

Čo ukazuje Android Auto

Statická reverzná analýza balíka

com.google.android.projection.gearhead 17.9.664044, ako ho distribuuje GrapheneOS, a čo telefón odovzdá autu, ktoré nemá pod kontrolou.

82

OPRÁVNENÍ

55

EXPORTOVANÝCH KOMPONENTOV

3

DOMÉNY DŮVERY

01 Zhrnutie

03 Anatómia aplikácie

05 Čo opúšťa telefón

07 Kam to ide

09 Odporúčania

11 Dôkazy

02 Pôvod a metóda

04 Tri domény dôvery

06 Kedy sa to deje

08 Rozdiel GrapheneOS

10 Nad rámec nastavení

12 Podpora

Auto je samostatná strana, ktorá dostáva obsah z telefónu.

17.9.664044

base.apk · 35 123 449 bajtov

sha256 115228a7af416c4c...

sha256 podpisovateľa 1ca8dcc0bed3cbd8...b65b5295

ANALÝZA DOKONČENÁ

Zhrnutie

Android Auto je most a sám zbiera málo. Jeho vlastná sieťová stopa je malá. Najosobnejšie dáta telefónu prenáša cez hranicu, ktorú používateľ nekontroluje, na obrazovku vo vlastníctve výrobcu auta, a navyše si trvalo pamätá register každého auta, ktorému kedy dôveroval.

82 DEKLAROVANÝCH OPRÁVNENÍ	55 EXPORTOVANÝCH KOMPONENTOV	26 427 DEKOMPILOVANÝCH TRIED	65 DOSLOVNÝCH HOSTITEĽOV
16 NEBEZPEČNÝCH OPRÁVNENÍ	31 NIKDY NEUDELITEĽNÝCH	26 MB BAJTKÓDU DEX	1 LISTENER OZNÁMENÍ

Päť hlavných zistení

- Head unit vidí všetko, čo telefón vykresľuje, vrátane oznámení.** Android Auto deklaruje exportovanú `NotificationListenerService`, takže po udelení prístupu k oznámeniam môže čítať každé oznámenie na zariadení: správy, bankové upozornenia, jednorazové kódy. Auto dostane to, čo telefón vykreslí. **ZISTENÉ**
- Trvalo si ukladá register áut vrátane prístupových údajov.** Tabuľka `allowedcars` uchováva výrobcu, model, modelový rok, ID vozidla od head unitu, lokálne vygenerované náhodné ID klienta, adresu Bluetooth, SSID/BSSID siete WiFi a heslo WiFi auta, ďalej subjekt a sériové číslo certifikátu TLS head unitu. Uloženie hesla potrebuje bezdrôtové opätovné pripojenie a databáza je v privátnom úložisku aplikácie, ktoré iné aplikácie na GrapheneOS nečítajú. **ZISTENÉ**
- Vlastná telemetria ide cez Play services.** Android Auto obsahuje klienta Clearcut od Googlu a loguje pod zdrojom `CAR.ANALYTICS`, no nemá vlastný koncový bod na odosielanie, takže udalosti idú cez binder GMS. Analytický kanál preto prežije sandbox presne tak ako pri Play services. **ZISTENÉ**
- To, čo Google dostáva priamo, pochádza z priložených SDK.** Telemetria Maps SDK, sieťová poloha (`clients4.google.com/glm/mmap`), ping reklám (`gen_204?id=gmob-apps`), hlas Asistenta cez gRPC a príznaky Phenotype. Takmer nič z toho nie je špecifické pre Android Auto, ide o dôsledok vloženia SDK od Googlu. **ZISTENÉ**
- Sandbox pomáha len pri oprávneniach, ktoré odmietnete.** 31 z 82 oprávnení je signature/privileged a nikdy sa neudelí. Zvyšok (SMS, kontakty, zoznam hovorov, kalendár, poloha, mikrofón) sú výzvy za behu, ktoré môžete odmietnuť, za cenu funkcií, ktoré ich potrebujú. **ODVODENÉ**

Čo sa s tým dá robiť. Sekcia 09 uvádza nastavenia, ktoré existujú dnes, a najväčší prínos má spustenie Android Auto vo vlastnom profile. Sekcia 10 ide ďalej: filtrovanie siete, vypínanie komponentov, úprava APK a patch GrapheneOS. Vlastná sieťová stopa Android Auto je malá, takže filtre veľa nezískajú. Android už dnes umožňuje filtrovať, čo listener Android Auto číta, podľa kategórie aj aplikácie, takže najužitočnejší patch, ktorý zostáva, je zoznam povolených domén pre aplikáciu v OS. Väčšinu ostatného som overil otváraním obrazoviek na zariadení a nič z toho som netestoval zmenou nastavení.

Rozsah. Iba statická analýza APK; nebolo žiadne živé zachytávanie a nebol pripojený žiadny head unit. **ZISTENÉ** znamená, že tvrdenie vedie k súboru a riadku v prílohe. **ODVODENÉ** znamená úvahu nad týmito dôkazmi. Čo robí výrobca auta s pixelmi, ktoré dostane, je mimo dosahu akéhokoľvek APK, a report to preto nedomýšľa.

02

Pôvod a metóda

Artefakt je oficiálny Android Auto podpísaný Googlom z vlastného repozitára GrapheneOS. Každý bajt bol pred čítaním overený voči podpísaným metadátam repozitára.

POLOŽKA	HODNOTA
Repozitár	https://apps.grapheneos.org/ · metadata.1.0.0.sjson
Balík	com.google.android.projection.gearhead · versionCode 179664044 · 17.9.664044-release
Kanál / SDK	stable · minSdk 32 · iba arm64-v8a
base.apk	35 123 449 bajtov · sha256 115228a7af416c4c... (zhoduje sa s metadátami)
Podpisovateľ	CN=Android, O=Google Inc. · sha256 1ca8dcc0bed3cbd8...b65b5295 (zhoduje sa s metadátami)
Splity	config.arm64_v8a (8,8 MB, natívne knižnice) · config.xxhdpi · config.en
Obsah	4 DEX · 26 MB bajtkódu · 148 023 reťazcov · 543 assetov · 8,7 MB natívneho kódu (split arm64)

Poznámka z repozitára, citát. „Oficiálne vydanie Android Auto bez úprav. Po inštalácii treba Android Auto nastaviť v *Settings > Apps > Sandboxed Google Play > Android Auto*." Tento prepínač udeľuje sandboxovanej aplikácii profil projekcie.

