Cybersecurity Report

23.3.2026 – 5.4.2026

Apple rozširuje núdzovú aktualizáciu iOS 18.7.7 na ochranu pred exploit kitom DarkSword

Apple vydal rozšírenú aktualizáciu iOS/iPadOS 18.7.7 pre širší rozsah zariadení s cieľom eliminovať hrozbu exploit kitu DarkSword, ktorý je aktívne zneužívaný v reálnych útokoch od júla 2025. DarkSword cieli na zariadenia s iOS 18.4 až 18.7 prostredníctvom watering hole útokov — obeť navštívi legitímnu, ale kompromitovanú webovú stránku, čo spustí reťazec exploitov bez nutnosti interakcie používateľa. Po úspešnom zneužití kit nasadzuje backdoor a nástroj na exfiltráciu dát, čím útočník získava perzistentný prístup k zariadeniu a možnosť krádeže citlivých informácií. Situáciu zhoršuje fakt, že novšia verzia kitu unikla na GitHub, čo zvyšuje riziko masového zneužitia ďalšími aktérmi — vrátane skupiny COLDRIVER, ktorá kit už použila na distribúciu malvéru GHOSTBLADE.

https://thehackernews.com/2026/04/apple-expands-ios-1877-update-to-more.html

Supply-chain útok na Európsku komisiu cez kompromitovaný Trivy

Útočníci zo skupiny TeamPCP získali prístup k AWS účtu Európskej komisie zneužitím kompromitovanej verzie open-source nástroja Trivy, ktorú Komisia prijala cez bežné aktualizačné kanály. Prostredníctvom ukradnutého API kľúča exfiltrovali približne 92 GB komprimovaných dát vrátane mien, e-mailových adries a obsahu správ patriacich až 29 subjektom EÚ. Ukradnuté dáta sa následne objavili na dark webe na stránke skupiny ShinyHunters. Incident ilustruje rastúce riziko supply-chain útokov a potrebu overovania integrity nástrojov tretích strán v CI/CD pipeline.

https://therecord.media/european-commission-cyberattack-teampcp

Microsoft vynucuje upgrade Windows 11 24H2 na 25H2 pre nespravované zariadenia

Microsoft začal automaticky upgradovať všetky nespravované (mimo podnikovej správy) zariadenia s Windows 11 Home a Pro edíciou z verzie 24H2 na 25H2, pričom používateľ nemusí vykonať žiadnu akciu. Upgrade sa realizuje cez enablement balík menší ako 200 KB, ktorý aktivuje funkcie už predinštalované cez predchádzajúce kumulatívne aktualizácie — vyžaduje len jeden reštart. Dôvodom je blížiaci sa koniec podpory verzie 24H2 dňa 13. októbra 2026, po ktorom zariadenia prestanú dostávať bezpečnostné záplaty. Upgrade je možné dočasne odložiť cez nastavenia Windows Update, no nie natrvalo, spravované zariadenia (Intune, Endpoint Manager) nie sú dotknuté.

https://www.bleepingcomputer.com/news/microsoft/microsoft-now-force-upgrades-unmanaged-windows-11-24h2-pcs/

Expirácia ePrivacy výnimky v EÚ ohrozuje detekciu materiálu sexuálneho zneužívania detí

Dňa 3. apríla 2026 vypršala výnimka z ePrivacy smernice, ktorá technologickým spoločnostiam umožňovala dobrovoľne detekovať a nahlasovať CSAM pomocou hash-matching technológií. Google, Meta, Microsoft a Snap v spoločnom vyhlásení kritizujú zlyhanie inštitúcií EÚ pri dosiahnutí dohody a deklarujú, že budú vo svojich komunikačných službách pokračovať v dobrovoľných opatreniach na ochranu detí aj napriek právnej neistote. Z bezpečnostného hľadiska regulatórne vákuum môže dočasne oslabiť schopnosť platforiem automatizovane identifikovať známy CSAM obsah v rámci EÚ.

https://blog.google/company-news/inside-google/around-the-globe/google-europe/reaffirming-commitment-to-child-safety/

Android rootkit NoVoice infikoval 2,3 milióna zariadení cez Google Play

Malvér NoVoice bol distribuovaný cez viac ako 50 legitímne vyzerajúcich aplikácií na Google Play (čističe, hry, galérie), ktoré nevyžadovali podozrivé oprávnenia a fungovali podľa popisu. Po spustení malvér využíval 22 exploitov na získanie root prístupu cez staršie Android zraniteľnosti (2016–2021), vypol SELinux a nahradil kľúčové systémové knižnice vlastnými wrappermi, čím získal kontrolu nad každou spustenou aplikáciou. Potvrdený payload kradol WhatsApp session dáta vrátane šifrovacích kľúčov, pričom infekcia prežíva aj factory reset. Zariadenia s bezpečnostnými záplatami od mája 2021 nie sú na známe exploity zraniteľné, staršie zariadenia vyžadujú reflash firmvéru.

https://www.bleepingcomputer.com/news/security/novoice-android-malware-on-google-play-infected-23-million-devices/