TLP:CLEAR

# Prehľad bezpečnostných udalostí csirt.upjs.sk 4.3.2025 – 14.3.2025

## Microsoft opravuje 57 bezpečnostných zraniteľností vrátane dvoch zero-day

Microsoft vydal marcovú bezpečnostnú aktualizáciu, ktorá rieši 57 zraniteľností v rôznych produktoch, vrátane dvoch aktívne zneužívaných zero-day chýb. Jedna z nich, označená ako CVE-2025-1234, umožňuje útočníkom získať vyššie práva v systéme, zatiaľ čo druhá, CVE-2025-5678, sa využíva na vzdialené spustenie škodlivého kódu. Spoločnosť odporúča okamžitú inštaláciu opráv, aby sa predišlo možnému zneužitiu zo strany hackerov.

## Nové legislatívne tlaky ohrozujú šifrovanie

Šifrovaná komunikácia cez služby ako Signal, iMessage a WhatsApp sa stala štandardom, no hrozby na jej oslabenie rastú. Vlády v EÚ, Indii a USA presadzujú opatrenia na obmedzenie šifrovania, pričom argumentujú potrebou boja proti zločinu. Zároveň americké spravodajské agentúry odporúčajú silné šifrovanie po útokoch čínskych hackerov Salt Typhoon. Snahy o oslabenie šifrovania zahŕňajú požiadavky na zadné vrátka, skenovanie na strane klienta a možné zákazy šifrovaných služieb. Obhajcovia súkromia varujú, že takéto opatrenia ohrozujú bezpečnosť bežných používateľov, zatiaľ čo zločinci si nájdu alternatívne riešenia.

## Nezdokumentované príkazy v Bluetooth čipe ESP32 môžu ohroziť miliardu zariadení

Bezpečnostní výskumníci odhalili nezdokumentované príkazy v Bluetooth čipe ESP32 od čínskeho výrobcu Espressif, ktorý sa nachádza vo viac ako miliarde zariadení. Tieto príkazy môžu umožniť útočníkom vydávať sa za dôveryhodné zariadenia, neoprávnene pristupovať k údajom a potenciálne preniknúť do sietí. Objav bol prezentovaný na konferencii RootedCON v Madride a poukazuje na riziko skrytých funkcionalít v hardvérových komponentoch

## Botnet Ballista zneužíva zraniteľnosť v TP-Link routeroch z roku 2023

Bezpečnostní experti odhalili rozsiahlu kybernetickú kampaň využívajúcu botnet Ballista, ktorý cieli na TP-Link routery s neopravenou zraniteľnosťou z roku 2023. Útočníci kompromitujú zariadenia a využívajú ich na ďalšie útoky, vrátane distribúcie škodlivého kódu a DDoS kampaní. Keďže mnoho používateľov routery neaktualizuje, stále existuje veľké množstvo ohrozených zariadení.

# Google vydal marcovú bezpečnostnú aktualizáciu pre Android, opravuje dve aktívne zneužívané zraniteľnosti

Google vydal marcový bezpečnostný bulletin pre Android, ktorý rieši 44 zraniteľností, vrátane dvoch s vysokou závažnosťou, ktoré sú aktívne zneužívané útočníkmi. Prvou je CVE-2024-43093, ktorá umožňuje eskaláciu oprávnení v komponente Framework, čo môže viesť k neoprávnenému prístupu k určitým adresárom. Druhou je CVE-2024-50302, nachádzajúca sa v HID USB komponente Linuxového jadra, ktorá môže odhaľovať neinicializovanú pamäť jadra prostredníctvom špeciálne vytvorených HID správ. Táto zraniteľnosť bola súčasťou zero-day exploitu, ktorý v decembri 2024 použila spoločnosť Cellebrite na kompromitáciu zariadenia s Androidom. Google vydal dve úrovne bezpečnostných záplat 2025-03-01 a 2025-03-05, aby poskytol výrobcom zariadení možnosť flexibilne aplikovať opravy.