Čo sa urobilo

Rozbalenie	apktool pre manifest a zdroje; surový zip pre assety a natívne knižnice
Reťazce	tabuľky reťazcov DEX parované priamo (148 023 položiek), z nich vytiahnutí hostitelia a URL

Kód	jadx 1.5.6, úplný prechod: 26 427 tried, 176 MB Javy, potom cielené čítanie projekcie, správ, telekomunikácií, telefónie, telemetrie a databázy áut
Politika	úrovne ochrany oprávnení porovnané s vetvou 17 GrapheneOS frameworks/base
Rozsah	base + 3 config splity; GMS a Play Store len ako kontext pre kanál binder

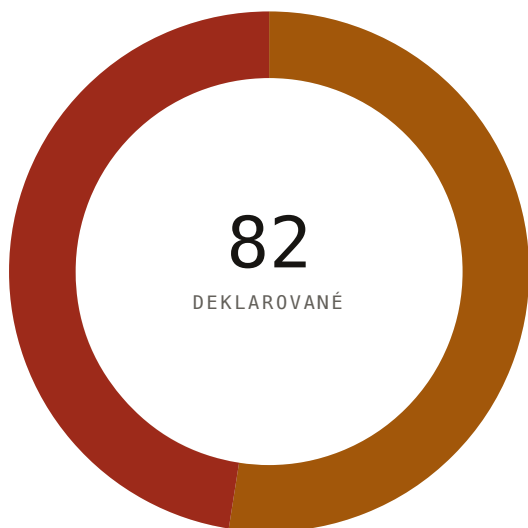
Čo sa nepodarilo zistiť

- Čo head unit zaznamenáva. Auto je z definície čierna skrinka; report pokrýva iba to, čo sa mu posiela.
- Presný formát prenosu projekčného spojenia. TLS sa používa a certifikát auta je pripnutý, ale samotné dáta tvorí proprietárny protokol prenášaný cez USB accessory / TCP.
- Či sa stípec s heslom WiFi auta niekde inde pred vložením nešifruje. Vkladacia cesta uloží hodnotu priamo, ale obal by ju mohol šifrovať (žiadny sa nenašiel). V sandboxe GrapheneOS a pri šifrovaní úložiska zariadenia je to dôsledok návrhu, nie nález.
- Akékoľvek uchovávanie alebo spájanie na strane Googlu.

03

Anatómia aplikácie

Android Auto je štíhlejší než Play services, má 196 komponentov namiesto 1 310, ale oprávnenia, o ktoré žiada, sú tie, na ktorých záleží. Je to veľmi prepojené používateľské rozhranie.



Obrázok 1: 82 oprávnení: dajú sa niekedy udeliť?

Profil oprávnení

Iba 31 je signature/privileged a 8 je mimo AOSP. Väčšinu, 23 normálnych a 16 nebezpečných, tvorí množina, ktorú rozhranie pre šoféra potrebuje a ktorú môže používateľ odovzdať.

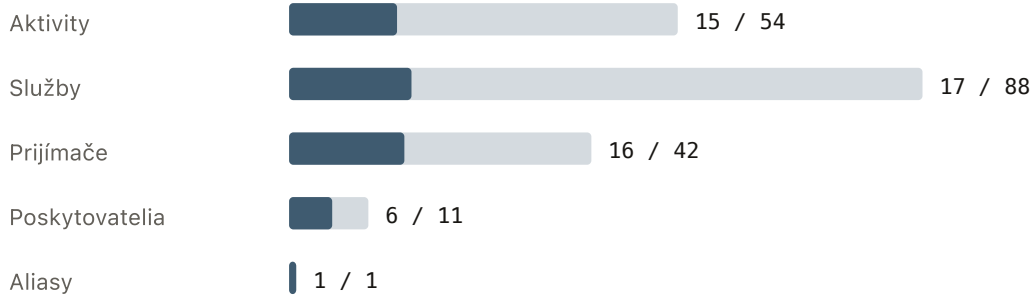
Chýbajú tri oprávnenia: `AD_ID`, `READ_SMS` (deklarované iba prijímanie a odosielanie) a poloha na pozadí. Nebezpečné oprávnenia pokrývajú SMS, kontakty, zoznam hovorov, kalendár, presnú polohu, mikrofón a stav telefónu.



■ normálne · 23 ■ nebezpečné · 16 ■ špeciálne · 12 ■ signature/privileged · 31 ■ mimo AOSP · 8

Obrázok 2: tých istých 82 oprávnení podľa úrovne ochrany

Povrch útoku



Obrázok 3: deklarované vs. exportované komponenty (exportované / spolu)

196 komponentov, z toho 55 exportovaných. Dôležitejšie než aktivity sú listenery, ktoré Android Auto dávajú dosah: listener oznámení, služba počas hovoru, prehliadač médií, služba sprievodného zariadenia a most chimera do Play services.

```
AndroidManifest.xml
com.google.android.gearhead.notifications.SharedNotificationListenerManager$ListenerService
    android:permission="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE"
com.google.android.apps.auto.components.telecom.service.CarProjectionInCallServiceImpl
com.google.android.apps.auto.components.ace.AceInsightRendererService (osobný kontext Androidu 16)
com.google.android.apps.auto.carservice.gmscorecompat.CarChimeraService
    action="com.google.android.gms.car.service.START"
```

Hlavná expozícia. Listener oznámení číta obsah každého oznámenia z každej aplikácie, aj z tých, ktoré inak obsah zámerne nezverejňujú. Android Auto premieta oznámenia do auta zo svojej podstaty. Otázka súkromia je, či je auto dôveryhodný displej. [ZISTENÉ](#)

Nastavenia v manifeste

NASTAVENIE	ČO TO TU ZNAMENÁ
QUERY_ALL_PACKAGES	Deklarované. Je to normálne oprávnenie, takže Android Auto vie vypísať všetky nainštalované aplikácie bez výzvy. 16 dekompilovaných súborov sa dopytuje na balíky alebo intenty. ZISTENÉ
allowBackup="true"	Je zaregistrovaný <code>SettingsBackupAgent</code> . Jeho špecifikácia uvádza preferenčné súbory <code>carservice</code> a <code>common_user_settings</code> a kľúče launchera. Databáza <code>allowedcars</code> v tom zozname nie je, takže uložené heslá Wi-Fi touto cestou zrejme necestujú. Či sú zahrnuté ďalšie dáta, tu nie je vidieť. ZISTENÉ · NEZNÁME
cleartextTrafficPermitted="true"	Nešifrované HTTP je povolené pre všetky domény. Žiadna zo 63 nájdených URL nezačína <code>http://</code> . ZISTENÉ
sharedUserId	<code>com.google.android.projection.gearhead</code> . Všetky balíky tejto rodiny bežia ako jeden používateľ Linuxu. ZISTENÉ
special access	Deklarované sú <code>SYSTEM_ALERT_WINDOW</code> , <code>WRITE_SETTINGS</code> a <code>MANAGE_EXTERNAL_STORAGE</code> . ZISTENÉ

exported providers

6 z 11 je exportovaných. `SharedPreferencesProvider` nemá oprávnenie v manifeste, ale v kóde odmieta volajúcich, ktorí nemajú rovnaké UID ako Android Auto a nie sú balíkom podpísaným Googlom (`SharedPreferencesProvider.java`, metóda `b`), a dovoľuje čítať aj zapisovať hodnoty preferencií. Provider mikrofónu kontroluje `RECORD_AUDIO` a volajúci balík. Providery stavu projekcie, troubleshooteru a farieb sú exportované bez oprávnenia a podrobne sa neauditovali. [ZISTENÉ](#)

04

Tri domény dôvery

Každé tvrdenie o súkromí v Android Auto sa týka jednej z troch domén. Ich zamieňanie je dôvod, prečo si ľudia myslia, že „je to len displej“.



Telefón je jediná strana, ktorá komunikuje s oboma. Auto sa k Googlu nikdy nedostane priamo a Google nikdy nevidí obrazovku auta.

