



ANDROID STATIC ANALYSIS REPORT

app_icon

 GPSMapApp

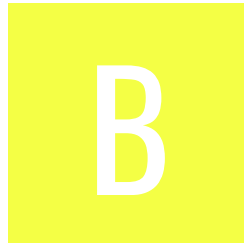
File Name: GPSMapApp-master (1).zip

Package Name: com.example.gpsmapapp






Scan Date: Oct. 27, 2024, 12:43 a.m.

App Security Score: 56/100 (MEDIUM RISK)

Grade:



FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
1	1	0	1	1

FILE INFORMATION

File Name: GPSMapApp-master (1).zip

Size: 0.11MB

MD5: 919dd74fb87cfaeb469073a215266712

SHA1: 71874324ad1d13ed1792c5db99bfa3b8117281da

SHA256: 0577a42381722914757f94c1679bdc84d1d54d02165fc20c380458fe5600f047

APP INFORMATION

App Name: GPSMapApp

Package Name: com.example.gpsmapapp

Main Activity: .MainActivity

Target SDK:

Min SDK:

Max SDK:

Android Version Name:

Android Version Code:

APP COMPONENTS

Activities: 1

Services: 0

Receivers: 0

Providers: 0

Exported Activities: 0

Exported Services: 0

Exported Receivers: 0

Exported Providers: 0

CERTIFICATE INFORMATION

Failed to read Code Signing Certificate or none available.

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.INTERNET	normal	full Internet access	Allows an application to create network sockets.

NETWORK SECURITY

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

CERTIFICATE ANALYSIS

TITLE	SEVERITY	DESCRIPTION
-------	----------	-------------

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	Activity (.MainActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (26) of the app to 29 or higher to fix this issue at platform level.

</> CODE ANALYSIS

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

👤 NIAP ANALYSIS v1.3

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

🔴🔴🔴 ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	3/24	android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.INTERNET
Other Common Permissions	0/45	

Malware Permissions:
Top permissions that are widely abused by known malware.

Other Common Permissions:
Permissions that are commonly abused by known malware.

☰ SCAN LOGS

Timestamp	Event	Error
2024-10-27 00:43:52	Extracting ZIP	OK
2024-10-27 00:43:52	Unzipping	OK
2024-10-27 00:43:52	Detecting source code type	OK
2024-10-27 00:43:52	Source code type - studio	OK
2024-10-27 00:43:52	Generating Hashes	OK
2024-10-27 00:43:52	Getting Hardcoded Certificates/Keystores	OK
2024-10-27 00:43:52	Parsing AndroidManifest.xml	OK
2024-10-27 00:43:52	Extracting Manifest Data	OK
2024-10-27 00:43:52	Fetching Details from Play Store: com.example.gpsmapapp	OK
2024-10-27 00:43:53	Manifest Analysis Started	OK

2024-10-27 00:43:53	Checking for Malware Permissions	OK
2024-10-27 00:43:53	Guessing icon path	OK
2024-10-27 00:43:53	Code Analysis Started on - java	OK
2024-10-27 00:43:53	Android SAST Completed	OK
2024-10-27 00:43:53	Android API Analysis Started	OK
2024-10-27 00:43:54	Android Permission Mapping Started	OK
2024-10-27 00:43:54	Android Permission Mapping Completed	OK
2024-10-27 00:43:54	Finished Code Analysis, Email and URL Extraction	OK
2024-10-27 00:43:54	Extracting String data from Code	OK
2024-10-27 00:43:54	Extracting String values and entropies from Code	OK
2024-10-27 00:43:54	Performing Malware check on extracted domains	OK

2024-10-27 00:43:57	Updating Trackers Database....	OK
2024-10-27 00:43:57	Detecting Trackers from Domains	OK
2024-10-27 00:43:57	Saving to Database	OK

Report Generated by - MobSF v4.0.7

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.