ANDROID STATIC ANALYSIS REPORT

Maps (10.75.7)

File Name:	Maps.apk
Package Name:	com.google.android.apps.maps
Scan Date:	March 10, 2024, 4:50 a.m.
App Security Score:	47/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
3	60	0	0	1

FILE INFORMATION

File Name: Maps.apk
Size: 71.17MB
MD5: 88ec93bec644fc524be8264d8dede519
SHA1: 93aec314c865f4adce536220fb7ab788a553541f
SHA256: d32cd14cac16bb3ccb6c8a2455a74fd9457ec701657795abb3785e7227b2927d

APP INFORMATION

App Name: Maps
Package Name: com.google.android.apps.maps
Main Activity: com.google.android.maps.MapsActivity
Target SDK: 31
Min SDK: 23
Max SDK:
Android Version Name: 10.75.7
Android Version Code: 1065973339

APP COMPONENTS

Activities: 31

Services: 40

Receivers: 59

Providers: 5

Exported Activities: 21

Exported Services: 11

Exported Receivers: 24

Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2008-08-21 23:13:34+00:00
Valid To: 2036-01-07 23:13:34+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xc2e08746644a308d
Hash Algorithm: md5
md5: cde9f6208d672b54b1dacc0b7029f5eb
sha1: 38918a453d07199354f8b19af05ec6562ced5788
sha256: f0fd6c5b410f25cb25c3b53346c8972fae30f8ee7411df910480ad6b2d60db83
sha512: edf99db872937471eb94cbe576512a0089527e28b5b65df96f18f539737955ef1ce2553a51156ee31b521dcdc1559c52e965899f13038487d03743742b634326
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 843817f137559b510590075c0256a414a5767c6f32f91a46228077c065ba67fe
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
com.android.launcher.permission.INSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
android.permission.READ_SYNC_SETTINGS	normal	read sync settings	Allows an application to read the sync settings, such as whether sync is enabled for Contacts.
android.permission.WRITE_SYNC_SETTINGS	normal	write sync settings	Allows an application to modify the sync settings, such as whether sync is enabled for Contacts.
android.permission.DISABLE_KEYGUARD	normal	disable keyguard	Allows applications to disable the keyguard if it is not secure.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.CAR_SPEED	unknown	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.google.android.apps.maps.permission.PREFETCH	unknown	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.
android.permission.GET_PACKAGE_SIZE	normal	measure application storage space	Allows an application to find out the space used by any package.
com.google.android.googlequicksearchbox.permission.LENSVIEW_BROADCAST	unknown	Unknown permission	Unknown permission from android reference
com.google.android.googlequicksearchbox.permission.LAUNCH_FROM_GMM	unknown	Unknown permission	Unknown permission from android reference
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.ACCESS_MEDIA_LOCATION	dangerous	access any geographic locations	Allows an application to access any geographic locations persisted in the user's shared collection.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>/home/mobsf/.MobSF/uploads/88ec93bec644fc524be8264d8dede519/88ec93bec644fc524be8264d8dede519.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Obfuscator</td><td>DexGuard</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.HARDWARE check
Build.BOARD check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table></td></tr>
<tr><td>classes3.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
<tr><td>classes4.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes5.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.HARDWARE check
possible Build.SERIAL check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table></td></tr>
<tr><td>classes6.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
<tr><td>classes7.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table></td></tr>
</table>