Čo si Android Auto pamätá o aute

Najviac prezrádza tabuľka SQLite `allowedcars`, do ktorej sa zapisuje vždy, keď sa head unitu udelí dôvera.

```

defpackage/sqm.java:24 (schéma, doslovne)
CREATE TABLE allowedcars (
  id, manufacturer, model, modelyear, vehicleid, vehicleidclient,
  headUnitProtocolMajorVersionNumber, headUnitProtocolMinorVersionNumber,
  bluetoothConnectionAllowed, connectiontime, nickname,
  bluetoothaddress, wifissid, wifiBssid, wifipassword, wifisecurity,
  wifiProjectionProtocolOnTcp, wifiProjectionProtocolIpAddress,
  wifiProjectionProtocolTcpPort, headUnitMake, headUnitModel,
  headUnitSoftwareBuild, headUnitSoftwareVersion, vehicleType)
  
```

```

defpackage/jtb.java:34          contentValues.put("wifipassword", ...) // stored as TEXT
com/google/android/gms/carsetup/CarInfoInternal.java:107
... bluetoothaddress=..., wifiSsid=..., wifiBssid=..., sslSubjectName=...,
  sslSerialNumber=..., hashedVehicleId=[REDACTED] ...
  
```

01

ID vozidla

Hlásí ho head unit a slúži na rozpoznanie auta medzi pripojeniami. Typicky ide o identifikátor triedy VIN; presný zdroj určuje protokol. [ZISTENÉ](#) (pole) · [ODVODENÉ](#) (VIN)

02

ID klienta vozidla

Generuje sa lokálne ako `Long.toHexString(new SecureRandom().nextLong())` a ukladá sa vedľa auta. Je to vlastný pseudonym Android Auto pre dané vozidlo, nezávislý od toho, čo hlási auto. **ZISTENÉ** jtb.java:128

03

Certifikát head unitu

`sslSubjectName` a `sslSerialNumber`: identita TLS, ktorú predkladá auto a ktorou sa pripína dôvera. Je to zároveň stabilný odtlačok konkrétneho head unitu. **ZISTENÉ** CarInfoInternal

04

Bezdrôtové prihlasovacie údaje

SSID, BSSID a heslo hotspotu pre bezdrôtovú projekciu, plus koncový bod TCP, keď auto komunikuje projekciou cez TCP. Pretrvávajú medzi reláciami, kým sa auto neodstráni zo zoznamu. **ZISTENÉ**

05

Analytická relácia

Každá relácia projekcie dostane ID, ktoré putuje s udalosťami Clearcut, takže Google vie telemetriu zoskupovať podľa jazdy, nie podľa dňa. **ZISTENÉ** AnalyticsSessionInfo

Problém prenajatého auta. Pri spárovaní prenajatého auta sa do `allowedcars` uloží jeho MAC Bluetooth, prihlasovacie údaje WiFi a sériové číslo certifikátu a obrazovka toho auta získa po dobu pripojenia prístup k vašim oznámeniam. Odstránenie auta zo zoznamu je opatrenie na ochranu súkromia.

05

Čo opúšťa telefón

Nasledujú dve tabuľky, jedna pre každého príjemcu. Auto a Google vidia rôzne dáta a ich zamieňanie je najčastejšia chyba v diskusiách o Android Auto.

Do head unitu

KANÁL	ČO PRECHÁDZA HRANICOU	PODMIENKA
Obrazovka	Vykreslené snímky premietaného rozhrania: navigácia, správy, kontakty, médiá, nastavenia, teda všetko, čo je práve na obrazovke.	vždy (v tom spočíva produkt)
Oznámenia	Obsah oznámení zo všetkých aplikácií: odosielateľa, text, akcie. Vráťane citlivých oznámení, ak ich OS nezakryje.	prístup k oznámeniam, ktorý udelil používateľ
Správy	Vlákná SMS/MMS, identita odosielateľa, texty správ; odpovede písané alebo diktované v aute.	RECEIVE_SMS, SEND_SMS, READ_CONTACTS
Kontakty	Mená, čísla, fotky, obľúbené, história hovorov pre telefonovanie.	READ_CONTACTS, READ_CALL_LOG

KANÁL	ČO PRECHÁDZA HRANICOU	PODMIENKA
Hovory	Stav hovoru, ID volajúceho, zvuk smerovaný cez mikrofón a reproduktory auta.	CALL_PHONE, služba počas hovoru
Kalendár	Udalosti a účastníci pre aplikáciu kalendára.	READ_CALENDAR
Médiá	Metadáta skladieb, obaly albumov, stromy prehliadania, ovládanie prehrávania.	prehliadač médií
Stav telefónie	Sila signálu a informácie o bunke, ak ich head unit neskryje.	READ_PHONE_STATE
Poloha	Pozícia na vykreslenie navigácie; auto dostane mapu, nie surové GPS, pokiaľ si ho nevyžiadate.	presná poloha

Do Googlu

KANÁL	KONCOVÝ BOD (AKO ZISTENÝ)	ČO ODCHÁDZA
Clearcut cez binder GMS	(žiadne lokálne odosielanie)	Udalosti pod zdrojom logov <code>CAR.ANALYTICS</code> : životný cyklus spojenia, chyby protokolu, diagnostika zvuku, stavy Bluetooth FSM, zamietnuté oprávnenia, príznaky funkcií. Nesú ID analytickej relácie a cez GMS aj Android ID a účet, ak je prítomný.
Asistent	assistant-maps.google.com gRPC cez GSA	Hlasový zvuk pri každom „Hey Google“ v aute plus kontext prepisu potrebný na odpoveď. Je to najväčší obsahový tok a zapína sa až použitím.
Maps / navigácia	mobilemaps-pa.googleapis.com mapsmobilesdfs- pa.googleapis.com autopush-navigationsdkusage...	Používanie máp, navigačné relácie, vyhľadávacie dotazy, vyhľadávanie miest (Places), metriky výkonu SDK.
Sieťová poloha	clients4.google.com/glm/mmap	Odtlačky buniek a WiFi odosielané na geolokáciu, keď GPS nie je k dispozícii. Je to klasické API polohy od Googlu.
Ping reklám	pagead2.googlesyndication. com/pagead/gen_204?id=gmob- apps	Ľahký maják reklamného SDK z priloženej knižnice mobilných reklám. Android Auto nedeclaruje oprávnenie AD_ID, takže reklamné ID mu nie je k dispozícii.
Konfigurácia	phenotype (cez GMS)	Sťahovanie príznakov a tokeny experimentov; ten istý kanál, aký opisuje report o Play services.
Atribúcia	InstallReferrerReceiver	Install referrer pri prvom spustení, ktorý ukazuje, ako sa inštalácia získala.
Spätná väzba	feedback-pa.googleapis.com	Hlásenia chýb a hodnotenia z podnetu používateľa vrátane snímok obrazovky, ak sú priložené.

Asymetria. Google dostáva telemetriu a hlas, auto obsah. Auto vidí vaše správy a Google vidí, ako sa aplikácia správala pri ich zobrazovaní. Riziká sú rozdielne a majú rôzne nápravy.

Používa Android Auto sám Play Integrity?

