Telefon od Googlu by měl hlásit výchozí polohu každých 15 minut, i když je GPS vypnutá

necenzurovanapravda.cz/2024/10/telefon-od-googlu-by-mel-hlasit-vychozi-polohu-kazdych-15-minut-i-kdyz-je-gps-vypnuta

9 října, 2024

Má být podobně „vybavený“ telefon v budoucnu zcela běžným, aby jej bylo možné využít ke sledování mas? Vždyť OSN 2,0 stanovila chytrý mobilní telefon jako „lidské právo.“ Nebude to nakonec povinnost?

Mobilní telefon by totiž měl obsahovat vše o vaší osobě – tedy vaši ID, která má být v bezhotovostní společnosti propojena s digitální měnou i systémem sociálních kreditů.

A jak jinak zjistit, zda se při klimatickém či pandemickém lockdownu daný jedinec nevzdálil ze svého 15minutového města, než právě na základě polohy jeho mobilu?

Možná si řeknete, že mobil nikdo nemusí mít s sebou. Jenže pokud bude fungovat jako doklad, bude to povinnost. Lze tedy velmi lehce předpovědět, nač má nový mobil od společnosti Google sloužit…

Technologičtí experti testovali nový Google Pixel 9 a odhalili šokující detaily. Informuje o tom i zpravodajský magazín Forbes .

Podezření, že mobilní telefony špehují uživatele, dostává další potvrzující důkazy. Údajně se zaznamenávají a přenášejí nejen údaje o poloze, ale také telefonní číslo, e-mailová adresa a další telemetrická data.

To, co se Google pomocí svých telefonů Pixel dotazuje a každých 15 minut hlásí „domov“(což znamená samotný Google a ne domov uživatele), bylo prozkoumáno a zdokumentováno redakční skupinou z „Cybernews.“

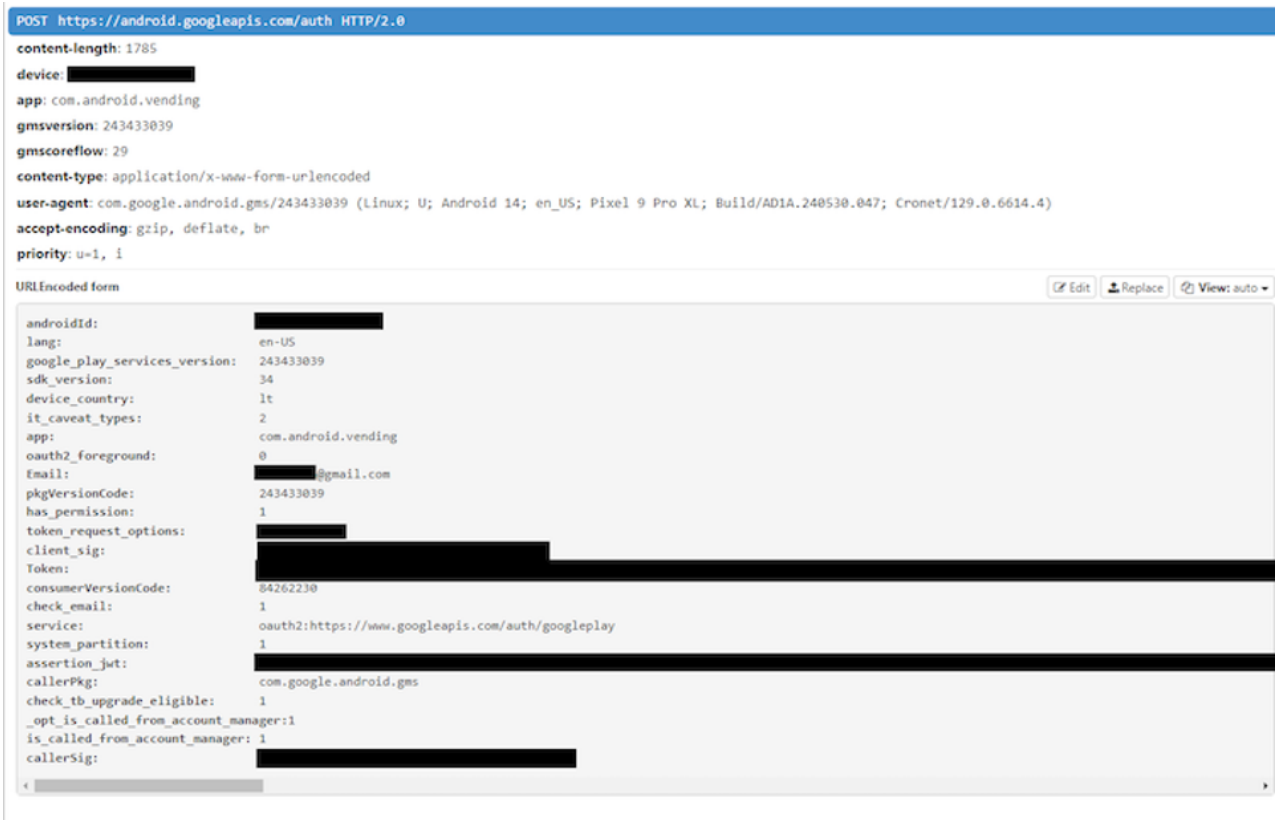
Kromě neustálých upozornění se telefony také pokoušejí stáhnout a spustit nový kód, což představuje další bezpečnostní riziko.

