TLP:CLEAR

Prehľad bezpečnostných udalostí csirt.upjs.sk 18.2.2025 – 22.2.2025

Apple odstraňuje end-to-end šifrovanie iCloudu v Spojenom kráľovstve

Spoločnosť Apple prestala v Spojenom kráľovstve ponúkať funkciu Advanced Data Protection (ADP), ktorá poskytuje end-to-end šifrovanie pre iCloud dáta. Tento krok nasledoval po tajnom príkaze britskej vlády, ktorá požadovala vytvorenie zadných vrátok pre prístup k nezašifrovaným údajom používateľov. Pre nových používateľov v Spojenom kráľovstve je funkcia ADP odteraz nedostupná, zatiaľ čo existujúci používatelia budú musieť túto funkciu deaktivovať, aby mohli naďalej používať svoje iCloud účty. Napriek tomu zostávajú niektoré dáta, ako napríklad iCloud Keychain a údaje z aplikácie Health, naďalej chránené end-to-end šifrovaním.

Falošné aktualizácie pre Mac

Výskumníci spoločnosti Proofpoint identifikovali dve nové kybernetické hrozby, označené ako TA2726 a TA2727, ktoré sa podieľajú na kampaniach využívajúcich škodlivé webové injekcie. Tieto kampane často používajú falošné výzvy na aktualizáciu softvéru, aby oklamali používateľov a prinútili ich stiahnuť škodlivý softvér. Zatiaľ čo TA2726 funguje ako distribučná služba pre iných útočníkov, TA2727 priamo šíri rôzne malvéry, vrátane nového škodlivého softvéru pre macOS nazvaného FrigidStealer. Tento malvér je schopný kradnúť citlivé informácie z infikovaných zariadení.

Microsoft testuje opravu chyby v systéme Windows 11, ktorá narúša SSH pripojenia

Spoločnosť Microsoft začala testovať opravu pre dlhodobý problém v systéme Windows 11 verzií 22H2 a 23H2, ktorý spôsobuje zlyhávanie SSH pripojení. Tento problém sa objavil po inštalácii októbrovej bezpečnostnej aktualizácie v roku 2024, kde služba OpenSSH nedokázala naštartovať bez podrobného logovania, čo vyžadovalo manuálny zásah na spustenie procesu sshd.exe. Microsoft teraz testuje opravu v zostave Windows 11 Build 26100.3321 (KB5052093) pre Insiderov v kanáli Release Preview na verzii Windows 11 24H2. Do dostupnosti oficiálnej opravy môžu postihnutí používatelia dočasne vyriešiť problém úpravou prístupových práv (ACL) pre adresáre C:\ProgramData\ssh a C:\ProgramData\ssh\logs, aby umožnili plnú kontrolu pre systémové účty a skupinu administrátorov, pričom autentifikovaným používateľom poskytnú len čítacie práva.

OpenAI zmazala účty zneužívajúce ChatGPT na sledovanie a ovplyvňovanie

Spoločnosť OpenAI zablokovala účty používateľov z Číny a Severnej Kórey, ktorí zneužívali technológiu ChatGPT na škodlivé účely, ako sú sledovanie a ovplyvňovanie verejnej mienky. Tieto aktivity zahŕňali generovanie protizápadných článkov v španielčine, ktoré boli publikované v latinskoamerických médiách pod menom čínskej spoločnosti, a vytváranie falošných pracovných profilov s cieľom získať zamestnanie v západných firmách. OpenAI použil vlastné AI nástroje na identifikáciu týchto operácií a následne zablokoval príslušné účty.

Google Chrome deaktivuje uBlock Origin pre niektorých používateľov v rámci prechodu na Manifest V3

Spoločnosť Google pokračuje v postupnom vypínaní rozšírení založených na Manifest V2, ako je uBlock Origin, v prehliadači Chrome. Tento krok je súčasťou prechodu na Manifest V3, novú špecifikáciu rozšírení, ktorá obmedzuje prístup rozšírení k sieťovým požiadavkám používateľov a zakazuje využívanie vzdialeného obsahu, čo má zlepšiť celkový výkon a bezpečnosť. Avšak tieto zmeny zároveň znižujú funkčnosť niektorých rozšírení, najmä tých zameraných na blokovanie reklám a ochranu súkromia. Vývojár uBlock Origin, Raymond Hill, vytvoril verziu uBlock Origin Lite, ktorá je kompatibilná s Manifest V3, avšak táto verzia má obmedzené možnosti filtrovania v dôsledku nových obmedzení.