Žiadne volanie klienta sa nenašlo. V dekompilovanom kóde nie je import klienta DroidGuard ani Play Integrity a žiadne volanie API na token integrity. Slovo `DROIDGUARD` sa objavuje iba ako názov: položka v zozname hlavičiek požiadavky (`qda.java:20` používa `vji.DROIDGUARD`), tri názvy príznakov (`qgw.java:102-104`) a označenie chyby (`q xv.java:67`), všetko v priloženom kóde knižníc. **ZISTENÉ** Čítam to tak, že ide o priloženú knižnicu na účty a podpisovanie požiadaviek, ktorá to pole nesie, a samotné volanie, ak vôbec nejaké, robí Play services. **ODVODENÉ** Android Auto stále závisí od modulu aut v Play services a Play services atestáciu pre vlastné funkcie využívajú, ako opisuje report o Play services.

06

Kedy sa to deje

Android Auto riadia udalosti. Takmer nič sa nedeje na časovači; takmer všetko sa deje pri zapojení kábla alebo nadviazaní spojenia Bluetooth.

pripojenie USB	Podanie ruky accessory. Vyjednávane AOA (<code>USB_ACCESSORY_ATTACHED</code> , <code>ACCESSORY_HANDSHAKE</code>), výmena verzie protokolu, potom projekcia. ZISTENÉ
pripojenie BT	Bezdrôtový spúšťač. Udalosti spojenia ACL/headset prebudia cestu bezdrôtového nastavenia; uložené auto sa spáruje podľa adresy Bluetooth a certifikátu. ZISTENÉ
štart projekcie	Relácia sa otvára. Vytvorí sa ID analytickej relácie; záznam auta sa v <code>allowedcars</code> vytvorí alebo aktualizuje. ZISTENÉ
počas jazdy	Prúdy. Snímky videa, zvuk, oznámenia, stav telefónie a poloha tečú nepretržite. Udalosti Clearcut sa radia do fronty, ako vznikajú. ZISTENÉ
boot / aktualizácia	Opätovné nastavenie. Inicializácia komponentov pri <code>BOOT_COMPLETED</code> a <code>MY_PACKAGE_REPLACED</code> ; prijímač obnovy FRX; aktualizácia príznakov Phenotype. ZISTENÉ
prvá inštalácia	Atribúcia. Install referrer sa spracuje, potom aplikácia čaká na nastavenie. ZISTENÉ
na požiadanie	Hlas. Mikrofón sa otvorí iba pre reláciu Asistenta a potom sa zatvorí. ZISTENÉ

Žiadny nečinný maják. Na rozdiel od Play services nemá Android Auto vlastný 12-hodinový check-in. Jeho aktivita na pozadí je takmer nulová, kým sa neobjaví auto, takže otázka „kedy“ sa pri Android Auto redukuje na to, čo sa zapojilo.

Kam to ide

Celé APK má iba 65 doslovných hostiteľov, o rád menej než Play services, čo sedí aplikácii, ktorá prácu s cloudom deleguje.

HOSTITEĽ	ÚLOHA
<code>www.googleapis.com</code>	generická vstupná brána API Googlu, ktorú používajú priložené knižnice
<code>clients4.google.com/glm/mmap</code>	sieťová poloha (bunky/WiFi na súradnice)
<code>mobilemaps-pa.googleapis.com</code>	kanál telemetrie Maps
<code>mapsmobilesdks-pa.googleapis.com</code>	metriky používania Maps SDK
<code>autopush-navigationsdkusage.sandbox.googleapis.com</code>	telemetria používania Navigation SDK
<code>assistant-maps.google.com</code>	integrácia Asistenta pre mapy/navigáciu
<code>pagead2.googleadsyndication.com</code>	maják reklamného SDK (<code>gen_204</code>)
<code>www.google-analytics.com</code> · <code>ssl.google-analytics.com</code>	klasické koncové body Google Analytics
<code>feedback-pa.googleapis.com</code>	spätná väzba a hlásenia chýb od používateľov
<code>play.google.com</code>	odkazy do obchodu, výzvy na aktualizáciu
<code>support.google.com/androidauto</code>	články pomocníka otvárané vo WebView
<code>developers.google.com</code> · <code>console.developers.google.com</code>	odkazy na nastavenie kľúča Maps API zobrazované používateľom
<code>goo.gl</code>	krátke odkazy v texte pomocníka

Hostiteľ `play.googleapis.com` sa nevyskytuje, čo naznačuje, že Android Auto nemá vlastné odosielanie Clearcut. Trieda `PlayLoggerContext` je priložená, ale transportom je binder `GMS`, ako ukazujú podpis `CarTelemetryLogger` a most `com.google.android.gms.car.service.START`.

Ako čítať zoznam. Hostiteľ v APK neznamena prevádzku. Viaceré z nich sú dosiahnuteľné iba z priložených SDK, keď sa použije funkcia (navigácia, hlas, spätná väzba). Zoznam je horná hranica možností a neopisuje ustálenú prevádzku.

Rozdiel GrapheneOS

V GrapheneOS beží Android Auto v sandboxe Play. Expozíciu obsahu to mení menej, než by sa čakalo, a privilégiá viac, než by sa čakalo.

SCHOPNOSTĚ	PŮVODNÝ AOSP	SANDBOX GRAPHENEOS
Čítanie SMS / kontaktov / zoznamu hovorov	cez výzvy za behu	rovnako, ale každé sa dá samostatne odvolať a je auditované
Prístup k oznámeniam	prepínač používateľa	rovnako; nič ho neudelí potichu
Zachytenie zabezpečeného videa / pridanie dôveryhodného displeja	systémová aplikácia	zamietnuté (signature/privileged)
Správa USB / tetheringu	privilegované	zamietnuté pre privilegované cesty; režim accessory stále funguje
Privilegované operácie Bluetooth	áno	zamietnuté; platí bežné BLUETOOTH_CONNECT/SCAN
Čítanie privilegovaného stavu telefónu	áno	zamietnuté; iba výzva READ_PHONE_STATE
Prístup k sieti	vždy	odvolateľný pre väčšinu aplikácií, ale pre Android Auto zamknutý na zapnuté („Device requires this permission to operate“)
Lokálna sieť (bezdrôtová projekcia)	normálne	s výzvou: ACCESS_LOCAL_NETWORK je nebezpečné oprávnenie

Čo sandbox odoberá

- 31 oprávnení signature/privileged: zachytenie zabezpečeného videa, dôveryhodné displeje, virtuálne zariadenia, privilegovaný Bluetooth, privilegovaný stav telefónu.
- Tiché privilégiá na pozadí; Android Auto súperí s ostatnými aplikáciami.
- Možnosť stať sa systémovou súčasťou zážitku v aute.

Čo neodoberá

- Tok troch domén: obsah stále ide do auta, telemetria stále ide Googlu.
- Clearcut cez binder GMS.
- Hlas Asistenta, telemetria Maps, sieťová poloha.
- Všetko, čo udelíte za behu: SMS, kontakty, oznámenia, polohu, mikrofón.

Hranice sandboxu. Sandboxom sa privilegovaný komponent auta mení na aplikáciu s rovnakými právami ako ktorákoľvek iná. Pri produkte, ktorého úlohou je odovzdať dáta obrazovke tretej strany, to znižuje rozsah škôd, ale expozíciu to nerobí súkromnou. Dáta stále idú do auta.