FILE	DETAILS

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
	Schemes: geo.replay://, google.navigation://, geo://, google.maps://, http://, https://, google.streetview://, google.maps.timeline://, Hosts: business.google.com, ditu.google.com, local.google.com, maps.google.ad, maps.google.ae, maps.google.as, maps.google.at, maps.google.ba, maps.google.be, maps.google.bf, maps.google.bg, maps.google.bi, maps.google.bj, maps.google.bs, maps.google.bt, maps.google.by, maps.google.ca, maps.google.cat, maps.google.cd, maps.google.cf, maps.google.cg, maps.google.ch, maps.google.ci, maps.google.cl, maps.google.cm, maps.google.co.ao, maps.google.co.bw, maps.google.co.ck, maps.google.co.cr, maps.google.co.id, maps.google.co.il, maps.google.co.in, maps.google.co.jp, maps.google.co.ke, maps.google.co.kr, maps.google.co.ls, maps.google.co.mz, maps.google.co.nz, maps.google.co.th, maps.google.co.tz, maps.google.co.ug, maps.google.co.uk, maps.google.co.ve, maps.google.co.vi, maps.google.co.za, maps.google.co.zm, maps.google.co.zw, maps.google.com, maps.google.com.ag, maps.google.com.ai, maps.google.com.ar, maps.google.com.au, maps.google.com.bd, maps.google.com.bh, maps.google.com.bn, maps.google.com.bo, maps.google.com.br, maps.google.com.bz, maps.google.com.co, maps.google.com.cu, maps.google.com.do, maps.google.com.ec, maps.google.com.eg, maps.google.com.et, maps.google.com.fj, maps.google.com.gh, maps.google.com.gi, maps.google.com.gt, maps.google.com.hk, maps.google.com.jm, maps.google.com.kh, maps.google.com.kw, maps.google.com.lb, maps.google.com.ly, maps.google.com.mm, maps.google.com.mt, maps.google.com.mx, maps.google.com.my, maps.google.com.na, maps.google.com.ng, maps.google.com.ni, maps.google.com.np, maps.google.com.om, maps.google.com.pa, maps.google.com.pe, maps.google.com.pg, maps.google.com.ph, maps.google.com.pr, maps.google.com.py, maps.google.com.qa, maps.google.com.sa, maps.google.com.sb, maps.google.com.sg, maps.google.com.sl, maps.google.com.sv, maps.google.com.tr, maps.google.com.tw, maps.google.com.ua,

