutočnosti slúžia na šírenie malvéru REALST STEALER. Stránky slúžiace na stiahnutie malvéru sú generované prostredníctvom umelej inteligencie a obsahujú JavaScript slúžiaci na pripojenie kryptopeňaženky obete. Realst Stealer infikuje zariadenia s operačnými systémami Windows a macOS a zameriava sa na exfiltráciu kryptopeňaženiek, prihlasovacích údajov, bankových údajov, cookies a hesiel uložených vo webových prehliadačoch.

Čínske hackerské skupiny v rámci útokov aktívne zneužívajú funkcie Visual Studio Code

Bezpečnostní výskumníci zo spoločnosti SENTINELLABS a TINEXTA CYBER zverejnili informácie o kampani, v rámci ktorej čínski hackeri na vytvorenie perzistentného prístupu ku kompromitovaným systémom zneužívajú tunely vo VISUAL STUDIO CODE. Tunely sú súčasťou funkcionality Microsoft Remote Development, ktorá prostredníctvom infraštruktúry Azure umožňuje vzdialený prístup k systémom, vrátane prístupu k súborovému systému a možnosti vykonávania príkazov. Kampaň bola zachytená počas júna a júla 2024 a hoci sa nejedná o prvé zneužitie tunelov v rámci útokov, poukazuje na vynaliezavosť čínskych štátom podporovaných skupín. Administrátorom a používateľom odporúčame monitorovať spustenia VSCode, odchádzajúce spojenia na *.devtunnels.ms a limitovať využívanie tunelov.



FBI útok na bitcoin burzu DMM atribuovala severokórejskej APT skupine TRADERTRAITOR

Americká FBI útok na japonskú bitcoinovú burzu DMM, ktorý sa uskutočnil v máji 2024, atribuovala severokórejskej štátom sponzorovanej skupine TRADERTRAITOR. V rámci útoku boli odcudzené kryptomeny v celkovej hodnote 308 miliónov dolárov. Útočníci vydávajúci sa za náborárov prostredníctvom služby LinkedIn kontaktovali zamestnanca japonskej spoločnosti Ginco s ponukou práce a v rámci pohovoru mu poskytli odkaz na GitHub repozitár so škodlivým obsahom. Malvér umožnil prienik do systémov spoločnosti Ginco a následne sa útočníkom v rámci laterálneho pohybu po sieti podarilo dostať až do systémov burzy DMM. Phishingové útoky s tematikou pracovných ponúk sú obľúbeným modusom operandi severokórejských skupín.

VÝZNAMNÉ UDALOSTI VO SVETE

Spoločnosť AKAMAI zverejnila informácie o novom botnete na báze MIRAI

Bezpečnostní výskumníci zo spoločnosti AKAMAI zverejnili informácie o novom botnete na báze Mirai, ktorý sa šíri aktívnym zneužívaním zraniteľností v NVR zariadeniach DigiEver DS-2105 PRO, zariadeniach od spoločnosti TP-Link a routeroch Teltonika RUT9XX. Kritická zraniteľnosť v DigiEver NVR nemá pridelený CVE identifikátor a spočíva v nedostatočnom overovaní používateľských vstupov. Vzdialený neautorizovaný útočník by ju zaslaním špeciálne vytvorených HTTP POST požiadaviek mohol zneužiť na injekciu príkazov a následné vzdialené vykonanie kódu. Kompromitované zariadenia sú zneužívané na identifikáciu a útoky na ďalšie zraniteľné zariadenia a realizáciu DDoS útokov.

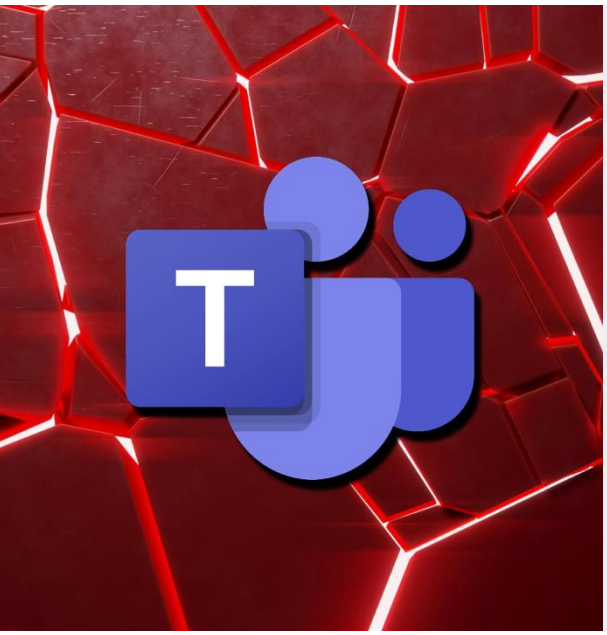
Password-spraying útoky zamerané na sieťové zariadenia Citrix Netscaler