Tri profily používateľ'a

PROFIL	ČO JE VYSTAVENÉ	RIZIKO
Iba kábel, správy zamietnuté	Navigácia a médiá do auta; telemetria Maps a Asistent (ak sa používa) do Googlu. Cez hranicu neprechádzajú žiadne správy, kontakty ani oznámenia.	NÍZKE obsah zostáva v telefóne
Bezdrôtovo + správy + oznámenia	Plná projekcia: správy, kontakty, oznámenia, hovory. Uložené prihlasovacie údaje auta. Telemetria za každú jazdu.	STREDNÉ auto sa stáva príjemcom dát
Prenajaté / zdieľané auto, všetko udelené	Všetko vyššie, na hardvéri, ktorý nevlastníte ani mu nedôverujete, a jeho prihlasovacie údaje zostanú potom uložené v telefóne.	VYSOKÉ obrazovka tretej strany s vašimi oznámeniami

09

Odporúčania

Zoradené podľa toho, koľko každý krok prinesie na jednotku nepohodlia. Žiadny z nich nevyžaduje vzdať sa navigácie a každá položka je nastavenie alebo funkcia, ktorá existuje dnes. Značky ukazujú, o čo sa tvrdenie opiera: **ZISTENÉ** v APK, na zariadení s GrapheneOS alebo v používateľskej príručke GrapheneOS, **ODVODENÉ** z videného, **NETESTOVANÉ** nevyskúšané na živom zariadení.

Kde klikat'

Názvy menu nižšie boli overené na zariadení s GrapheneOS (build 2026102101, Android 17) otváraním obrazoviek, nie ich zmenou. Rozcestník je **Settings > Apps > Sandboxed Google Play > Android Auto**. Obsahuje *Android Auto settings*, skupinu *Permissions* so štyrmi prepínačmi, *Android Auto app info*, *Notification access settings* a zoznam voliteľných závislostí (Google Maps, Speech Recognition & Synthesis, Google app). **ZISTENÉ**

CIEĽ	CESTA	NASTAVIŤ NA
Vybrať, ktoré balíky oprávnení Android Auto dostane	Android Auto > Permissions: <i>Allow permissions for wired Android Auto, for wireless Android Auto, Allow to reroute audio from device to the car, Allow permissions for handling phone calls</i>	Vypnúť balíky, ktoré nepoužívate (napríklad wireless, ak sa len pripájate káblom). Prepínače som neprepínal, takže čo ktorý odoberie, je NETESTOVANÉ .
Obmedziť, ktoré oznámenia môže auto čítať	Android Auto > Notification access settings > <i>Allow notification access</i> , potom kategórie <i>Real-time, Conversations, Notifications, Silent</i> a nakoniec <i>See all apps</i> (nadpis obrazovky „Apps shown on device“)	Odznačiť kategórie a každú aplikáciu, ktorú nechcete na displeji auta. Jedno políčko na aplikáciu.
Nepúšťať oznámenia ku Googlu	Android Auto settings > Messaging > <i>Notifications with Assistant</i> („Allow Android Auto to send your notifications to Google for features like playing your messages“)	Vypnúť, ak nechcete, aby Assistant čítal správy nahlas
Menej textu správ na displeji	Android Auto settings > Messaging > <i>Show message notifications, Show group conversations, Show first line of messages</i>	Vypnúť tie, ktoré nepotrebujete

CIEĽ	CESTA	NASTAVIŤ NA
Žiadne funkcie telefónu na zamknutom telefóne	Android Auto settings > Startup > <i>Start Android Auto while locked</i> („Access to your phone features will be available on the vehicle screen while locked“)	Vypnúť
Autá, ktoré si Android Auto pamätá	Android Auto settings > Connection > <i>Vehicles</i> (zoznam <i>Accepted vehicles</i> a <i>Rejected vehicles</i>)	Otvoriť záznam a odstrániť autá, ktoré už nepoužívate. Záznam som neotváral, takže presné znenie akcie odstránenia je NETESTOVANÉ .
Žiadne spúšťanie nastavenia pre neznáme autá	Tá istá obrazovka, <i>Add new vehicles to Android Auto</i>	Vypnúť, kým nepridávate auto (požičané autá)
Kontakty bez ich odovzdania	Android Auto > Android Auto app info > Permissions > <i>Contacts and accounts</i> > <i>Contact Scopes</i>	Zapnúť namiesto <i>Allow</i>
Mikrofón	Android Auto app info > Permissions > Microphone	<i>Don't allow</i> , ak nikdy nepoužívate hlas
Vlastný prístup Android Auto k sieti	Android Auto app info > Permissions > Network	Nedá sa zmeniť: <i>Allow</i> aj <i>Don't allow</i> sú sivé s textom „Device requires this permission to operate“. Použite vypínač siete pre Play services (report o Play services, „Kde klikat“).
Samostatný profil	Settings > Security & privacy > Privacy > Private space	Android Auto nastaviť tam

1. Dajte Android Auto vlastný profil

Príručka GrapheneOS hovorí, že Android Auto sa dá nastaviť v sekundárnom profile alebo v Private Space, z *Settings > Apps > Sandboxed Google Play > Android Auto* **ZISTENÉ**. Listener oznámení dostáva len oznámenia používateľa, v ktorom beží, a dopyt na balíky vidí len balíky tohto používateľa **ODVODENÉ**. Nechajte v profile iba navigačné a mediálne aplikácie a auto neuvidí nič z hlavného profilu. Cena: aplikácia na správy, ktorú chcete v aute, musí byť v tom istom profile.

2. Zúžte, čo môže listener oznámení čítať

Listener robí z auta čitateľa najcitlivejšieho prúdu v telefóne, vrátane jednorazových kódov a bankových upozornení. Android ho vie zúžiť aj bez patchu: obrazovka *Notification access settings* v Android Auto má štyri políčka kategórií a zoznam aplikácií. **ZISTENÉ** (na zariadení) Nechajte v zozname len niekoľko aplikácií, ktoré chcete na displeji. Na bankové a autentifikačné aplikácie sa nespoliehajte len na toto: najbezpečnejšie nastavenie je profil, ktorý Android Auto nevidí (bod 1). **ODVODENÉ**

3. Zastavte posielanie oznámení Googlu

Prepínač *Notifications with Assistant* dovoľuje Android Auto posilať vaše oznámenia Googlu pre funkcie ako čítanie správ nahlas. Vypnite ho, pokiaľ túto funkciu nepoužívate. **ZISTENÉ** (na zariadení, znenie citované vyššie)

4. SMS a kontakty udeľte len, ak v aute píšete správy

Odomykajú dialer a rozhranie správ. Bez nich Android Auto stále navigujú, hrajú médiá a prijímajú hlasové príkazy. Funkcia Contact Scopes v GrapheneOS vytvorí dojem, že aplikácia má oprávnenie Contacts, a pritom nevráti nič a zápis blokuje **ZISTENÉ** (príručka). Volanie menom z auta nebude fungovať. **ODVODENÉ**

5. Zabudnite autá, ktoré už nepoužívate, a nové predvolene neprijímajte

Tabuľka `allowedcars` uchováva ID vozidla, adresu Bluetooth, údaje o Wi-Fi a sériové číslo certifikátu. Pred predajom telefónu alebo vrátením požičaného auta odstráňte auto v zozname vozidiel. Odpojenie kábla záznam neodstráni. **ZISTENÉ** Vypnite *Add new vehicles to Android Auto*, keď nenastavujete auto, aby neznáma hlavná jednotka nemohla spustiť nastavenie. **ODVODENÉ**

