Cybersecurity Report

14.7.2025 – 27.7.2025

Stories

Detekcia eskalácie práv cez ADCS (ESC1) pomocou Microsoft Sentinel

Ak nie je zapnutý audit v Active Directory Certificate Services (ADCS), nie je možné detegovať útoky typu ESC1, ktoré umožňujú bežnému účtu získať oprávnenia správcu domény. Po aktivácii auditu cez certsrv > Vlastnosti > Auditovanie a nastavení zaznamenávania udalostí ako 4886 (žiadosť o certifikát) a 4887 (vydanie certifikátu), je možné pomocou KQL dotazu v Microsoft Sentinel zachytiť, keď sa líši požívateľ žiadosti a subjekt certifikátu. Tento rozdiel indikuje pokus o eskaláciu práv. Na základe požiadavky sa vytvorí pravidlo, ktoré spustí alert každých 5 minút. Dodatočne možno detegovať chyby ako Event ID 39 alebo 41, ktoré Microsoft pridáva ako ochranu, keď SID žiadateľa a SID cieľa nesúhlasia. Medzi ďalšie zaujímavé udalosti patria 4900 (zmena oprávnení šablóny) a 4899 (úprava šablóny). Správnym nastavením logovania a Sentinel pravidiel možno identifikovať viaceré ADCS útoky v reálnom čase.

https://www.blackhillsinfosec.com/detecting-adcs-privilege-escalation/

Soco404: Kryptominér schovaný v 404 chybových stránkach

Nová kampaň nazývaná Soco404 zneužíva falošné 404 stránky na distribúciu škodlivého kódu ukrytého v base64 formáte medzi HTML tagmi, čím obchádza tradičné bezpečnostné kontroly. Útočníci využívajú Google Sites, kompromitované Tomcat servery a otvorené PostgreSQL databázy, kde cez funkciu COPY FROM PROGRAM spúšťajú príkazy. Na Linux systémoch sa skript sťahuje cez curl alebo wget, po čom vymaže logy, vypne konkurenčné minery a aktivuje optimalizácie CPU pre ťaženie kryptomeny. Na Windows zariadeniach sa payload doručuje cez certutil alebo Invoke-WebRequest, pričom sa spúšťa ako ok.exe, injektuje miner a následne sa maže. Malware sa maskuje ako systémové procesy, udržiava si prežitie cez cron joby, shell hooky a watchdog vlákna. Celá operácia je postavená na falošnej stránke hostenej na fastsoco.top, ktorá do pamäte zariadenia prenáša škodlivý kód bez zanechania stôp na disku.

https://cybersecuritynews.com/beware-of-fake-error-pages-that-linux-and-windows-systems/

ToolShell: neobmedzená hostina pre útočníkov

ESET Research objavil útoky zneužívajúce nové zero-day zraniteľnosti s názvom ToolShell v on-premise Microsoft SharePoint Serveri. Ide o CVE-2025-53770 (vzdialené vykonanie kódu) a CVE-2025-53771 (server spoofing), ktoré umožňujú útočníkom obísť multifaktorové overovanie a Single Sign-On, získať prístup k citlivým údajom a nasadiť škodlivé webshell-y, napr. spinstall0.aspx. Zneužívanie začalo medzi 17. a 22. júlom 2025. ESET zaznamenal, že útoky vykonávali rôzne skupiny – od bežných kyberkriminálnikov až po APT skupiny napojené na Čínu (napr. LuckyMouse). Útočníci často využívajú jednoduché ASP webshell-y ako ghostfile346.aspx a ghostfile972.aspx na získanie MachineKey a trvalého prístupu k serveru. Niektoré útočné kampane prebiehali kompletne v pamäti (tzv. "no shell") bez zápisu na disk, pričom využívali .NET moduly načítané priamo do RAM, čím sa výrazne znižuje šanca na ich odhalenie. Medzi známe IOCs patria IP adresy ako 96.9.125[.]147 a 107.191.58.76. Microsoft vydal záplaty dňa 21. júla 2025. Ohrozené sú on-prem verzie SharePoint 2016, 2019 a Subscription Edition. Cloudová verzia SharePoint Online v rámci Microsoft 365 týmto útokom nečelí.

https://www.welivesecurity.com/en/videos/sharepoint-under-fire-toolshell-attacks-hit-organizations-worldwide/

Prvý známy malvér s podporou LLM od hackerov APT28 integruje schopnosti umelej inteligencie do metodiky útoku

Ukrajinské CERT-UA odhalilo novú kyberšpionážnu kampaň LAMEHUG, za ktorou stojí ruská APT skupina APT28. Malware využíva veľký jazykový model (LLM) Qwen2.5-Coder-32B-Instruct z Hugging Face API na generovanie príkazov v reálnom čase priamo na infikovanom zariadení. Týmto spôsobom útočníci nemusia dopredu hardkódovať príkazy – každý infikovaný host dostane príkaz šitý na mieru podľa prostredia. Infekcia sa začína phishingovým emailom s prílohou „Додаток.pdf.zip“, ktorá po otvorení spustí PyInstaller-kompilovaný spustiteľný súbor a zobrazí falošný PDF dokument. Malware následne dekóduje embedded prompt a odošle ho do LLM, ktoré vráti príkazy ako systeminfo, wmic, a rekurzívne zbieranie súborov z Desktopu, Dokumentov a Downloads. Výstup sa ukladá do %PROGRAMDATA%\info. Exfiltrovanie dát prebieha buď cez SFTP tunel na IP 144.126.202.227, alebo cez HTTP POST na kompromitovanú doménu stayathomeclasses.com. Vďaka používaniu bežných protokolov a legitímne pôsobiacej AI komunikácii malware uniká detekcii tradičnými

bezpečnostnými nástrojmi. Toto je prvý známy prípad, keď je cloudový AI model využívaný priamo ako "mozog" malvéru.

https://cybersecuritynews.com/llm-powered-malware-from-apt28-hackers-integrates-ai-capabilities/

CISA varuje pred zraniteľnosťou overovania vstupu 0-Day v prehliadači Google Chromium zneužívanou pri útokoch

Americká CISA vydala naliehavé varovanie pred zraniteľnosťou CVE-2025-6558, ktorá sa aktívne zneužíva a ohrozuje všetky prehliadače postavené na jadre Chromium, vrátane Google Chrome, Microsoft Edge a Opera. Zraniteľnosť spočíva v nesprávnej validácii vstupu v komponentoch ANGLE a GPU, čo útočníkom umožňuje pomocou špeciálne upravených HTML stránok prekonať sandbox prehliadača – kľúčovú bezpečnostnú bariéru, ktorá bráni neoprávnenému prístupu k systému. Útoky môžu viesť k spusteniu škodlivého kódu, krádeži údajov alebo trvalému kompromitovaniu zariadenia. CISA zaradila túto zraniteľnosť do zoznamu známych zneužívaných zraniteľností (KEV) a stanovila termín na odstránenie hrozby do 12. augusta 2025.

https://cybersecuritynews.com/cisa-google-chromium-0-day/