ACTIVITY	INTENT
com.google.android.maps.MapsActivity	maps.google.com.uy, maps.google.com.vc, maps.google.cv, maps.google.cz, maps.google.de, maps.google.dj, maps.google.dk, maps.google.dm, maps.google.dz, maps.google.ee, maps.google.es, maps.google.fi, maps.google.fm, maps.google.fr, maps.google.ga, maps.google.ge, maps.google.gg, maps.google.gl, maps.google.gm, maps.google.gp, maps.google.gr, maps.google.gy, maps.google.hn, maps.google.hr, maps.google.ht, maps.google.hu, maps.google.ie, maps.google.im, maps.google.iq, maps.google.is, maps.google.it, maps.google.it.ao, maps.google.je, maps.google.jo, maps.google.kg, maps.google.ki, maps.google.kz, maps.google.la, maps.google.li, maps.google.lk, maps.google.lt, maps.google.lu, maps.google.lv, maps.google.mg, maps.google.mk, maps.google.ml, maps.google.mn, maps.google.ms, maps.google.mu, maps.google.mv, maps.google.mw, maps.google.ne, maps.google.ng, maps.google.nl, maps.google.no, maps.google.nr, maps.google.nu, maps.google.pl, maps.google.pn, maps.google.pt, maps.google.ro, maps.google.rs, maps.google.ru, maps.google.rw, maps.google.sc, maps.google.se, maps.google.sh, maps.google.si, maps.google.sk, maps.google.sm, maps.google.sn, maps.google.so, maps.google.st, maps.google.td, maps.google.tg, maps.google.tk, maps.google.tl, maps.google.tn, maps.google.to, maps.google.tt, maps.google.vg, maps.google.vu, maps.google.ws, mapsengine.google.com, www.google.ad, google.com, www.google.ae, www.google.as, www.google.at, www.google.ba, www.google.be, www.google.bf, www.google.bg, www.google.bi, www.google.bj, www.google.bs, www.google.bt, www.google.by, www.google.ca, www.google.cat, www.google.cd, www.google.cf, www.google.cg, www.google.ch, www.google.ci, www.google.cl, www.google.cm, www.google.cn, www.google.co.ao, www.google.co.bw, www.google.co.ck, www.google.co.cr, www.google.co.id, www.google.co.il, www.google.co.in, www.google.co.jp, www.google.co.ke, www.google.co.kr, www.google.co.ls, www.google.co.ma, www.google.co.mz, www.google.co.nz, www.google.co.th, www.google.co.tz, www.google.co.ug, www.google.co.uk, www.google.co.ve, www.google.co.vi, www.google.co.za, www.google.co.zm, www.google.co.zw, www.google.com, www.google.com.ag, www.google.com.ai, www.google.com.ar, www.google.com.au, www.google.com.bd, www.google.com.bh, www.google.com.bn, www.google.com.bo, www.google.com.br, www.google.com.bz, www.google.com.co, www.google.com.cu, www.google.com.do, www.google.com.ec, www.google.com.eg, www.google.com.et, www.google.com.fj, www.google.com.gh, www.google.com.gi, www.google.com.gt, www.google.com.hk, www.google.com.iq, www.google.com.jm, www.google.com.kh, www.google.com.kw, www.google.com.lb, www.google.com.ly, www.google.com.mm, www.google.com.mt, www.google.com.mx, www.google.com.my, www.google.com.na, www.google.com.ng, www.google.com.ni, www.google.com.np, www.google.com.om, www.google.com.pa, www.google.com.pe, www.google.com.pg, www.google.com.ph, www.google.com.pr, www.google.com.py, www.google.com.qa, www.google.com.sa, www.google.com.sb, www.google.com.sg, www.google.com.sl, www.google.com.sv, www.google.com.tr, www.google.com.tw, www.google.com.ua, www.google.com.uy, www.google.com.vc, www.google.cv, www.google.cz, www.google.de, www.google.dj, www.google.dk, www.google.dm, www.google.dz, www.google.ee, www.google.es, www.google.fi, www.google.fm, www.google.fr, www.google.ga, www.google.ge, www.google.gg, www.google.gl, www.google.gm, www.google.gp, www.google.gr, www.google.gy, www.google.hn, www.google.hr, www.google.ht, www.google.hu, www.google.ie, www.google.im, www.google.iq, www.google.is, www.google.it, www.google.it.ao, www.google.je, www.google.jo, www.google.kg, www.google.ki, www.google.kz, www.google.la, www.google.li, www.google.lk, www.google.lt, www.google.lu, www.google.lv, www.google.mg, www.google.mk, www.google.ml, www.google.mn, www.google.ms, www.google.mu, www.google.mv, www.google.mw, www.google.ne, www.google.ng, www.google.nl, www.google.no, www.google.nr, www.google.nu, www.google.pl, www.google.pn, www.google.pt, www.google.ro, www.google.rs,

ACTIVITY	INTENT
	www.google.ru, www.google.rw, www.google.sc, www.google.se, www.google.sh, www.google.si, www.google.sk, www.google.sm, www.google.sn, www.google.so, www.google.st, www.google.td, www.google.tg, www.google.tk, www.google.tl, www.google.tn, www.google.to, www.google.tt, www.google.vg, www.google.vu, www.google.ws, g.co, goo.gl, plus.codes, search.google.com, Mime Types: application/vnd.google.panorama360+jpg, image/*, video/*, vnd.android.cursor.item/postal-address_v2, Paths: /, /maps, /maps/, /maps/preview, /local/writereview/mobile, Path Prefixes: /message, /messages/l, /conversations/l, /maps_message, /locationhistory, /maps, /maps/me, /localguides/signup, /map/viewer, /map/u/.*/viewer, /maps/timeline, /maps/contrib, /maps/match, /local/guides/signup, /local/ugc/interstitial, /maps/@, /maps/place/, /maps/search/, /maps/dir/, /maps/offline, /maps/placelists/all, /maps/placelists/list/, /maps/preview/@, /maps/preview/place/, /maps/preview/search/, /maps/preview/dir/, /maps/d/viewer, /maps/reserve/v/pickup, /2, /3, /4, /5, /6, /7, /8, /9, /C, /F, /G, /H, /J, /M, /P, /Q, /R, /V, /W, /X, Path Patterns: /messages/l/.*/optout.*, /n/.*/reviews, /n/.*/reviews/.*, /maps/d/u/.*/viewer,
com.spotify.sdk.android.authentication.AuthCallbackActivity	Schemes: @string/com_spotify_sdk_redirect_scheme://, Hosts: @string/com_spotify_sdk_redirect_host,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