6. Uprednostnite káblové pripojenie a vypnite balík pre wireless

Káblové pripojenie neukladá prihlasovacie údaje hotspotu. Manifest deklaruje `ACCESS_LOCAL_NETWORK`, `NEARBY_WIFI_DEVICES`, `CHANGE_WIFI_STATE` a skenovanie a pripojenie Bluetooth pre bezdrôtovú cestu. **ZISTENÉ** V GrapheneOS sa tieto oprávnenia pre Android Auto udeľujú ako systémovo pevné a objavujú sa ako balíky vo štyroch prepínačoch vyššie, nie ako jednotlivé výzvy. **ZISTENÉ** (na zariadení) Ak balík pre wireless vypnete, bezdrôtové premietanie pravdepodobne prestane fungovať. **ODVODENÉ**

7. Vypínač siete funguje na Play services, nie na Android Auto

Vlastné oprávnenie Network má Android Auto zamknuté na zapnuté. Vypnutie siete pre Play services zastaví Assistant, prevádzku Maps a telemetriu, ktoré cez ne idú, a pokazí aj navigáciu, ktorá potrebuje živé dáta. Berte to ako politiku pre zariadenie, nie ako všeobecný vypínač súkromia. **ZISTENÉ** (zamknuté oprávnenie) · **ODVODENÉ** (účinnok)

8. Odmietnite špeciálny prístup, ktorý Android Auto žiada, ale nepotrebuje

Manifest deklaruje `SYSTEM_ALERT_WINDOW`, `WRITE_SETTINGS` a `MANAGE_EXTERNAL_STORAGE`. Premietanie funguje aj bez nich, takže ak vás o ne žiada stránka podpory, spochybnite to. **ZISTENÉ** (deklarácie) · **ODVODENÉ** (nie sú potrebné)

Kábel stále odhaľuje obrazovku. Kábel nesie rovnakú vykreslenú obrazovku ako bezdrôtové spojenie. Zmena prenosu mení, ktoré prihlasovacie údaje sa ukladajú. Rovnaká obrazovka sa dostane do auta oboma spôsobmi.

10

Nad rámec nastavení: blokovanie a patchovanie

Nastavenia končia tam, kde Google zvolil sprístupniť ovládanie. Táto sekcia ide ďalej: filtrovanie siete, vypínanie komponentov, úprava APK a patchovanie GrapheneOS. Sú to inžinierske návrhy postavené na inventároch hostiteľov a komponentov v tomto reporte. **Žiadny z nich nebol vyskúšaný na zariadení.** Android Auto je malá aplikácia, ktorá sa pri telemetrii opiera o Play services, preto sekcia odkazuje aj na zodpovedajúce kroky v reporte o Play services.

10.1 Filtrovať sieť zvonka

Bez patchu, plne vratné, APK zostáva podpísané Googlom. Použite Private DNS s filtrujúcim resolverom alebo firewall VPN nainštalovaný len v profile, v ktorom je Android Auto (VPN v Androide sú per používateľ **ODVODENÉ**). Filter DNS alebo SNI vidí názvy hostiteľov, nikdy cesty.

HOSTITEĽ	ÚLOHA	BLOKOVAŤ?	DÔSLEDOK
pagead2.googlesyndication.com	maják reklamného SDK ZISTENÉ	ÁNO	Nič viditeľné. Android Auto nemá reklamnú plochu.
www.google-analytics.com, ssl.google-analytics.com	klasická analytika ZISTENÉ	ÁNO	Nič viditeľné.
autopush-navigationsdkusage.sandbox.googleapis.com	používanie Navigation SDK ZISTENÉ	ÁNO	Je to koncový bod staging prostredia. Nič viditeľné.
feedback-pa.googleapis.com	spätná väzba a hlásenia chýb	ÁNO	Spätná väzba sa neodošle.
clients4.google.com	sieťová poloha (glm/mmap) ZISTENÉ	VOLITEĽNÉ	GrapheneOS predvolene presmeruje žiadosti Play o polohu na vlastnú službu (používateľská príručka), takže ju Android Auto nemusí potrebovať. NETESTOVANÉ
mobilemaps-pa.googleapis.com, mapsmobilesds-pa.googleapis.com	telemetria Maps a používanie SDK	RISKANTNÉ	Môžu to byť tí istí hostitelia, ktorých používa navigácia. Pred spoliehaním sa otestujte.
assistant-maps.google.com	Asistent pre mapy	AK BEZ HLASU	Hlasové príkazy zlyhávajú.
www.googleapis.com	zdieľaný hostiteľ API	NIE	Používajú ho priložené knižnice aj Play services.

Nešifrované spojenie je povolené, použitie sa nenašlo. Konfigurácia zabezpečenia siete nastavuje `cleartextTrafficPermitted="true"` pre každú doménu, no žiadna z 63 URL nájdených v APK nezačína `http://`. Schopnosť tam teda je a jej použitie sa nenašlo. ZISTENÉ Telemetria, na ktorej záleží, ide cez Play services, takže filter zo sekcie 10.1 reportu o Play services platí aj pre ňu.

10.2 Vypínať komponenty cez adb, bez patchu

Pri zapnutom ladení USB môže shell vypínať jednotlivé komponenty pre každého používateľa, napríklad `adb shell pm disable --user <id> com.google.android.projection.gearhead/<component>`. NETESTOVANÉ

KOMPONENT (VŠETKY ZISTENÉ V MANIFESTE)	ČO ZASTAVÍ	PRAVDEPODOBNÁ CENA
gearhead.telemetry.InstallReferrerReceiver	atribúcia inštalácie	Žiadna
gearhead.feedback.CrashReporterReceiver\$CollectFeedbackService, components.feedback.*	zber hlásení o pádoch a spätnej väzby	Žiadna
auto.components.ace.AceInsightRendererService	poznatky z osobného kontextu (Android 16)	Táto funkcia
libraries.assistant.auto.aaptransport.callbacks.CarAssistantCallbacksService	spätné volania Asistenta	Hlas v aute

KOMPONENT (VŠETKY ZISTENÉ V MANIFESTE)	ČO ZASTAVÍ	PRAVDEPODOBNÁ CENA
gearhead.notifications. SharedNotificationListenerManager\$ListenerService	premietanie oznámení	Oznámenia na palubnej doske. Odvolanie prístupu k oznámeniam urobí to isté jednoduchšie.

Telemetria. Udalosti Android Auto odchádzajú cez binder Play services, takže komponenty, na ktorých pri nej záleží, sú v Play services (pozri sekciu 10.2 toho reportu). Platí rovnaké varovanie: Play services si môžu svoje komponenty zapnúť späť.

