

Oblúbené Android aplikácie ticho posielajú vašu presnú polohu reklamným agentom

6.8.2026 - Tomáš Kanálik | Zajtra studio spol.

Dávate aplikáciám na predpoveď počasia, navigáciu či iným užitočným nástrojom povolenie na prístup k polohovým službám s cieľom získať presné informácie pre vaše okolie? Nové zistenia odhaľujú, že toto nevinné povolenie môže nevedomky otvoriť dvere masívnemu a nekontrolovanému zberu osobných dát.

Podľa najnovšej správy známej neziskovej organizácie *Electronic Frontier Foundation (EFF)*, o ktorej informuje *Android Authority*, totiž mnohé z oblúbených Android aplikácií ticho unikajú presné polohové údaje používateľov a posielajú ich priamo do rúk reklamných spoločností a brokerov s dátami.

Na vine nie sú priamo autori aplikácií, ale vývojárske balíčky

Zaujímavým a zároveň znepokojujúcim zistením je, že za týmto zberom dát vo väčšine prípadov nestojí priamy zlý úmysel vývojárov samotných aplikácií. Hlavným vinníkom sú takzvané vývojárske softvérové balíčky tretích strán, známe pod skratkou **SDK** (Software Development Kits).

Zdroj: Miroslav Schwamberg

Vývojári ich bežne používajú na jednoduchú integráciu hotových funkcií – od zobrazovania reklám cez meranie ich výkonu až po monetizáciu softvéru, čím si šetria čas pri písaní vlastného kódu od nuly. Analýza organizácie EFF však upozorňuje na to, že mnohé reklamné SDK balíčky majú funkciu zberu a zdieľania presných GPS súradníc predvolene zapnutú bez toho, aby na to tvorcovi aplikácie výrazne upozornili.

Jedno povolenie pre všetkých a neviditeľný zber dát

Základné úskalie ochrany súkromia v systéme Android spočíva v princípe, kde jedno povolenie platí pre všetky súčasti aplikácie. Ak napríklad aplikácii povolíte prístup k polohe, aby vám ukázala presné zrážky vo vašom meste, toto rozhodnutie automaticky sprístupní vaše súradnice aj všetkým integrovaným nástrojom tretích strán.

Používateľ žije v domnení, že uzavrel dôveryhodnú dohodu výhradne s tvorcom aplikácie, no v pozadí sa k jeho dátam dostáva neviditeľná sieť reklamných systémov. V minulosti sa pritom presné polohové dáta získané z reklamného prostredia zneužívali na sledovanie vojenského personálu, vyšetrovanie či rôzne spy-nástroje, čo celému odhaleniu dodáva mimoriadne vážny rozmer.

Rýchle riešenie existuje, no vyžaduje aktívny prístup

Vo svojej podrobnej analýze EFF priamo označila štyri známe reklamné balíčky, ktoré vo svojich základných nastaveniach automaticky zhromažďujú a zdieľajú polohové dáta používateľov. Ide o systémy **InMobi**, **BidMachine**, **HyBid** od spoločnosti Verve a **Petal Ads** od čínskeho giganta Huawei.

Dobrou správou je, že vývojári aplikácií majú možnosť tieto nežiaduce funkcie v nastaveniach SDK

manuálne vypnúť ešte pred zverejnením aplikácie. Hlavným problémom však zostáva, že tieto prepínače bývajú ukryté hlboko v konfiguráciách. Odborníci preto apelujú na vývojárov, aby dôkladne preverovali každý kód tretej strany, a zároveň vyzývajú regulátorov k prísnejšej kontrole firiem, ktoré skrytý zber osobných dát podporujú.

Nemali by ste prehliadnuť:

- **Kedy uvidíme skladací iPhone Ultra a prémiový iPhone 18 Pro?**
- **Google Asistent končí. Od septembra začne z androidov miznúť**
- **CMF Clip Pro: Otvorené slúchadlá s ovládaním na puzdre a cenou pod 80 eur**

<https://www.mojandroid.sk/oblubene-android-aplikacie-ticho-posielaju-vasu-presnu-polohu>