Spoločnosť CITRIX a nemecké BSI varovali pred intenzívnymi password-spraying útokmi zameranými na sieťové zariadenia CITRIX NETSCALER. Tento typ útoku možno okrem úspešného prieniku do systému zneužiť aj na zneprístupnenie služby. Nakoľko zariadenia logujú všetky neúspešné pokusy o prihlásenie, v prípade rozsiahleho útoku môže dôjsť k zahlteniu výpočtových prostriedkov a úložiska. Výrobca odporúča implementovať multifaktorovú autentifikáciu, povoliť len pokusy o autentifikáciu adresované na FQDN (Fully Qualified Domain Name) a nie priamo na IP adresy, nasadenie WAF (Web Application Firewall) a limitovanie dostupnosti zariadení využívajúcich pre-nFactor autentifikáciu. Podobné útoky na Cisco zariadenia boli zachytené aj v apríli 2024.

ESET Threat Report H2 2024: Phishingové kampane s tematikou výhodných investícií

Spoločnosť ESET v rámci Threat Report H2 2024 zverejnila informácie o phishingovej kampani s tematikou výhodných investícií, v rámci ktorej útočníci na promovanie svojho obsahu zneužívajú falošné alebo kompromitované účty na sociálnych sieťach, platenú reklamu a deepfake videá zneužívajúce identitu známych subjektov generované prostredníctvom AI nástrojov. Phishingové stránky slúžia na získanie kontaktných údajov, pomocou ktorých útočníci obete kontaktujú telefonicky a snažia sa ich presvedčiť na investovanie do kryptomien a inštaláciu nástrojov pre vzdialenú kontrolu zariadení. Využitie YANDEX nástrojov na sledovanie návštevníkov a prítomnosť komentárov v cyrilike naznačuje, že sa môže jednať o rusky hovoriaceho aktéra. Podobné útoky boli zachytené aj v rámci kybernetického priestoru SR.

VÝZNAMNÉ UDALOSTI VO SVETE



Útočníci zneužívajú MS Teams videokonferencie na šírenie malvéru DARKGATE

Spoločnosť RAPID7 varuje pred rozsiahlou phishingovou kampaňou, v rámci ktorej útočníci e-mailami rozposielajú pozvánky na MS TEAMS videokonferencie. V rámci volania sa obeť snažia presvedčiť na inštaláciu nástrojov pre vzdialenú kontrolu (napr. Anydesk) a infekciu zariadenia malvérom DARKGATE slúžiacim na ďalšie získavanie a exfiltráciu citlivých údajov. Článok na portáli The Hacker News obsahuje prehľadnú sumarizáciu v súčasnosti najpoužívanejších metód šírenia malvéru.

Botnet MIRAI infikuje Juniper Session Smart Routre s predvolenými heslami

Spoločnosť JUNIPER NETWORKS varovala majiteľov SESSION SMART routerov pred útokmi, v rámci ktorých dochádza k infekcii zariadení malvérom MIRAI. Útočníci skenovaním internetu vyhľadávajú nesprávne nakonfigurované zariadenia alebo zariadenia s predvolenými heslami. Kompromitované zariadenia zapojené do botnet siete sú zneužívané na realizáciu útokov DDoS. Varovanie obsahuje postup pre identifikáciu kompromitovaných zariadení a taktiež odporúčania pre ich zabezpečenie.

Srbská vláda údajne zneužíva malvér NOVISPY na sledovanie vybraných subjektov

AMNESTY INTERNATIONAL SECURITY LAB na mobilnom zariadení novinára odhalila nový Android malvér NOVISPY, ktorý má srbská vláda zneužívať na sledovanie aktivistov, novinárov a účastníkov protestov. K infekcii zariadenia dochádza počas kontroly. Fyzický prístup k zariadeniu možno zneužiť na jeho odomknutie prostredníctvom forenzných nástrojov od spoločnosti CELLEBRITE, ktoré na obídenie bezpečnostných mechanizmov a perzistentnú inštaláciu malvéru na úrovni jadra zneužívajú zero-day zraniteľnosti v ovládači Qualcomm ADSPRPC. Malvér počas svojej činnosti komunikuje s IP adresami prepojenými s BIA (srbská tajná služba). Srbská polícia obsah reportu a zneužitie produktov Cellebrite kategoricky odmietla.