10.3 Upraviť APK

Je to vôbec možné? Technicky áno. Je to bežné podpísané APK a nič v tejto analýze nebráni jeho rozbaleniu, úprave a novému podpísaniu. Inštaláciu som neskúšal a nehladal som kontrolu vlastnej integrity v aplikácii. Praktické prekážky podľa tejto analýzy:

PREKÁŽKA	PREČO NA TOM ZÁLEŽÍ
Cesta inštalácie	Príručka GrapheneOS hovorí, že Android Auto sa nedá inštalovať cez Play Store ani iné zdroje, iba cez GrapheneOS App Store, a že závisí od sandboxed Google Play. ZISTENÉ (používateľská príručka) Znovu podpísané zostavenie už nie je balík App Store a už sa tam neaktualizuje. ODVODENÉ
Zdieľané UID	Manifest deklaruje <code>sharedUserId="com.google.android.projection.gearhead"</code> , takže každý balík tejto rodiny musí byť podpísaný rovnakým kľúčom. ZISTENÉ
Pripnuté certifikáty	Kód Play services, ktorý pripína dvojicu balíka a certifikátu, uvádza Play Store, aplikáciu Google, Fitness a Wear, ale nie <code>com.google.android.projection.gearhead</code> . ZISTENÉ Tým odpadá jedna prekážka, ktorá platí pre samotné Play services. Moduly Play services týkajúce sa áut môžu volajúcich overovať iným spôsobom. NEZNÁME
Vrstva kompatibility	GrapheneOS spúšťa Android Auto cez rozšírenie svojej vrstvy kompatibility Play so zníženými privilégiami. Nekontroloval som, ako táto vrstva Android Auto rozpoznáva. Ak sa riadi podpisovateľom, potrebný je aj patch OS. NETESTOVANÉ
Auto	Telefón pripína certifikát head unitu. Či head unit kontroluje niečo o podpise na strane telefónu, v APK nie je vidieť. Znovu podpísané zostavenie by niektoré autá mohli odmietnuť. NEZNÁME
Zmeny pri obfuskácii	Názvy tried sa menia pri každom zostavení (<code>jt_b</code> , <code>plo</code> , ...), takže smali patch treba pri každom vydaní nájsť znova. Názvy verejných komponentov sú stabilné. ODVODENÉ

Jediný patch, ktorý prežije zmeny verzií, je patch iba manifestu: nastaviť `android:enabled="false"` na komponentoch z 10.2 binárnym editorom manifestu, DEX nechať nedotknutý, zipalign a podpísať base a tri splity vlastným kľúčom. **NETESTOVANÉ** Čokoľvek, čo mení správanie v kóde, napríklad zabalenie uloženého hesla Wi-Fi kľúčom z Keystore, znamená smali patch pre každé vydanie.

Posudzuje server Googlu upravený Android Auto?

Menej než pri Play services. Android Auto sám nevolá žiadnu atestáciu: v dekompilovanom kóde sa nikde neimportuje klient DroidGuard ani Play Integrity (sekcia 05). Jeho kontakty so serverom tvoria prevádzka Maps,

Asistenta a konfigurácie a jeho telemetria ide cez Play services. Znovu podpísaný Android Auto by sa sám nekontroloval. Narazil by na modul áut v Play services, s ktorým komunikuje, a či tento modul prijme neznámeho podpisovateľa, nie je známe. NEZNÁME Riziko atestácie pre telefón ako celok je opísané v reporte o Play services, v sekcii 10.3.

10.4 Patchnúť GrapheneOS

Na úrovni OS podpis zostáva nedotknutý a zmena prežije aktualizácie. Museli by ste zostaviť a podpísať vlastný GrapheneOS, čo znamená vlastný kľúč verified boot a žiadne oficiálne aktualizácie cez vzduch. Nekontroloval som, ktoré z týchto nápadov už existujú upstream. Overte to a pred zostavovaním založte issue.

NÁVRH	KDE	ÚČINOK	NÁROČNOSŤ / RIZIKO
A. Filter oznámení	Notification access settings v Android Auto	Už existuje: štyri políčka kategórií a zoznam podľa aplikácií („Apps shown on device“). Nie je to patch, preto sa presunul do sekcie 09. Jemnejšia verzia, napríklad filtrovanie podľa konverzácie, by patch bola. ZISTENÉ (na zariadení)	Žiadna pre existujúcu obrazovku.
B. Rozsahy balíkov	Filter viditeľnosti balíkov	<code>QUERY_ALL_PACKAGES</code> je deklarované a 16 dekompilovaných súborov sa dopytuje na balíky alebo intenty ZISTENÉ . Brať ho ako nedržané, ako sa navrhuje pre Play services.	Stredná. Zdieľané s návrhom pre Play services.
C. Zoznam povolených domén pre aplikáciu	Sieťový stack, podľa UID	Povoliť hostiteľov Maps a Asistenta, zahodiť analytiku a reklamy. Rovnaký mechanizmus ako pri Play services.	Vysoká. Len názvy hostiteľov.
D. Vymazanie údajov áut	Životný cyklus profilu a zálohy	Vymazať záznamy áut Android Auto, keď sa profil vymaže alebo sa používateľ odhlási, aby prihlasovacie údaje Wi-Fi neprežili profil. ODVODENÉ	Nízka až stredná. Potrebuje hook, nie patch Android Auto.

Moje poradie: C, potom B, potom D. A už existuje. C nepotrebuje súčinnosť Googlu ani zmenu kódu Android Auto.

10.5 Ktorú možnosť vybrať

MOŽNOSŤ	PRÍNOS PRE SÚKROMIE	POŠKODENIE FUNKCIÍ	NÁMAHA	ÚDRŽBA
Nastavenia a vlastný profil (09)	Vysoký pri oznámeniach	Nízke	Minúty	Žiadna
Prepínač siete	Plný, offline	Navigácia, hlas	Sekundy	Žiadna
Filter DNS / VPN (10.1)	Nízky až stredný	Nízke	Hodiny	Údržba zoznamu
Vypnutie cez adb (10.2)	Nízky	Nízke	Hodiny	Po aktualizáciách
APK upravené v manifeste (10.3)	Nízky	Stredné, pri autách neznáme	Dni	Každé vydanie

MOŽNOSŤ	PRÍNOS PRE SÚKROMIE	POŠKODENIE FUNKCIÍ	NÁMAHA	ÚDRŽBA
Patch OS (10.4)	Vysoký	Nízke	Týždne	Každé vydanie OS

Odporúčaný postup. Začnite vyhradeným profilom, filtrom oznámení nastaveným na niekoľko aplikácií, ktoré chcete na displeji, vypnutým prepínačom Assistant a odstraňovaním áut po použití. Filtre a vypínače komponentov pri Android Auto veľa nezískajú, lebo jeho vlastná sieťová stopa je malá. Ak ste ochotní udržiavať fork, zostavte zoznam povolených domén pre aplikáciu (10.4 C). Prebaľovanie Android Auto preskočte: zisk je malý a autá sú nevyskúšaná premenná.

11

Dôkazy

Každé tvrdenie so značkou **ZISTENÉ** sa dá tu dohľadať. Cesty sú také, ako ich pomenúva jadx 1.5.6 pre APK z indexu artefaktov, pokiaľ nie je uvedený manifest alebo reťazce.

Nezverejnené. Dekompilované zdrojáky a APK sú proprietárny softvér Googlu a nešírim ich. Ak chcete tvrdenie overiť, stiahnite si rovnaké APK z repozitára GrapheneOS (hash je v indexe artefaktov), dekompilujte ho sami cez jadx 1.5.6 a otvorte uvedenú cestu.

Krížové kontroly

Základné tvrdenia reportu boli overené priamo v dekompilovanom kóde.