Byl analyzován datový provoz zcela nového mobilního telefonu Pixel 9 Pro XL s novým účtem Google a výchozím nastavením. Bylo také možné dešifrovat obsah dat, která byla odeslána do Googlu.

Autoři popisují obsah těchto datových balíčků jako „obzvláště citlivá data," protože jsou vhodná k tomu, aby bylo možné vyvozovat přesné závěry o životě příslušného zákazníka.

> „Každých 15 minut odešle Google Pixel 9 Pro XL datový paket do Googlu. Zařízení sdílí polohu, e-mailovou adresu, telefonní číslo, stav sítě a další telemetrická data.
>
> Ještě znepokojivější je, že telefon se pravidelně pokouší stáhnout a spustit nový kód, což může představovat bezpečnostní riziko."
>
> *Cybernews*

Zobrazení shromážděných a přenášených dat:



Redakce zjistila, že údaje o poloze byly také zaznamenány a přeneseny do Googlu, i když byla deaktivována GPS na mobilním telefonu.

Poloha pak byla načtena z okolních WiFi sítí a odhadnuta.

Zařízení Pixel se také připojovalo ke službám, které uživatel nepoužíval a ke kterým nebyl udělen výslovný souhlas. Jedním příkladem jsou „koncové body seskupování tváří“ – což vyvolává obavy o soukromí.

Zaměstnanci Cybernews nikdy nespustili aplikaci pro fotografie na svém testovacím mobilním telefonu, nikdy nepořídili žádné fotografie – a v telefonu nebyly uloženy žádné fotografie.

Na dotaz Google obvinění odmítl. Všechny tyto funkce údajně můžete vypnout.

> Bezpečnost uživatelů a soukromí jsou hlavní priority Pixelu. Sdílení dat, oprávnění aplikací a další můžete spravovat během nastavování zařízení a v nastavení.
>
> Tato zpráva postrádá zásadní kontext, chybně vykládá technické podrobnosti a plně nevysvětluje, že přenosy dat jsou vyžadovány pro legitimní služby na všech mobilních zařízeních bez ohledu na výrobce, model nebo operační systém, jako jsou aktualizace softwaru, funkce na vyžádání a přizpůsobené prostředí. .
>
> *Zpětná vazba od Googlu pro Forbes*

Závěr Cybernews však zní:

Množství přenesených dat a možnost vzdálené správy vzbuzují pochybnosti o tom, kdo zařízení skutečně vlastní.

Uživatelé za to možná zaplatili, ale hluboká integrace monitorovacích systémů do ekosystému může způsobit, že uživatelé budou zranitelní vůči únikům dat.