TITLE	SEVERITY	DESCRIPTION
Certificate algorithm vulnerable to hash collision	high	Application is signed with MD5. MD5 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: 2 | WARNING: 57 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Activity-Alias (com.google.android.apps.maps.TransitSchematicMapActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Activity-Alias (com.google.android.apps.maps.TransitStationActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Activity-Alias (com.google.android.maps.driveabout.app.NavigationActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity-Alias (com.google.android.apps.maps.TrafficHubActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
9	Activity-Alias (com.google.android.apps.maps.ShowSearchAlongRouteActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Activity-Alias (com.google.android.apps.maps.LocationSharesForPersonalSafetyShortcutActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Activity-Alias (com.google.android.apps.maps.ShowSharedLocationsScreenActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	Activity-Alias (com.google.android.apps.maps.LocationShareShortcutActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
13	Activity-Alias (com.google.android.maps.driveabout.app.DestinationActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
14	Activity-Alias (com.google.android.maps.PlacesActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
15	Broadcast Receiver (com.google.android.apps.gmm.geofence.GeofenceBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
16	Broadcast Receiver (com.google.android.apps.gmm.traffic.notification.service.AreaTrafficNotificationGeofenceReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
17	Broadcast Receiver (com.google.android.apps.gmm.navigation.service.detection.StartDetectionReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
18	Broadcast Receiver (com.google.android.libraries.geo.mapcore.internal.prefetch.background.TilePrefetchBroadcastReceiver) is Protected by a permission. Permission: com.google.android.apps.maps.permission.PREFETCH protectionLevel: signature [android:exported=true]	info	A Broadcast Receiver is found to be exported, but is protected by permission.
19	Service (com.google.android.apps.gmm.wearable.GmmWearableListenerService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
20	Broadcast Receiver (com.google.android.apps.gmm.notification.channels.NotificationChannelBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
21	Broadcast Receiver (com.google.android.apps.gmm.cloudmessage.CloudMessageBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
22	Broadcast Receiver (com.google.android.apps.gmm.cloudmessage.chime.ChimeCloudMessageReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
23	Broadcast Receiver (com.google.android.apps.gmm.notification.log.NotificationBlockStateReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
24	Service (com.google.android.apps.gmm.ugc.phototaken.PhotoTakenObserverService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
25	Service (com.google.android.apps.gmm.place.timeline.service.postvisitbadge.PostVisitBadgeService) is Protected by a permission. Permission: com.google.android.apps.maps.permission.TIMELINE_POST_VISIT_BADGE protectionLevel: signature [android:exported=true]	info	A Service is found to be exported, but is protected by permission.