- Schéma `allowedcars` (`sqm.java:24`), vloženie hesla Wi-Fi (`jtb.java:34`), URL sieťovej polohy (`qbf.java:12`), maják reklám (`qtf.java:16`), 82 oprávnení bez `AD_ID` a bez `READ_SMS` a absencia `play.googleapis.com` v reťazcoch. **ZISTENÉ**
- Náhodné ID klienta vozidla sa generuje na `jtb.java:147` a `jtb.java:454`.
- Heslo Wi-Fi sa nielen ukladá: `plo.java:511` ho loguje, ale iba pri nastavenej ladiacej systémovej vlastnosti (`debug.gh.print_wifi_info`) a dvoch príznakoch. Bežné zostavenia na ten riadok nedôjdu. **ZISTENÉ**. **ODVODENÉ** (bežné zostavenia)
- Heslo sa do `setWpa2Passphrase` / `setWpa3Passphrase` (`plo.java:579–593`) dostane tak, ako je uložené. V aplikácii sa nenašiel žiadny kód Keystore ani šifrovaných preferencií. **ZISTENÉ** Súbor na GrapheneOS chráni sandbox aplikácie a šifrovanie zariadenia, takže to je kontext, nie chyba.

Overené navyše: zistenia o manifeste v sekcii 03 (`QUERY_ALL_PACKAGES`, záložný agent, nešifrovaná prevádzka, zdieľané UID, špeciálny prístup, exportované providery) a odpoveď o Play Integrity v sekcii 05. Samotná trieda listenera oznámení je 7-riadková podtrieda `qrk`, ktorej `onNotificationPosted` odovzdá príspevok do `mir.a` (`qrk.java:90–93`); čo sa deje potom, sa nesledovalo. **ZISTENÉ**

Miesta v kóde

DÔKAZ	ČO PREUKAZUJE
AndroidManifest.xml	82 oprávnení (bez AD_ID), exportovaný listener oznámení, most binder GMS pre autá
defpackage/sqm.java:24,125	schéma allowedcars, stĺpec wifipassword
defpackage/jtb.java:34	heslo WiFi zapísané do tabuľky
defpackage/jtb.java:147,454	náhodné ID klienta vozidla (SecureRandom)
defpackage/plo.java:509–511,579–593	heslo Wi-Fi sa loguje iba pri ladiacej vlastnosti; do setterov hesla WPA2/WPA3 sa odovzdáva tak, ako je uložené
defpackage/qrk.java:90–93	základná trieda listenera oznámení, <code>onNotificationPosted</code>
defpackage/qda.java:20, qgw.java:102–104, qxv.java:67	iba názvy DroidGuard, žiadne volanie klienta
.../config/preferences/contentprovider/SharedPreferencesProvider.java	exportovaný provider s kontrolou volajúceho v kóde
res/xml/network_security_config.xml	nešifrovaná prevádzka povolená pre všetky domény
com/google/android/gms/carsetup/CarInfoInternal.java:107	záznam auta vrátane subjektu/sériového čísla SSL, hashované VIN začernené
com/google/android/gms/clearcut/ · PlayLoggerContext.java	priložený klient clearcut; nikde v APK nie je URL na odosielanie
com/google/android/gearhead/telemetry/InstallReferrerReceiver.java	atribúcia inštalácie
defpackage/qbf.java:12	koncový bod sieťovej polohy (glm/mmap)
defpackage/qtf.java:16	maják gen_204 reklamného SDK
com/google/android/gms/car/AnalyticsSessionInfo.java	ID analytiky pre reláciu
com/google/android/projection/gearhead/messaging/SmsMessagingService.java	služba projekcie SMS
strings · CAR_API_* / AUDIO_DIAGNOSTICS_*	rodiny udalostí telemetrie

Index artefaktov

base.apk	35 123 449 bajtov · sha256 115228a7af416c4c... · podpisovateľ 1ca8dcc0...
splity	config.arm64_v8a 8,8 MB · config.xxhdpi · config.en
metadáta	metadata.1.0.0.sjson · versionCode 179664044
dekompilované	výstup jadx 1.5.6 na mojom stroji · 176 MB · 26 427 tried (nezverejnené)
reťazce	148 023 položiek extrahovaných z APK (nezverejnené)
hostitelia	65 hostiteľov, 63 URL extrahovaných z reťazcov (nezverejnené)

Zdroje

ODKAZ	MIESTO
Repozitár aplikácií	https://apps.grapheneos.org/ · metadata.1.0.0.sjson
Artefakt	packages/com.google.android.projection.gearhead/179664044/base.apk
Nástroje	jadx 1.5.6 · apktool · aapt2 · apksigner 36.0.0
Dokumentácia GrapheneOS	https://grapheneos.org/usage · frameworks_base branch 17

Hranice merania

Tento report meria APK a nevynáša verdikt o produkte. Ukazuje, na čo je Android Auto zapojený a čo ukladá. Nevie ukázať, čo zaznamenáva konkrétne auto ani čo Google uchováva. Značky čítajte doslovne: hranica medzi **ZISTENÉ** a **ODVODENÉ** oddeľuje to, čo APK ukazuje, od toho, čo sa z neho usudzuje.

Ako to zopakovať

```
curl -O https://apps.grapheneos.org/metadata.1.0.0.sjson
curl -O https://apps.grapheneos.org/packages/com.google.android.projection.gearhead/179664044/base.apk

apksigner verify --print-certs base.apk          # očakávané 1ca8dcc0bed3cbd8...b65b5295
apktool d -f --no-src -o res base.apk          # manifest + zdroje
jadx -d out --no-res --show-bad-code base.apk   # 26 427 tried

# klasifikácia oprávnení: 82 položiek uses-permission z APK sa spája s
# protectionLevel z GrapheneOS frameworks_base branch 17 (core/res/AndroidManifest.xml)
```

Hashe v tomto reporte boli pred akoukoľvek analýzou overené voči metadátam repozitára podpísaným signifikantne. Ak sa hash z metadát a hash APK líšia, zastavte: nepozeráte sa na artefakt, ktorý tento report opisuje.

Podpora

Ak vám rozbor pomohol a chcete ho podporiť, môžete poslať ľubovoľnú sumu. Vyberte si, čo vám vyhovuje.



Lightning (BOLT 12)

<lno1pg98xatswphhyapq2d93vggz7yjsxr1fqjju2xf4qnvqd9fjk8acdy4cf7e7kep33vsryw8kplcs>

[Zaplatiť v peňaženke](#)



Monero

<89jGcmA65CReki73oLFvxHUzyR45wMqTN8G93ZYRizwVF2XUQgYKbPLGQYgxj2YjX4fxAUPQ7tLr4ATP7fpR4dSeHH3r9iH>

[Zaplatiť v peňaženke](#)



Zcash (unified adresa)

u1defv75w2x9p6u82qu8je0rrz5g98gnhvs0ervckctfrjvsscvcx00e4qgfk63vm0uar587exxhtp3ps7gwd54anwm32a3sg2432htr53nv22d23agngdpdkdt75lzd8pp0e3f6s2c6n52nk9ecmnjwvdxggfcl7ndsh5uq3wqptk60z

Ostatné formy podpory: juraj.bednar.io/podporte-ma/