VÝZNAMNÉ UDALOSTI VO SVETE

- Bezpečnostní výskumníci zo spoločnosti BINARLY zverejnili analýzu nedávno objaveného linuxového UEFI bootkitu BOOTKITTY
- EUROPOL zadržal predstaviteľov spoločnosti dodávajúcej satelitné prijímače so skrytou funkcionalitou
- Ruská APT skupina TURLA v rámci útokov zneužíva infraštruktúru iných hackerských skupín
- Ransomvérová skupina TERMITE prenikla do systémov celosvetového poskytovateľa software-as-a-service služby BLUE YONDER
- EUROPOL rozložil sieť kyberkriminálnikov, ktorá sa špecializovala na pranie špinavých peňazí, phishingové kampane a online podvody zneužívajúce identity bánk
- Rumunský ústavný súd v súvislosti s kybernetickými útokmi na volebné systémy a vplyvovými operáciami zo strany Ruskej federácie zrušil výsledky prezidentských volieb
- Kompromitované NPM balíky RSPACK a VANT boli zneužité v rámci útokov na dodávateľský reťazec šíriacich kryptominery
- Bezpečnostní výskumníci identifikovali sieť 193 RDP proxy serverov zneužívaných v rámci útokov ruskej štátom sponzorovanej skupiny APT29
- Ruskej hackerskej skupine GAMAREDON na sledovanie a exfiltráciu údajov začala využívať Android spywary BONESPY a PLAINGNOME

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Bezpečnostní výskumníci zverejnili PoC kód pre zneužitie kritickej zraniteľnosti v Progress WhatsUp Gold

Bezpečnostní výskumníci zo spoločnosti Tenable zverejnili proof-of-concept kód demonštrujúci postup zneužitia kritickej zraniteľnosti v produkte Progress WhatsUp Gold, ktorá bola opravená aktualizáciami zo septembra 2024. CVE-2024-8785 možno zneužiť na vykonanie neoprávnených zmien v systéme a následné vykonanie škodlivého kódu.

Kritická zraniteľnosť v IAM systéme SailPoint IdentityIQ

Spoločnosť SailPoint vydala bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť v produkte IdentityIQ. Jedná sa o IAM (Identity and Access Management) platformu pre overovanie identity používateľov. CVE-2024-10905 možno zneužiť na získanie neoprávneného prístupu k citlivým údajom a získanie úplnej kontroly nad systémom.

Kritická zraniteľnosť manažmentového nástroja Veeam Service Provider Console

Spoločnosť Veeam vydala bezpečnostné aktualizácie nástroja Veeam Service Provider Console (VSPC), ktoré opravujú dve zraniteľnosti, z čoho jedna je označená ako kritická. CVE-2024-42448 možno zneužiť na vzdialené vykonanie kódu na serveroch VSPC.

Vysoko závažná zraniteľnosť v plugine WordPress WPForms

Vývojári WordPress pluginu WPForms vydali bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú zraniteľnosť. CVE-2024-11205 možno vykonaním neoprávnených zmien v systéme zneužiť vrátenie platieb alebo zrušenie predplatného implementovaného prostredníctvom služby Stripe a spôsobiť tak finančné škody prevádzkovateľom zraniteľných webových stránok.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritické bezpečnostné zraniteľnosti v produktoch Ivanti CSA, ICS a IPS

Spoločnosť Ivanti vydala bezpečnostné aktualizácie, ktoré opravujú 8 bezpečnostných zraniteľností v produktoch Ivanti Cloud Services Application (CSA), Ivanti Desktop and Server Management (DSM), Ivanti Connect Secure (ICS), Ivanti Policy Secure (IPS), Sentry a Patch SDK, z čoho 5 je označených ako kritické. Kritické zraniteľnosti v produktoch CSA, ICS a IPS možno zneužiť na SQL injekciu, vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Ostatné zraniteľnosti možno zneužiť na zneprístupnenie služby, vykonanie neoprávnených zmien v systéme a obídenie bezpečnostných mechanizmov.

