TLP: CLEAR

Cybersecurity Report

31.03.2025 - 13.04.2025

Stories

Pozor na falošnú aplikáciu mParivahan, ktorá útočí na mobilných používateľov cez WhatsApp s cieľom kradnúť citlivé údaje

Kyberzločinci spustili kampaň s malvérom zameranú na používateľov Androidu tým, že sa vydávali za aplikáciu NextGen mParivahan od Ministerstva cestnej dopravy a diaľnic. Obete boli oklamané falošnými správami na WhatsAppe, aby si nainštalovali škodlivú aplikáciu, ktorá kradne dáta. Podľa spoločnosti Seqrite ide o pokročilejší malvér, ktorý cieli na SMS, sociálne siete a e-commerce správy. Malvér sa skrýva, odosiela dáta na servery pod kontrolou útočníkov a používa poškodené APK súbory (0x1998), aby obišiel nástroje ako Apktool a Jadx. Druhý variant ukladá informácie o serveri do knižnice .so, ku ktorej pristupuje cez natívny kód. Inštalácia je možná len na Androidoch verzie 9 a vyššie.

https://cybersecuritynews.com/beware-of-fake-mparivahan-app-attacking-mobile-users/

Google predstavuje protokol A2A, ktorý umožňuje AI agentom spolupracovať a automatizovať pracovné procesy

9.apríla 2025 spoločnosť Google predstavila Agent2Agent Protocol (A2A) – otvorený štandard, ktorý umožňuje AI agentom bezpečne komunikovať, zdieľať dáta a koordinovať úlohy naprieč podnikových systémami. A2A, podporovaný viac ako 50 partnermi, rieši problémy s interoperabilitou medzi agentmi od rôznych dodávateľov. Protokol je postavený na HTTP a JSON-RPC, ponúka bezpečnosť na úrovni podnikov, podporuje dlhodobo bežiace úlohy a pracuje s textom,

zvukom aj videom. Agenti používajú tzv. Agent Cards na zdieľanie svojich schopností a výmenu štruktúrovaných častí pre pokročilú spoluprácu. A2A tak umožňuje škálovateľnú a bezpečnú spoluprácu viacerých AI agentov v podnikových prostrediach.

https://cybersecuritynews.com/google-unveils-a2a-protocol-that-enable-ai-agents-collaborate/

Zraniteľnosť vo Windows Kerberos umožňovala útočníkom obísť bezpečnostnú funkciu a získať prístup k povereniam

Microsoft opravil zraniteľnosť CVE-2025-29809 vo Windows Kerberos, ktorá bola zverejnená počas aprílovej Patch Tuesday aktualizácie. S hodnotením 7.1 CVSS umožňuje lokálnym útočníkom obísť Windows Defender Credential Guard a získať prístup ku Kerberos povereniam kvôli nebezpečnému ukladaniu dát. Chybu nahlásil Ceri Coburn z NetSPI. Zatiaľ nebola zneužitá, ale odborníci ju považujú za pravdepodobnú hrozbu. Oprava zlepšuje spôsob, akým Kerberos spracováva autentifikačné údaje, vrátane aktualizácií komponentov Virtual Secure Mode. Záplaty pre Windows 10 (x64 aj 32-bit) ešte nie sú dostupné. Organizácie používajúce Virtualization-based Security by mali prekonfigurovať politiky a túto aktualizáciu uprednostniť.

https://cybersecuritynews.com/windows-kerberos-vulnerability/

Zraniteľnosť vo Windows Active Directory Domain Services umožňovala útočníkom zvýšiť oprávnenia

Microsoft zverejnil zraniteľnosť v Active Directory Domain Services s označením CVE-2025-29810, ktorá umožňuje útočníkom s nízkymi oprávneniami získať prístup na úroveň SYSTEM a potenciálne prevziať plnú kontrolu nad postihnutými systémami. Chyba bola opravená v rámci aprílovej Patch Tuesday aktualizácie, má hodnotenie Important s CVSS skóre 7.5 a spadá pod CWE-284: Nesprávne riadenie prístupu. Na zneužitie je potrebný sieťový útok s nízkymi oprávneniami bez interakcie používateľa, no pravdepodobnosť zneužitia je nižšia pre svoju vysokú zložitosť. Zraniteľnosť má dopad na dôvernosť, integritu

aj dostupnosť. Chybu nahlásil bezpečnostný výskumník Matthieu Buffet a zatiaľ neexistujú dôkazy o jej aktívnom zneužívaní. Záplaty sú dostupné pre väčšinu systémov, no aktualizácie pre Windows 10 (x64 aj 32-bit) ešte chýbajú. Odborníci odporúčajú záplatu urýchlene nasadiť, monitorovať autentifikačnú prevádzku a uplatňovať zásadu najmenších oprávnení.

https://cybersecuritynews.com/windows-active-directory-domain-vulnerability-let-attackers-escalate-privileges/

Microsoft posilňuje e-mailový ekosystém Outlooku na ochranu doručenej pošty

Od 5. mája 2025 bude Microsoft Outlook vyžadovať prísnejšie overovanie pre domény, ktoré denne odosielajú viac ako 5 000 e-mailov, aby zlepšil bezpečnosť doručenej pošty a dôveru používateľov. Odosielatelia s vysokým objemom správ musia dodržiavať protokoly SPF, DKIM a DMARC, ktoré overujú pravosť e-mailov a pomáhajú blokovať spoofing a phishing. Minimálne je vyžadovaná DMARC politika „p=none“, odporúčaná je však „p=reject“. Microsoft zároveň odporúča používať platné odosielacie adresy, poskytovať možnosť odhlásenia, udržiavať čisté zoznamy príjemcov a dodržiavať transparentné e-mailové praktiky. E-maily, ktoré nebudú v súlade s týmito požiadavkami, budú od mája smerované do priečinka nevyžiadanej pošty, neskôr ich bude Outlook úplne odmietať. Tieto zmeny majú znížiť množstvo spamu a zvýšiť doručiteľnosť a dôveryhodnosť v rámci e-mailového prostredia Outlooku.

https://cybersecuritynews.com/microsoft-strengthens-outlook/
