



ANDROID STATIC ANALYSIS REPORT

app_icon

 GpsGoogleMapsKev (1.0)

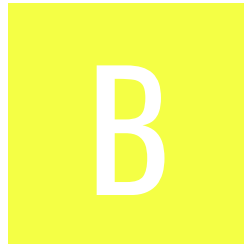
File Name: app-debug.apk

Package Name: com.example.gpsgooglemapskev






Scan Date: Oct. 26, 2025, 2:47 a.m.

App Security Score: 45/100 (MEDIUM RISK)

Grade:



FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
2	3	0	1	1

FILE INFORMATION

File Name: app-debug.apk

Size: 6.71MB

MD5: 8b454c4001d602b2232f2b55450d0e40

SHA1: b93ac462840d778a10bf6522607bdb20a28793c5

SHA256: b567b71245b519c4e6aeaf8cfd706eeca24bbf1f910503881e90371894f3abd

APP INFORMATION

App Name: GpsGoogleMapsKev

Package Name: com.example.gpsgooglemapskev

Main Activity: com.example.gpsgooglemapskev.MainActivity

Target SDK: 36

Min SDK: 26

Max SDK:

Android Version Name: 1.0

Android Version Code: 1

APP COMPONENTS

Activities: 4

Services: 0

Receivers: 1

Providers: 1

Exported Activities: 0

Exported Services: 0

Exported Receivers: 1

Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed

v1 signature: False

v2 signature: True

v3 signature: False

v4 signature: False

X.509 Subject: CN=Android Debug, O=Android, C=US

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2025-09-30 01:30:50+00:00

Valid To: 2055-09-23 01:30:50+00:00

Issuer: CN=Android Debug, O=Android, C=US

Serial Number: 0x1

Hash Algorithm: sha256

md5: 7d5008822fae63db70c9ba8e89bfa96c

sha1: 206d8b57109f3adc837d1c7ffdccf7a3639651a0

sha256: 2b03a733e83ee7ab0963fe89d6c543795b72a906b645bdea697bedf97f255c4f

sha512: 1a13a6e0a29c2eb4569c984877cd55b548feea62af450633808e9041e54faa614cbdf305560892c89ddab9261972cfccbe862a2f1ac9132b817687c18c367a12

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 77cd39517dedc6f1163afaf930945be5e0aa2d71758e1743fc0f6b0742a45340

Found 1 unique certificates

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.example.gpsgooglemapskev.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

FILE	DETAILS	
classes3.dex	FINDINGS	DETAILS
	Compiler	r8
classes2.dex	FINDINGS	DETAILS
	Compiler	unknown (please file detection issue!)
classes4.dex	FINDINGS	DETAILS
	Compiler	r8 without marker (suspicious)
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check
	Compiler	r8

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 3 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.

NO	ISSUE	SEVERITY	DESCRIPTION
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.
4	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 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.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
----	-------	----------	-----------	-------

📄 NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

🏗️ BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	com/example/gpsgooglemapskev/HilosSensoresActivity.java
00030	Connect to the remote server through the given URL	network	com/example/gpsgooglemapskev/HilosSensoresActivity.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE
Other Common Permissions	0/44	

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
i.ytimg.com	ok	IP: 142.251.38.86 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"google_maps_key" : "AlzaSyCiSyECVSyexJq5xQDj8vnKncFVXQAb4vE"

SCAN LOGS

Timestamp	Event	Error
-----------	-------	-------

2025-10-26 02:47:39	Generating Hashes	OK
2025-10-26 02:47:39	Extracting APK	OK
2025-10-26 02:47:39	Unzipping	OK
2025-10-26 02:47:40	Parsing APK with androguard	OK
2025-10-26 02:47:40	Extracting APK features using aapt/aapt2	OK
2025-10-26 02:47:41	Getting Hardcoded Certificates/Keystores	OK
2025-10-26 02:47:44	Parsing AndroidManifest.xml	OK
2025-10-26 02:47:44	Extracting Manifest Data	OK
2025-10-26 02:47:44	Manifest Analysis Started	OK
2025-10-26 02:47:44	Performing Static Analysis on: GpsGoogleMapsKev (com.example.gpsgooglemapskev)	OK
2025-10-26 02:47:45	Fetching Details from Play Store: com.example.gpsgooglemapskev	OK

2025-10-26 02:47:45	Checking for Malware Permissions	OK
2025-10-26 02:47:45	Fetching icon path	OK
2025-10-26 02:47:45	Library Binary Analysis Started	OK
2025-10-26 02:47:45	Reading Code Signing Certificate	OK
2025-10-26 02:47:45	Running APKID 3.0.0	OK
2025-10-26 02:47:48	Detecting Trackers	OK
2025-10-26 02:47:51	Decompiling APK to Java with JADX	OK
2025-10-26 02:48:21	Converting DEX to Smali	OK
2025-10-26 02:48:21	Code Analysis Started on - java_source	OK
2025-10-26 02:48:22	Android SBOM Analysis Completed	OK
2025-10-26 02:48:31	Android SAST Completed	OK

2025-10-26 02:48:31	Android API Analysis Started	OK
2025-10-26 02:48:37	Android API Analysis Completed	OK
2025-10-26 02:48:38	Android Permission Mapping Started	OK
2025-10-26 02:48:44	Android Permission Mapping Completed	OK
2025-10-26 02:48:45	Android Behaviour Analysis Started	OK
2025-10-26 02:48:51	Android Behaviour Analysis Completed	OK
2025-10-26 02:48:51	Extracting Emails and URLs from Source Code	OK
2025-10-26 02:48:51	Email and URL Extraction Completed	OK
2025-10-26 02:48:51	Extracting String data from APK	OK
2025-10-26 02:48:52	Extracting String data from Code	OK
2025-10-26 02:48:52	Extracting String values and entropies from Code	OK

2025-10-26 02:48:54	Performing Malware check on extracted domains	OK
2025-10-26 02:48:55	Saving to Database	OK

Report Generated by - MobSF v4.4.3

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.