NO	ISSUE	SEVERITY	DESCRIPTION
26	Broadcast Receiver (com.google.android.apps.gmm.ugc.phototaken.StartPhotoTakenNotifierServiceReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
27	Broadcast Receiver (com.google.android.apps.gmm.parkinglocation.ParkingLocationNotificationReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
28	Broadcast Receiver (com.google.android.apps.gmm.ugc.tasks.nearby.UgcTasksNearbyBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
29	Broadcast Receiver (com.google.android.apps.gmm.reportaproblem.common.service.DismissNotificationBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
30	Activity (com.google.android.apps.gmm.directions.appwidget.CreateDirectionsShortcutActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
31	Activity (com.google.android.apps.gmm.navigation.ui.freenav.shortcut.FreeNavCreateShortcutActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
32	Activity (com.google.android.apps.gmm.traffic.shortcut.TrafficHubCreateShortcutActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
33	Activity (com.google.android.apps.gmm.locationsharing.widget.LocationSharingCreateShortcutActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
34	Activity (com.google.android.apps.gmm.locationsharing.widget.SelectedPersonCreateShortcutActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
35	Service (com.google.android.apps.gmm.car.GmmCarProjectionService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
36	Service (com.google.android.apps.gmm.car.LimitedGmmCarProjectionService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
37	Service (com.google.android.apps.gmm.car.WidescreenWidgetLimitedGmmCarProjectionService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
38	Service (com.google.android.apps.gmm.car.projected.auxiliarymap.GmmCarAuxiliaryProjectionService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
39	Service (com.google.android.apps.gmm.car.androidauto.CarNavigationProviderService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
40	Activity (com.google.android.apps.gmm.car.projected.firstrun.GmmProjectedFirstRunActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
41	Activity-Alias (com.google.android.apps.gmm.car.firstrun.GmmProjectedFirstRunActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
42	Broadcast Receiver (com.google.android.apps.gmm.locationsharing.reporting.RestartDetectionBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
43	Broadcast Receiver (com.google.android.apps.gmm.locationsharing.usr.LocationAvailabilityChecker$LocationProvidersChangedBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
44	Broadcast Receiver (com.google.android.apps.gmm.locationsharing.usr.NetworkAvailabilityChecker$ConnectivityChangedBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
45	Broadcast Receiver (com.google.android.apps.gmm.transit.TransitStationBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
46	Broadcast Receiver (com.google.android.apps.gmm.backup.GmmBackupBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
47	Broadcast Receiver (com.google.android.apps.gmm.plugins.serverrecovery.PhenotypeServerRecoveryHandlerImpl) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.PHENOTYPE_UPDATE_BROADCAST [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
48	Service (com.google.android.apps.gmm.locationsharing.interprocess.impl.LocationSharingReportingService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
49	Broadcast Receiver (com.google.android.apps.gmm.offline.appindex.OfflineAppIndexingReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.APPINDEXING [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
50	Service (com.google.android.apps.gmm.offline.update.OfflineAutoUpdateJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
51	Broadcast Receiver (com.google.android.apps.gmm.offline.update.StartAutoUpdatesCheckingReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
52	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
53	Activity (com.google.android.libraries.abuse.reporting.ReportAbuseActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
54	Broadcast Receiver (com.google.android.libraries.phenotype.client.stable.AccountRemovedBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
55	Broadcast Receiver (com.google.android.libraries.phenotype.client.stable.PhenotypeUpdateBackgroundBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.PHENOTYPE_UPDATE_BROADCAST [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
56	Activity (com.google.android.libraries.social.licenses.LicenseMenuActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
57	Broadcast Receiver (com.google.android.libraries.social.peoplekit.thirdparty.viewcontrollers.ThirdPartyReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
58	Activity (com.google.android.libraries.surveys.internal.view.SurveyActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
59	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
60	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
61	Activity (com.spotify.sdk.android.authentication.AuthCallbackActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libgmm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk', '__read_chk']	False warning Symbols are available.
2	arm64-v8a/libgmm-jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__vsnprintf_chk', '__read_chk']	False warning Symbols are available.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	13/24	android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.GET_ACCOUNTS, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.VIBRATE, android.permission.READ_CONTACTS, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.CAMERA, android.permission.RECORD_AUDIO
Other Common Permissions	11/45	android.permission.ACCESS_BACKGROUND_LOCATION, com.google.android.gms.permission.ACTIVITY_RECOGNITION, android.permission.ACTIVITY_RECOGNITION, com.android.launcher.permission.INSTALL_SHORTCUT, android.permission.CHANGE_NETWORK_STATE, android.permission.CHANGE_WIFI_STATE, com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, android.permission.BROADCAST_STICKY, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
tactile-1035.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://tactile-1035.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
appro@openssl.org geo-releaser-mobile@vwra18.prod	lib/arm64-v8a/libgmm-jni.so
appro@openssl.org geo-releaser-mobile@vwra18.prod	apktool_out/lib/arm64-v8a/libgmm-jni.so

