TLP: CLEAR

Cybersecurity Report

28.07.2025 - 10.08.2025

Stories

AgentFlayer: Zero-click exfiltrácia dát z ChatGPT Connectors

Na konferencii Black Hat bola prezentovaná kritická zraniteľnosť v ChatGPT Connectors, označená ako “AgentFlayer”, ktorá umožňuje zero-click exfiltráciu dát zo služieb ako Google Drive. Útok je postavený na technike indirect prompt injection. Malvér dokáže prinútiť agenta vyhľadávať citlivé súbory či API kľúče a odosielať ich útočníkom cez image-based exfiltration s využitím Azure Blob Storage URL, čím obchádza existujúce “url_safe” kontroly. Riziko sa netýka len Google Drive, ale všetkých konektorov (SharePoint, OneDrive, GitHub), čím vzniká nový vektor útokov na LLM-integrované podnikové prostredia. OpenAI nasadilo mitigácie, no architektonický problém pretrváva, čo potvrdzuje aj zaradenie prompt injection medzi OWASP Top 10 pre LLM aplikácie.

https://cybersecuritynews.com/chatgpt-0-click-connectors-vulnerability/

CVE-2025-38236: Privilege Escalation cez MSG_OOB v Linux kerneli

Google Project Zero výskumník Jann Horn odhalil kritickú zraniteľnosť (CVE-2025-38236) v Linux kerneli (verzia 6.9+), ktorá umožňuje únik zo sandboxu Chrome rendereru a eskaláciu práv na úroveň jadra. Problém pochádza z málo používanej funkcie MSG_OOB v UNIX domain sockets, zaveden ej v Linuxe 5.15, ktorá obsahovala use-after-free (UAF) chybu. Exploit umožňuje čítanie a manipuláciu s pamäťou jadra kombináciou techník ako reštartovanie freed objektov cez pipe pages či manipulácia page tabuliek. Zraniteľnosť zdôrazňuje

riziko zbytočne exponovaných kernelových funkcionalít v sandboxoch — Chrome musel MSG_OOB blokovať a kernel bol opravený. Prípad ukazuje limity fuzzingu (syzkaller zachytil súvisiaci bug až rok po zavedení) a potrebu prísnejšieho obmedzenia systémových volaní dostupných pre sandboxované procesy. .

https://cybersecuritynews.com/new-linux-kernel-vulnerability/

CVE-2025-53786: Privilege Escalation v Microsoft Exchange Hybrid

Podľa dát Shadowserver Foundation je na internete vystavených vyše 28 000 neopravených Microsoft Exchange serverov zraniteľných voči chybe CVE-2025-53786 (CVSS 8.0). Zraniteľnosť sa týka hybridných nasadení Exchange, kde on-premises servery a Exchange Online zdieľajú rovnaký service principal. Tento dizajnový nedostatok umožňuje útočníkom s admin prístupom na lokálny server vytvárať falšované autentifikačné tokeny platné 24 hodín, čím získajú prístup k Microsoft 365 a obchádzajú conditional access politiky – prakticky ide o privilege escalation bez detekovateľných audit trailov. Microsoft vydal aprílový 2025 hotfix a odporúča nasadiť samostatné hybrid aplikácie a vyčistiť legacy credentials. CISA reagovala vydaním Emergency Directive 25-02, ktorá nariaďuje federálnym agentúram opravu do 11. augusta 2025. Microsoft zároveň avizuje, že po 31. októbri 2025 dôjde k trvalému zablokovaniu Exchange Web Services cez zdieľaný principal, pričom prechod na bezpečnejšie Graph API sa stane povinným.

https://cybersecuritynews.com/microsoft-exchange-servers-vulnerable/

DarkCloud Stealer – Fileless Variant so špecializovaným zberom dát

Nová varianta DarkCloud infostealera cieli na Windows používateľov prostredníctvom phishingových kampaní s archívmi RAR maskovanými ako obchodné ponuky. Po spustení škodlivého JavaScriptu sa spustí viacstupňová infekcia, ktorá nasadí DarkCloud

fileless technikami bez tradičných signatúr. Malvér využíva process hollowing, ukrýva .NET DLL payload do JPEG obrázka na archive.org a načítava ho priamo do pamäte. DarkCloud cieli na prihlasovacie údaje, platobné karty a kontakty uložené v Chrome, Edge, Firefox a Brave, pričom priamo spúšťa SQL dotazy nad databázami pre extrakciu hesiel a čísel kariet. Pre perzistenciu kopíruje JS skript do C:\Users\Public\Downloads\edriophthalma.js a vytvára autorun kľúč v registre. Na úrovni vyhýbania sa detekcii implementuje anti-sandbox techniky – monitoruje klávesnicu a myš cez GetAsyncKeyState(), a spustí sa až pri reálnej interakcii používateľa, čím obchádza behaviorálnu analýzu v sandboxoch.

https://cybersecuritynews.com/new-windows-based-darkcloud-stealer-attacking-computers/

Mustang Panda útočí na používateľov Windowsu pomocou malvéru ToneShell, ktorý napodobňuje Google Chrome

APT skupina Mustang Panda spustila kampaň s malvérom ToneShell, ktorý sa maskuje ako Google Chrome a šíri sa cez phishingové emaily a kompromitované weby s falošnými inštalátormi či aktualizáciami. Malvér využíva process hollowing, injektuje payload do legitímneho procesu chrome.exe a vytvára perzistenciu úpravou registrov a plánovanými úlohami. ToneShell funguje ako backdoor – zabezpečuje vzdialený prístup, exfiltráciu dát a laterálny pohyb v sieti, pričom sieťovú komunikáciu maskuje ako legitímnu prevádzku Chrome. Kampaň cieli na vládne a technologické sektory a predstavuje výraznú hrozbu pre organizácie, keďže umožňuje špionáž a odcudzenie citlivých informácií.

https://cybersecuritynews.com/mustang-panda-attacking-windows-users/
