

ANDROID STATIC ANALYSIS REPORT

app_icon

GPSMapApp (1.0)

File Name:	app-debug.apk
Package Name:	com.example.gpsmapapp
Scan Date:	Oct. 25, 2024, 10:10 p.m.
App Security Score:	45/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	◎ HOTSPOT
2	3	0	1	1

FILE INFORMATION

File Name: app-debug.apk

Size: 6.02MB

MD5: 0375a9e8eaf1da1cfad4cfc6af050074

SHA1: 2d56afac53168f6390b461e47b53e932423e6fee

SHA256: 0b8ef854650c596583a715213d5edab83728190bbca038df6cfae89b81531d54

1 APP INFORMATION

App Name: GPSMapApp

Package Name: com.example.gpsmapapp

Main Activity: com.example.gpsmapapp.MainActivity

Target SDK: 34 Min SDK: 26 Max SDK:

Android Version Name: 1.0 **Android Version Code:** 1

B APP COMPONENTS

Activities: 3 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: 2024-09-14 18:37:08+00:00 Valid To: 2054-09-07 18:37:08+00:00

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

Serial Number: 0x1 Hash Algorithm: sha256

md5: 5f17c772472efd9bc9de65dc41d5e191

sha1: 678f341ca1bf6f6936beb0d86d49418c5db6d1f4

sha256: 8fd1c736d2871d15eee391a40b71595ef615e42acaca20f29f17ab692612548b

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 609752b5012a1465f7f83cf70c3b7fb43718b22d5c9a278f963b6f55336c895c

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.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.gpsmapapp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference



FILE	DETAILS			
	FINDINGS DETAILS			
classes3.dex	Compiler	r8 without marker (sus	picious)	
classes4.dex	FINDINGS	DETAILS		
Classes4.uex	Compiler	r8 without marker (suspicious)		
classes2.dex	FINDINGS		DETAILS	
3.355552.4357	Compiler		dx	
	FINDINGS	DETAILS		
classes.dex	Anti-VM Code Build.FINGERPRINT of Build.MODEL check Build.MANUFACTURI			
	Compiler r8 without marker (s		spicious)	



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.

Q 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.
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 (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 ISS	SUE SEVERITY	STANDARDS	FILES
--------	--------------	-----------	-------

■ NIAP ANALYSIS v1.3

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

:::: ABUSED PERMISSIONS

ТҮРЕ	MATCHES	PERMISSIONS
Malware Permissions	4/24	android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE

TYPE	MATCHES	PERMISSIONS
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.



POSSIBLE SECRETS

"google_maps_key" : "AlzaSyDcvrFuHhcAF9DiyDasfcPwM5fa5cfdyb4"

∷ SCAN LOGS

Timestamp	Event	Error
2024-10-25 22:10:33	Generating Hashes	ОК
2024-10-25 22:10:33	Extracting APK	ОК

2024-10-25 22:10:33	Unzipping	ОК
2024-10-25 22:10:33	Getting Hardcoded Certificates/Keystores	ОК
2024-10-25 22:10:35	Parsing AndroidManifest.xml	ОК
2024-10-25 22:10:35	Parsing APK with androguard	ОК
2024-10-25 22:10:35	Extracting Manifest Data	ОК
2024-10-25 22:10:35	Performing Static Analysis on: GPSMapApp (com.example.gpsmapapp)	ОК
2024-10-25 22:10:35	Fetching Details from Play Store: com.example.gpsmapapp	ОК
2024-10-25 22:10:36	Manifest Analysis Started	ОК
2024-10-25 22:10:36	Checking for Malware Permissions	ОК
2024-10-25 22:10:36	Fetching icon path	ОК
2024-10-25 22:10:36	Library Binary Analysis Started	ОК

2024-10-25 22:10:36	Reading Code Signing Certificate	ОК
2024-10-25 22:10:36	Running APKiD 2.1.5	ОК
2024-10-25 22:10:39	Updating Trackers Database	ОК
2024-10-25 22:10:39	Detecting Trackers	ОК
2024-10-25 22:10:40	Decompiling APK to Java with jadx	ОК
2024-10-25 22:10:56	Converting DEX to Smali	ОК
2024-10-25 22:10:56	Code Analysis Started on - java_source	ОК
2024-10-25 22:12:31	Android SAST Completed	ОК
2024-10-25 22:12:31	Android API Analysis Started	ОК
2024-10-25 22:14:01	Android Permission Mapping Started	ОК

2024-10-25 22:14:09	Android Permission Mapping Completed	OK
2024-10-25 22:14:09	Finished Code Analysis, Email and URL Extraction	OK
2024-10-25 22:14:09	Extracting String data from APK	OK
2024-10-25 22:14:09	Extracting String data from Code	ОК
2024-10-25 22:14:09	Extracting String values and entropies from Code	OK
2024-10-25 22:14:10	Performing Malware check on extracted domains	OK
2024-10-25 22:14:10	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.

© 2024 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.