Cybersecurity Report

30.6.2025 – 13.7.2025

Stories

Kritická RCE zraniteľnosť v mcp-remote ohrozuje LLM nástroje

Závažná chyba CVE-2025-6514 (CVSS 9.6) v nástroji mcp-remote (verzie 0.0.5 až 0.1.15) umožňuje vzdialené spustenie ľubovoľných príkazov na systémoch, ktoré sa pripájajú k nedôveryhodným MCP serverom. Zraniteľnosť vzniká počas OAuth autorizácie, kde škodlivé servery môžu podsunúť PowerShell príkaz v parametri authorization_endpoint, čo vedie k vykonaniu napr. cmd.exe. Riešenie spočíva v okamžitej aktualizácii na verziu 0.1.16, používaní len HTTPS spojení a kontrole dôveryhodnosti MCP serverov.

https://cybersecuritynews.com/critical-mcp-remote-vulnerability-exposes-llm-clients/

Microsoft odstránil vysoké privilégiá v Microsoft 365 ako súčasť bezpečnostnej reform

Spoločnosť Microsoft oznámila úspešné odstránenie viac než 1 000 scenárov s vysokými privilégiami v rámci ekosystému Microsoft 365, čím ukončila vážnu bezpečnostnú slabinu umožňujúcu aplikáciám pristupovať k citlivému obsahu zákazníkov bez kontextu autentifikácie. Tento krok je súčasťou iniciatívy Secure Future Initiative, ktorá vychádza z princípu najnižších potrebných práv (least-privilege). Problém spočíval v zastaraných service-to-service autentifikačných protokoloch, ktoré poskytovali zbytočne široké oprávnenia. Microsoft redizajnoval architektúru a zaviedol obmedzené oprávnenia ako Sites.Selected namiesto Sites.Read.All, čím výrazne znížil bezpečnostné riziká pri kompromitácii služieb alebo úniku tokenov. Nová architektúra zahŕňa aj monitorovanie na identifikáciu prípadných zostávajúcich nadmerných oprávnení.

https://cybersecuritynews.com/microsoft-enhance-microsoft-365-security/

MacOS infostealery: Nová vlna útokov na Apple zariadenia

Kybernetická bezpečnosť čelí nárastu infostealer malvéru zameraného na macOS, ktorý útočníci čoraz častejšie využívajú na krádež prihlasovacích údajov, cookies a informácií z prehliadačov. Tento posun od tradičných Windows útokov súvisí s rastúcim nasadením Apple zariadení vo firmách. Najznámejšie malvéry ako Atomic Stealer, Poseidon, Cthulu a Banshee mesačne spracujú stovky miliónov prihlasovacích údajov a využívajú platformovo špecifické techniky vrátane falošných systémových výziev cez AppleScript. Po infikovaní zneužívajú nástroje ako system_profiler na zber údajov o zariadení a cez HTTP POST posielajú údaje na útočnícke servery. Cielene kradnú údaje z Keychainu, Chrome, či Firefoxu, čím predstavujú vážnu hrozbu pre organizácie používajúce macOS.

https://cybersecuritynews.com/infostealers-actively-attacking-macos-users/

Kritická chyba v Linux kerneli umožňuje lokálnu eskaláciu práv

V linuxovom kerneli (verzie 5.6-rc1 až 6.13-rc3) bola objavená závažná chyba typu double-free v module nftables pipapo, ktorá umožňuje neprivilegovaným útočníkom získať root prístup. Problém vzniká v dôsledku neinicializovanej premennej v funkcii nft_add_set_elem, ktorá vedie k poškodeniu pamäte pri spracovaní špeciálne upravených netlink správ. Útok prebieha v dvoch krokoch: najprv sa odstráni prvok zo setu (prvé free) a potom celý set (druhé free tej istej pamäte). Exploit využíva túto chybu na obídenie KASLR a vytvorenie ľubovoľného zápisu do pamäte. Ohrozené sú systémy, kde je CONFIG_INIT_STACK_ALL_ZERO zakázané.

https://cybersecuritynews.com/linux-kernel-double-free-vulnerability/

Zraniteľnosť obchádzania nástroja Windows BitLocker umožňuje útočníkom obísť bezpečnostnú funkciu

Zraniteľnosť CVE-2025-48818 (CVSS 6.8) v BitLocker šifrovaní umožňuje fyzickým útočníkom obísť ochranu cez TOCTOU (time-of-check to time-of-use) útok. Chyba zasahuje Windows 10, 11 a Server a umožňuje získať prístup k šifrovaným dátam bez autentifikácie. Microsoft vydal bezpečnostné záplaty (KB5062552, KB5062553, KB5062554, KB5062560), ktoré by organizácie mali ihneď nasadiť. Útok nevyžaduje žiadnu interakciu používateľa a je možný len pri priamom fyzickom prístupe k zariadeniu.

https://cybersecuritynews.com/windows-bitlocker-bypass-vulnerability/