TLP: CLEAR

Cybersecurity Report

18.05.2025 - 31.05.2025

Stories

Závažná chyba v OneDrive File Picker umožňuje aplikáciám prístup k celému úložisku

Výskumníci zo spoločnosti Oasis Security upozornili 28. mája 2025 na kritickú zraniteľnosť v Microsoft OneDrive File Picker, ktorá umožňuje webovým aplikáciám získať plný prístup k celému OneDrive používateľa namiesto iba k vybraným súborom. Problém spôsobuje príliš široké OAuth oprávnenie (napr. Files.ReadWrite.All) a zavádzajúce súhlasy používateľa, ktoré nezobrazujú rozsah povoleného prístupu. Chyba sa týka stoviek aplikácií ako Slack, Trello, ChatGPT a ohrozuje milióny používateľov. Staršie verzie (6.0–7.2) navyše nebezpečne ukladajú prístupové tokeny do URL alebo localStorage, nové verzie zas ukladajú tokeny v sessionStorage v nešifrovanej forme. Dlhodobé Refresh Tokeny navyše zvyšujú riziko trvalého zneužitia. Microsoft chybu uznal, ale neoznámil žiadny konkrétny plán opravy.

https://cybersecuritynews.com/onedrive-file-picker-vulnerability/

Chrome 137 prináša AI ochranu pred podvodmi a opravuje kritické zraniteľnosti

Google 27. mája 2025 uvoľnil Chrome 137 ako stabilnú verziu pre Windows, macOS a Linux. Aktualizácia obsahuje 11 bezpečnostných opráv, vrátane vážnych chýb CVE-2025-5063 (use-after-free v Compositing) a CVE-2025-5280 (out-of-bounds zápis vo V8 engine), ktoré mohli umožniť vzdialené spustenie kódu. Chrome zároveň integruje Gemini Nano, AI model priamo v zariadení používateľa,

ktorý v reálnom čase deteguje scamy zneužívajúce klávesové skratky či vzhľad stránky. Tento systém výrazne zlepšuje ochranu proti podvodným webom, ktoré často existujú len niekoľko minút. Nová verzia prináša aj technické novinky ako podpora Ed25519 v WebCrypto API, Document-Isolation-Policy pre zjednodušenú cross-origin ochranu a plávajúce desatinné farby v canvas. S 65 % podielom na trhu má táto aktualizácia globálny dopad na miliardy používateľov a predstavuje nový štandard v bezpečnosti prehliadačov.

https://cybersecuritynews.com/chrome-security-update-code-execution/

GhostSpy: Nový pokročilý Android malware umožňuje úplné ovládnutie zariadenia

Výskumníci zo spoločnosti Cyfirma odhalili nebezpečný Android malvér GhostSpy, ktorý po infikovaní zariadenia získava plnú kontrolu nad smartfónom vrátane kradnutia hesiel, nahrávania obrazovky a zvuku, sledovania polohy a zneužívania bankových aplikácií. Šíri sa ako falošná aktualizácia alebo systémová aplikácia a zneužíva Accessibility Services a Device Admin API na obídenie bezpečnostných obmedzení. Infekcia prebieha v dvoch fázach – úvodný dropper získa oprávnenia na inštaláciu a následne spustí druhý škodlivý APK balíček (“com.support.litework”), ktorý automaticky udeľuje povolenia simulovaním dotykov a preklikávaním cez rôzne jazykové verzie systému. GhostSpy dokáže obísť screenshot ochranu bankových aplikácií, čo z neho robí vážnu hrozbu pre finančné aj súkromné údaje. Riadiace servery malvéru sú aktívne vo viacerých krajinách, pričom hlavný C2 server beží na stealth.gstpainel.fun.

https://cybersecuritynews.com/new-android-malware-ghostspy/

SharpSuccessor zneužíva chybu BadSuccessor vo Windows Server 2025 na eskaláciu práv až na úroveň doménového administrátora

Výskumníci odhalili kritickú zraniteľnosť BadSuccessor v mechanizme delegovaných Managed Service Accounts (dMSA) vo Windows Server 2025, ktorú zneužíva nový nástroj SharpSuccessor, vytvorený v .NET Loganom Goinsom. Útočník s minimálnymi právami v Active Directory (napr. možnosťou vytvárať objekty v ľubovoľnej Organizačnej jednotke) môže vytvoriť škodlivý dMSA objekt a získať práva cieľového používateľa, vrátane Domain Administrator. Útok využíva manipuláciu atribútov msDS-ManagedAccountPrecededByLink a msDS-DelegatedMSAState. Následne útočník spúšťa viackrokový Kerberos reťazec pomocou nástroja Rubeus, čím získava TGT a TGS tikety pre škodlivý účet a získa SMB prístup k doménovým kontrolérom. Analýza ukazuje, že až 91 % domén má používateľov s právami postačujúcimi na vykonanie útoku, dokonca aj bez aktívneho používania dMSA. Microsoft označil chybu len ako stredne závažnú a zatiaľ neposkytol opravu.

https://cybersecuritynews.com/sharpsuccessor-poc-badsuccessor/

.Net Chihuahua Infostealer zneužíva Google Drive a kradne prihlasovacie údaje prehliadača a krypto peňaženky

V apríli 2025 bol odhalený sofistikovaný .NET malvér s názvom Chihuahua Infostealer, ktorý cieli na prehliadačové údaje a kryptopeňaženky. Šíri sa cez PowerShell skripty ukryté v súboroch na platformách ako Google Drive či OneDrive, pričom využíva viacstupňový infikovaný reťazec a spúšťa sa len v pamäti, čo sťažuje detekciu. V prvej fáze sa spustí Base64 kódovaný skript, v druhej fáze sa vytvorí naplánovaná úloha sledujúca .normaldaki súbory, a v tretej fáze sa stiahne .NET payload z flowers.hold-me-finger[.]xyz. Malvér kradne uložené heslá, cookies, históriu, a údaje z krypto pluginov ako EVER Wallet či Rabby. Dáta šifruje pomocou AES a posiela ich cez HTTPS na C2 servery. Obsahuje ruské rapové texty ako podpis autora a mapuje sa na techniky MITRE ATT&CK ako T1059.001 (PowerShell), T1053.005 (naplánované úlohy), či T1555.003 (krádež prihlasovacích

údajov). Ide o vysokorizikový infostealer, ktorý využíva dôveryhodné platformy a legitímne nástroje na skrytý zber dát.

https://cybersecuritynews.com/net-based-chihuahua-infostealer-exploit-google-drive-steals-browser-credentials-and-crypto-wallets/
