Cybersecurity Report

23.2.2026 – 8.3.2026

Google potvrdzuje zneužívanie Android zraniteľnosti CVE-2026-21385 v čipoch Qualcomm

Google potvrdil, že zraniteľnosť CVE-2026-21385 v grafickom komponente čipov Qualcomm používaných v Android zariadeniach je už aktívne zneužívaná v reálnych útokoch. Chyba (CVSS 7.8) je spôsobená buffer over-read a chybou v práci s pamäťou, ktorá môže viesť k narušeniu pamäte pri spracovaní používateľských dát. Google ju opravil v Android Security Update z marca 2026, ktorý rieši celkovo 129 zraniteľností v systéme vrátane ďalších kritických chýb umožňujúcich napríklad vzdialené spustenie kódu alebo eskaláciu oprávnení. Spoločnosť uviedla, že exploitácia je zatiaľ limitovaná a cielená, no odporúča používateľom aj organizáciám okamžite aplikovať bezpečnostné aktualizácie zariadení.

https://thehackernews.com/2026/03/google-confirms-cve-2026-21385-in.html

Deepfakes a injection útoky narúšajú systémy overovania identity

Výskumníci upozorňujú, že kombinácia deepfake technológií a tzv. injection útokov výrazne oslabuje moderné systémy digitálneho overovania identity, ktoré sa používajú napríklad pri registrácii účtov, KYC procesoch či obnove prístupu k účtom. Útočníci dokážu pomocou syntetických videí alebo hlasov napodobniť skutočnú osobu, prípadne úplne obísť kameru tým, že priamo vložia manipulovaný obraz alebo video do vstupného dátového streamu systému, čím obídu klasické „liveness“ kontroly. Takéto útoky môžu viesť k vytváraniu falošných identít, prevzatiu účtov alebo získaniu prístupu k interným systémom organizácie. Odborníci preto upozorňujú, že samotná detekcia deepfake už nestačí a moderné riešenia musia analyzovať celú verifikačnú reláciu vrátane zariadenia, správania používateľa a integrity vstupného signálu.

https://www.bleepingcomputer.com/news/security/how-deepfakes-and-injection-attacks-are-breaking-identity-verification/

Hackeri zneužívajú OAuth chybové presmerovania na šírenie malvéru

Microsoft upozornil na phishingové kampane, v ktorých útočníci zneužívajú legitímny OAuth redirection mechanizmus na obchádzanie ochrany v e-mailoch a prehliadačoch a presmerovanie obetí na škodlivé stránky. Útoky sa zameriavajú najmä na vládne a verejné organizácie a využívajú phishingové správy (napr. pozvánky na Teams, reset hesla či e-podpis), ktoré obsahujú manipulované OAuth URL. Po kliknutí dôjde k vyvolaniu chyby v autentifikačnom procese a používateľ je následne presmerovaný na útočníkom kontrolovanú stránku, kde sa stiahne škodlivý payload alebo phishingový kit. Táto technika je účinná, pretože využíva dôveryhodnú autentifikačnú infraštruktúru a umožňuje vytvárať odkazy, ktoré vyzerajú legitímne, čím sa zvyšuje úspešnosť útokov a zároveň sa obchádzajú tradičné detekčné mechanizmy.

https://www.bleepingcomputer.com/news/security/microsoft-hackers-abuse-oauth-error-flows-to-spread-malware/

Wikipedia zasiahla samoreplikujúca JavaScript worm kampaň

Wikimedia Foundation riešila bezpečnostný incident, pri ktorom sa na platforme objavil samoreplikujúci JavaScript worm, ktorý automaticky upravoval používateľské skripty a vandalizoval stránky na Meta-Wiki. Červ sa šíril tak, že po spustení v prehliadači prihláseného editora injektoval škodlivý kód do globálneho skriptu MediaWiki:Common.js a do používateľských common.js súborov, čím zabezpečil ďalšie šírenie medzi používateľmi. Počas incidentu bolo upravených približne 3 996 stránok a kompromitovaných asi 85 používateľských skriptov, pričom Wikimedia dočasne obmedzila editovanie a následne škodlivý kód odstránila. Podľa nadácie bol skript aktívny približne 23 minút, počas ktorých došlo iba k vandalizácii obsahu a neexistujú dôkazy o úniku osobných údajov.

https://www.bleepingcomputer.com/news/security/wikipedia-hit-by-self-propagating-javascript-worm-that-vandalized-pages/

Chrome chyba umožnila škodlivým rozšíreniam získať vyššie oprávnenia cez Gemini panel

Bezpečnostní výskumníci odhalili zraniteľnosť v Google Chrome (CVE-2026-0628, CVSS 8.8), ktorá mohla umožniť škodlivým rozšíreniam eskalovať oprávnenia a získať prístup k citlivým dátam vrátane lokálnych súborov. Chyba súvisela s nedostatočným presadzovaním bezpečnostných politík v komponente WebView a mohla byť zneužitá prostredníctvom Gemini side panelu, kde útočník dokázal spustiť vlastný JavaScript kód a obísť štandardný bezpečnostný model rozšírení. Google zraniteľnosť opravil v aktualizácii Chrome vydanej začiatkom roka 2026 a používateľom odporúča aktualizovať prehliadač na najnovšiu verziu, aby sa predišlo potenciálnemu zneužitiu.

https://thehackernews.com/2026/03/new-chrome-vulnerability-let-malicious.html