TRACKERS

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"PARKING_SESSION_ACTIVE_INDICATOR" : "ACTIVO"
"REVIEW_THUMBS_UP_ACCESSIBILITY_REVIEW_PLACE_AND_AUTHOR" : "%2$s□□%1$s□□□□□"
"LIST_PRIVATE" : "Privada"
"RAP_PLACE_IS_PRIVATE" : "Privé"
"LIST_PRIVATE" : "□□"
"RAP_ROAD_ATTRIBUTE_SELECTION_PRIVATE_TITLE" : "□□"
"NAVIGATION_SESSION_DISTANCE" : "□□"
"FACTUAL_MODERATION_PRIVATE_QUESTION" : "□□□□□□□□□□□□□□"
"RAP_PLACE_IS_PRIVATE" : "Privata"
"LIST_SHARING_OPTIONS_PRIVATE_CAPTION" : "□□□□□□□□□□□□□□□□"
"PARKING_PAYMENT_ACTIVE_SESSION_TITLE" : "□□□□□□"
"RAP_PLACE_IS_PRIVATE" : "□□"

POSSIBLE SECRETS
"RAP_ROAD_ATTRIBUTE_SELECTION_PRIVATE_TITLE" : "□□□□□□"
"REVIEW_THUMBS_UP_ACCESSIBILITY_REVIEW_AUTHOR" : "□□□□%s□"
"RAP_PLACE_IS_PRIVATE" : "□□□"
"google_crash_reporting_api_key" : "AIzaSyAwL-YrZb2V2cHyiT40jAXVFYDqlqs41gs"
"NAVIGATION_SESSION_DURATION" : "□□□□"
"PARKING_SESSION_END_TIME_PREFIX" : "bis %s"
"LIST_AUTHOR_LINK_A11Y_DESCRIPTION" : "%1$s□□%2$s□□□□"
"RAP_ROAD_ATTRIBUTE_SELECTION_PRIVATE_DESCRIPTION" : "□□□□□□□□□□□□□□□□"
"YOUR_PRIVATE_LIST" : "□□□□□□"
"LIST_AUTHOR_LINK_A11Y_DESCRIPTION_WITHOUT_AUTHOR_NAME" : "□%1%s□□□□"
"PARKING_SESSION_ACTIVE_INDICATOR" : "□□"
"RAP_PLACE_IS_PRIVATE" : "Private"
"firebase_database_url" : "https://tactile-1035.firebaseio.com"
"PARKING_SESSION_ACTIVE_INDICATOR" : "ATTIVO"
"PLACE_STATUS_PRIVATE" : "□□□□□□□□□□"
"NAVIGATION_SESSION_DURATION" : "Durée"

POSSIBLE SECRETS
"LIST_PRIVATE" : "Privat"
"LIST_AUTHOR_LINK_A11Y_DESCRIPTION" : "%1$s□□□□%2$s□□□□□□"
"PARKING_SESSION_ACTIVE_INDICATOR" : "AKTIV"
"RAP_ROAD_ATTRIBUTE_SELECTION_PRIVATE_TITLE" : "Privatweg/-straße"
"NAVIGATION_SESSION_DISTANCE" : "Distanza"
"NAVIGATION_SESSION_DISTANCE" : "Distance"
"NAVIGATION_SESSION_DURATION" : "Duration"
"BY_LIST_AUTHOR" : "□□□%s"
"FACTUAL_MODERATION_PRIVATE_TITLE" : "□□□□"
"YOUR_PRIVATE_LIST" : "□□□□□□"
"LIST_PRIVATE" : "□□□"
"LIST_AUTHOR_LINK_BUTTON_LABEL" : "□□□□□□□□□□"
"NAVIGATION_SESSION_AVERAGE_SPEED" : "□□□□"
"NAVIGATION_SESSION_DISTANCE" : "Distancia"
"FACTUAL_MODERATION_PRIVATE_TITLE" : "□□□□□□"
"PLACE_STATUS_PRIVATE" : "□□□□□□□"