Microsoft v rámci decembrového Patch Tuesday opravil 17 kritických zraniteľností

Spoločnosť Microsoft vydala v decembri 2024 balík opráv pre portfólio svojich produktov opravujúci 72 zraniteľností, z ktorých 31 umožňuje vzdialené vykonávanie kódu. Kritické zraniteľnosti sa nachádzajú v komponentoch Windows Remote Desktop Services a Client, Windows Lightweight Directory Access Protocol a Client, Windows Hyper-V, Microsoft Message Queuing, Windows Local Security Authority Subsystem Service a možno ich zneužiť vzdialené vykonanie škodlivého kódu. Zraniteľnosť v komponente Windows Common Log File System Driver (CVE-2024-49138) v súčasnosti útočníci aktívne zneužívajú.

Zraniteľnosti SSL-VPN v zariadeniach série SMA100 od spoločnosti SonicWall

Spoločnosť SonicWall vydala bezpečnostné aktualizácie, ktoré opravujú 6 zraniteľností vo funkcionalite SSL-VPN zariadení série SMA100. Najzávažnejšie zraniteľnosti s označením CVE-2024-53703, CVE-2024-45318, CVE-2024-40763 a CVE-2024-38475 možno zneužiť na vzdialené vykonanie kódu a získanie neoprávneného prístupu k citlivým údajom.

Aktívne zneužívaná zraniteľnosť v nástrojoch pre zabezpečený prenos súborov od spoločnosti Cleo

Bezpečnostní výskumníci zo spoločnosti Huntress informovali o aktívne zneužívanej zraniteľnosti v nástrojoch pre zabezpečený prenos a zdieľanie súborov Cleo Harmony, Cleo VLTrader a Cleo LexiCom. Zraniteľnosť CVE-2024-55956 možno zneužiť na získanie neoprávneného prístupu k citlivým údajom, vykonanie neoprávnených zmien v systéme a vzdialené vykonanie kódu. Zraniteľnosť v súčasnosti zneužíva aj ransomvérová skupina Clop.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritické bezpečnostné zraniteľnosti v produktoch Adobe

Spoločnosť Adobe vydala bezpečnostné aktualizácie niektorých svojich produktov, ktoré opravujú 165 zraniteľností, z čoho 45 sú označené ako kritické. Kritické zraniteľnosti by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na vykonanie škodlivého kódu, eskaláciu privilégií a získanie neoprávneného prístupu k citlivým údajom. Ostatné zraniteľnosti umožňujú vykonanie škodlivého kódu, získanie neoprávneného prístupu k citlivým údajom, obídenie bezpečnostných prvkov a zneprístupnenie služby. Microsoft v rámci novembrového Patch Tuesday opravil 4 kritické zraniteľnosti.

Aktívne zneužívaná kritická zraniteľnosť vo frameworku Apache Struts

Vývojári open-source frameworku pre tvorbu Java EE webových aplikácií Apache Struts vydali bezpečnostné aktualizácie, ktoré opravujú aktívne zneužívanú kritickú zraniteľnosť. CVE-2024-53677 možno zneužiť na upload súborov a vzdialené vykonanie kódu. Na uvedenú zraniteľnosť je v súčasnosti dostupný proof-of-concept kód demonštrujúci postup jej zneužitia.

Kritická zraniteľnosť vo webových serveroch Apache Tomcat

Vývojári open-source webového servera Apache Tomcat vydali bezpečnostné aktualizácie opravujúce 2 zraniteľnosti, z ktorých jedna je označená ako kritická. CVE-2024-50379 by vzdialený neautentifikovaný útočník mohol zneužiť na vzdialené vykonanie kódu.

Kritická zraniteľnosť v produktoch Adobe ColdFusion

Spoločnosť Adobe vydala bezpečnostné aktualizácie, ktoré opravujú kritickú zraniteľnosť v produkte Adobe ColdFusion. CVE-2024-53961 možno zneužiť na získanie neoprávneného prístupu k citlivým údajom, ktoré možno následne zneužiť na realizáciu ďalších útokov a získanie úplnej kontroly nad systémom.

ZÁVAŽNÉ ZRANITEĽNOSTI BEŽNÝCH SOFTVÉROVÝCH PRODUKTOV

Kritické zraniteľnosti v produktoch Apache MINA, HugeGraph-Server a Traffic Control

Vývojári z The Apache Software Foundation vydali bezpečnostné aktualizácie, ktoré opravujú kritické zraniteľnosti v produktoch Apache MINA, Apache HugeGraph-Server a Apache Traffic Control. CVE-2024-52046 v sieťovom aplikačnom frameworku MINA možno zneužiť na vzdialené vykonanie škodlivého kódu. CVE-2024-43441 v Apache HugeGraph-Server umožňuje získanie úplnej kontroly nad systémom a CVE-2024-45387 (Traffic Control) možno zneužiť na realizáciu SQL injekcie.

