Cybersecurity Report

9.2.2026 – 22.2.2026

Útočníci zneužívajú falošné Google Forms na krádež prihlasovacích údajov

Útočníci aktívne používajú falošné stránky pripomínajúce Google Forms, ktoré imitujú legitímne dotazníky alebo webové formuláre s cieľom zbierať prihlasovacie údaje a iné citlivé informácie od obetí. Podvody fungujú tak, že používateľov presmerujú na stránku s doménou navrhnutou tak, aby vyzerala dôveryhodne a obsahovala formulár, ktorý po vyplnení odovzdá útočníkom zadané údaje, vrátane e-mailov a hesiel. Tieto kampane často cielia na organizácie či zamestnancov prostredníctvom sociálneho inžinierstva (napr. „overenie účtu“, “dôležitý interný formulár”), pričom používatelia nevedia odlíšiť falošný formulár od legitímneho Google Forms rozhrania.

https://cybersecuritynews.com/threat-actors-using-fake-google-forms-site/

Výskum ukazuje, že Copilot a Grok môžu neúmyselne vyzradiť interné kódy a tajomstvá

Nový výskum odhalil, že niektoré AI asistenti vrátane GitHub Copilot a Anthropic Grok môžu pri nesprávnom použití neúmyselne vyzradiť interné kódy, API kľúče, tokeny či ďalšie tajné údaje, pokiaľ ich modely boli trénované na dátach obsahujúcich takéto citliviny alebo ak používatelia neposkytujú primerané bezpečnostné obmedzenia vo svojich promptoch a prostrediach. Analýza ukázala, že AI generované odpovede môžu reflektovať vzory z trénovacích datasetov alebo recall mechanizmov, čo potenciálne vedie k úniku tajomstiev pri opakovaných či komplexných dopytoch a naznačuje, že organizácie by mali pri nasadzovaní LLM riešení dôsledne filtrovať dáta, striktne obmedziť prístupové rozsahy a implementovať bezpečnostné guardraily, aby zabránili prosakujúcemu úniku interných informácií.

https://thehackernews.com/2026/02/researchers-show-copilot-and-grok-can.html

Kyberútoky na poľskú energetiku zasiahli infraštruktúru veterných a solárnych zdrojov

Poľské úrady potvrdili, že koordinovaný kyberútok cielil na energetickú infraštruktúru krajiny vrátane veterných a solárnych zariadení, pričom útočníci sa zamerali na dodávateľské reťazce a priemyselné ovládacie systémy. Útoky spôsobili narušenie monitorovania a riadenia niektorých zariadení a aktéri pri tom využili kombináciu slabo zabezpečených sieťových rozhraní, kompromitovaných dodávateľských prístupov a zraniteľností v priemyselných protokoloch, čo demonštruje pretrvávajúce riziko pre kritickú infraštruktúru. Incident prinútil organizácie zvýšiť dohľad, segmentovať sieťové prostredia OT/IT a implementovať silnejšie autentifikačné a detekčné mechanizmy pre SCADA/ICS systémy, aby sa minimalizovalo riziko podobných útokov v budúcnosti.

https://www.darkreading.com/threat-intelligence/poland-energy-attack-wind-solar-infrastructure

---

WordPress plugin s 900 000 inštaláciami obsahuje kritickú RCE zraniteľnosť

Populárny WordPress plugin (pravdepodobne s asi 900 000 aktívnymi inštaláciami) bol nájdený s kritickou *remote code execution* chybou, ktorá útočníkom umožňuje spustiť ľubovoľný kód na zraniteľnom webe bez autentifikácie. Tento typ zraniteľnosti je mimoriadne nebezpečný, pretože útočník môže získať kontrolu nad serverom, ovplyvniť obsah webu, inštalovať malware či pristupovať k citlivým dátam. Prevádzkovatelia webov s týmto pluginom by mali okamžite aktualizovať na opravenú verziu, prípadne dočasne deaktivovať plugin, ak záplata ešte nie je dostupná, a zvážiť implementáciu WAF/IPS pravidiel, aby sa znížilo riziko zneužitia tejto chyby v produkčnom prostredí.

https://www.bleepingcomputer.com/news/security/wordpress-plugin-with-900k-installs-vulnerable-to-critical-rce-flaw/

Štúdia odhaľuje, že 25 % webov zverejňuje heslá pri „obnove účtu“

Nový výskum ukazuje, že približne 25 % webových služieb má nesprávne implementované mechanizmy obnovy hesla, ktoré môžu neúmyselne zverejňovať alebo slabým spôsobom vystavovať používateľské heslá počas procesu resetu alebo overenia identity. Chyby v návrhu týchto mechanizmov zahŕňajú napríklad odosielanie skutočných hesiel v e-mailoch, používanie predvídateľných reset tokenov, alebo slabé overenie identity pred povolením resetu, čo vo výsledku výrazne zvyšuje riziko kompromitácie účtov, krádeže identity a ďalších následných útokov. Štúdia tým upozorňuje na potrebu bezpečných štandardov pre obnovu účtu — ako je časovo obmedzený jednorazový token (OTP), silné overenie identity, a nepoužívanie pôvodných hesiel vôbec v procese obnovenia — aby sa predišlo takýmto zraniteľnostiam v moderných webových službách.

https://thehackernews.com/2026/02/study-uncovers-25-password-recovery.html