POSSIBLE SECRETS
"NAVIGATION_SESSION_DURATION" : "□□□□"
"NAVIGATION_SESSION_DURATION" : "Durata"
"LIST_AUTHOR_LINK_A11Y_DESCRIPTION_WITHOUT_AUTHOR_NAME" : "□%1%s□□□□□□□"
"FACTUAL_MODERATION_PRIVATE_QUESTION" : "□□□□□□□□□□□□□□□□□"
"RAP_PLACE_IS_PRIVATE" : "Privat"
"PARKING_SESSION_ACTIVE_INDICATOR" : "ACTIF"
"PARKING_SESSION_ACTIVE_INDICATOR" : "ACTIVE"
"google_api_key" : "AIzaSyAwL-YrZb2V2cHyiT40jAXVFYDqlqs41gs"
"LIST_PRIVATE" : "Private"
"LIST_PRIVATE" : "Privato"
"NAVIGATION_SESSION_DISTANCE" : "Entfernung"
"NAVIGATION_SESSION_DURATION" : "Dauer"
"RAP_PLACE_IS_PRIVATE" : "Privado"
"LIST_SHARING_OPTIONS_PRIVATE_CAPTION" : "□□□□□□□□□"
"RAP_ROAD_ATTRIBUTE_SELECTION_PRIVATE_DESCRIPTION" : "□□□□□□□□□□□□□□"
"PARKING_PAYMENT_ACTIVE_SESSION_TITLE" : "□□□□"

POSSIBLE SECRETS
"NAVIGATION_SESSION_DURATION" : "Duración"
"LIST_AUTHOR_LINK_BUTTON_LABEL" : "□□□□□□"
"PARKING_SESSION_ACTIVE_INDICATOR" : "□□□"

PLAYSTORE INFORMATION

Title: Google Maps

Score: 3.9718392 **Installs:** 10,000,000,000+ **Price:** 0 **Android Version Support:** **Category:** Travel & Local **Play Store URL:** com.google.android.apps.maps

Developer Details: Google LLC, 5700313618786177705, 1600 Amphitheatre Parkway, Mountain View 94043, http://maps.google.com/about/, apps-help@google.com,

Release Date: None **Privacy Policy:** Privacy link

Description:

Navigate your world faster and easier with Google Maps. Over 220 countries and territories mapped and hundreds of millions of businesses and places on the map. Get real-time GPS navigation, traffic, and transit info, and explore local neighborhoods by knowing where to eat, drink and go - no matter what part of the world you're in. Get there faster with real-time updates • Beat traffic with real-time ETAs and traffic conditions • Catch your bus, train, or ride-share with real-time transit info • Save time with automatic rerouting based on live traffic, incidents, and road closures Discover places and explore like a local • Discover local restaurant, events, and activities that matter to you • Know what's trending and new places that are opening in the areas you care about • Decide more confidently with "Your match," a number on how likely you are to like a place • Group planning made easy. Share a shortlist of options and vote in real-time • Create lists of your favorite places and share with friends • Follow must-try places recommended by local experts, Google, and publishers • Review places you've visited. Add photos, missing roads and places. More experiences on Google Maps • Offline maps to search and navigate without an internet connection • Street View and indoor imagery for restaurants, shops, museums and more • Indoor maps to quickly find your way inside big places like airports, malls and stadiums * Some features not available in all countries * Also available for Wear OS. Add a Tile on your Wear OS watch to quickly access home and work. * Navigation isn't intended to be used by oversized or emergency vehicles

Report Generated by - MobSF v3.9.4 Beta

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.