Aktívne zneužívaná zraniteľnosť v operačnom systéme Palo Alto PAN-OS

Spoločnosť Palo Alto Networks vydala bezpečnostné aktualizácie, ktoré opravujú vysoko závažnú zraniteľnosť v operačnom systéme PAN-OS. CVE-2024-3393 v komponente DNS Security možno zaslaním špeciálne vytvorených paketov zneužiť na zneprístupnenie služby a vyradenie firewallov. Zraniteľnosť súčasnosti aktívne zneužívajú útočníci.

Kritické zraniteľnosti vo firewalloch Sophos

Spoločnosť Sophos vydala bezpečnostné aktualizácie pre svoje firewally, ktoré opravujú tri zraniteľnosti, z ktorých dve sú označení ako kritické. CVE-2024-12727 a CVE-2024-12728 možno zneužiť na získanie neoprávneného prístupu do systému a vzdialené vykonanie kódu. Poslednú zraniteľnosť možno zneužiť na injekciu príkazov.

Kritické zraniteľnosti v moduloch WordPress WPLMS a VibeBP

Vývojári modulov WordPress WPLMS a VibeBP vydali bezpečnostné aktualizácie, ktoré opravujú 18 zraniteľností, z ktorých 7 je označených ako kritických. Kritické zraniteľnosti vo WPLMS možno zneužiť na nahranie súborov na server, vzdialené vykonanie kódu, eskaláciu privilégií a získanie úplnej kontroly nad systémom. Kritické zraniteľnosti vo VibeBP možno zneužiť na realizáciu SQL injekcie, eskaláciu privilégií z získanie úplnej kontroly nad systémom.

MESAČNÍK ZRANITEĽNOSTÍ DECEMBER 2024

CSIRT.SK vydáva a uverejňuje na svojej stránke prehľad kritických zraniteľností bežného softvérového vybavenia na mesačnej báze. Jedná sa o nasledovné produkty:

1. Operačné systémy Microsoft Windows
2. Kancelárske balíky Microsoft Office a Office Web Apps
3. Internetové prehliadače
   - Microsoft Internet Explorer Microsoft Edge
   - Mozilla Firefox
   - Google Chrome
4. Adobe Flash Player, Acrobat a Reader
5. Frameworky
   - Microsoft .NET Framework
   - Oracle Java
6. Iné tohtomesačné závažné zraniteľnosti
   - WordPress plugin WPLMS, WordPress plugin VibeBP
   - Sophos Firewall
   - Palo Alto PAN-OS, Prisma Access s PAN-OS
   - Apache MINA, Apache HugeGraph-Server, Apache Traffic Control
   - Adobe ColdFusion
   - Apache Tomcat
   - Apache Struts
   - Adobe Experience Manager, Acrobat DC, Acrobat Reader DC, Acrobat, Acrobat Reader, Adobe Media Encoder, Illustrator, Adobe After Effects, Adobe Animate, Adobe InDesign, Adobe PDFL Software Development Kit (SDK), Adobe Connect, Adobe Substance 3D Sampler, Photoshop 2025, Adobe Substance 3D Modeler, Adobe Bridge, Adobe Premiere Pro, Adobe Substance 3D Painter, Adobe FrameMaker
   - Cleo Harmony, Cleo VLTrader, Cleo LexiCom
   - Ivanti Cloud Services Application, Ivanti Desktop and Server Management, Ivanti Connect Secure, Ivanti Policy Secure, Ivanti Sentry, Ivanti Patch SDK, Ivanti Endpoint Manager, Ivanti Security Controls (iSec), Ivanti Patch for Configuration Manager, Ivanti Neurons for Patch Management, Ivanti Neurons Agent Platform
   - Microsoft 365 Apps for Enterprise, Microsoft Access, Microsoft Defender for Endpoint for Android, Microsoft Excel, Microsoft Office, Microsoft Office LTSC, Microsoft SharePoint Enterprise Server, Microsoft SharePoint Server, Microsoft Word, Microsoft/Muzic, Remote Desktop client for Windows Desktop, System Center Operations Manager (SCOM), Windows, Windows App Client for Windows Desktop, Windows Server
   - SSL-VPN v zariadeniach série SMA100 (SMA 200, 210, 400, 410 a 500v)

- WordPress plugin WPForms
- Veeam Service Provider Console
- SailPoint IdentityIQ
- Progress WhatsUp Gold

https://csirt.sk/posts/1899.html