ANDROID STATIC ANALYSIS REPORT

app_icon

🤖 GPSMapApp (1.0)

File Name:	app-debug.apk
Package Name:	com.example.gpsmapapp
Scan Date:	Oct. 22, 2024, 2:17 a.m.

App Security Score:	**44/100 (MEDIUM RISK)**

Grade:	B

FINDINGS SEVERITY

🐛 HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	🔍 HOTSPOT
2	2	0	1	1

FILE INFORMATION

File Name: app-debug.apk
Size: 12.58MB
MD5: a4fb66b4e5115c1b7c77316d7fb70ede
SHA1: 0026ff50b1d06ae1507efd5aaaf35fcb52e58deb
SHA256: 2798210f567729c83c6c9211dd56d34bd1c563ae6c986af07ed95d7a09cb3061

ℹ APP INFORMATION

App Name: GPSMapApp
Package Name: com.example.gpsmapapp
Main Activity: com.example.gpsmapapp.MainActivity
Target SDK: 34
Min SDK: 29
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

▣ APP COMPONENTS

Activities: 2
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: 2024-09-08 23:54:39+00:00
Valid To: 2054-09-01 23:54:39+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha256
md5: e55f3167c31b7cf61d71674074c9ef0a
sha1: abdd3fdf123cdf30ac7b88eeeef89480f3a756b1
sha256: e0dc3a73a513d8abc1b3ebc2126cd91c9d2561a96f498b0528fac298f6e5008a
sha512: bce176063dae0d32e7734e4ce08066fbef5df83c383c93dd18316e46e89d883db441a22c01a29a0b47cc6189e90651d7c83257cdc0c769b4de54644cb34547af
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 73e29ea78d358943519262cf13596b5dcd928e9d19becc15800a159c0b8a7591
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
com.example.gpsmapapp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

⊗ APKID ANALYSIS

FILE	DETAILS		
classes3.dex	**FINDINGS**	**DETAILS**	
	yara_issue	yara issue - dex file recognized by apkid but not yara module	
	Compiler	unknown (please file detection issue!)	
classes2.dex	**FINDINGS**	**DETAILS**	
	yara_issue	yara issue - dex file recognized by apkid but not yara module	
	Compiler	unknown (please file detection issue!)	
classes4.dex	**FINDINGS**	**DETAILS**	
	yara_issue	yara issue - dex file recognized by apkid but not yara module	
	Compiler	unknown (please file detection issue!)	

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

🔒 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

TITLE	SEVERITY	DESCRIPTION
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: **2** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	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.
3	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

⠿⠿ ABUSED PERMISSIONS

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

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"google_maps_key" : "AIzaSyBamdgouYEd_-QTO6BEn1EUynjDUwqxwTs"

SCAN LOGS

Timestamp	Event	Error
2024-10-22 02:16:02	Generating Hashes	OK
2024-10-22 02:16:03	Android Permission Mapping Started	OK
2024-10-22 02:16:03	Extracting APK	OK
2024-10-22 02:16:03	Unzipping	OK
2024-10-22 02:16:04	Getting Hardcoded Certificates/Keystores	OK
2024-10-22 02:16:04	Parsing AndroidManifest.xml	OK
2024-10-22 02:16:04	Parsing APK with androguard	OK
2024-10-22 02:16:08	Extracting Manifest Data	OK
2024-10-22 02:16:08	Performing Static Analysis on: GPSMapApp (com.example.gpsmapapp)	OK

2024-10-22 02:16:08	Fetching Details from Play Store: com.example.gpsmapapp	OK
2024-10-22 02:16:08	Manifest Analysis Started	OK
2024-10-22 02:16:08	Checking for Malware Permissions	OK
2024-10-22 02:16:08	Fetching icon path	OK
2024-10-22 02:16:08	Library Binary Analysis Started	OK
2024-10-22 02:16:09	Reading Code Signing Certificate	OK
2024-10-22 02:16:11	Running APKiD 2.1.5	OK
2024-10-22 02:16:17	Detecting Trackers	OK
2024-10-22 02:16:33	Decompiling APK to Java with jadx	OK
2024-10-22 02:16:56	Android Permission Mapping Completed	OK
2024-10-22 02:16:56	Finished Code Analysis, Email and URL Extraction	OK

2024-10-22 02:16:56	Extracting String data from APK	OK
2024-10-22 02:16:57	Extracting String data from Code	OK
2024-10-22 02:16:57	Extracting String values and entropies from Code	OK
2024-10-22 02:16:57	Converting DEX to Smali	OK
2024-10-22 02:16:57	Code Analysis Started on - java_source	OK
2024-10-22 02:16:58	Performing Malware check on extracted domains	OK
2024-10-22 02:16:58	Saving to Database	OK
2024-10-22 02:17:02	Android SAST Completed	OK
2024-10-22 02:17:02	Android API Analysis Started	OK
2024-10-22 02:17:13	Android Permission Mapping Started	OK
2024-10-22 02:17:15	Android Permission Mapping Started	OK

2024-10-22 02:17:22	Android Permission Mapping Completed	OK
2024-10-22 02:17:22	Finished Code Analysis, Email and URL Extraction	OK
2024-10-22 02:17:22	Extracting String data from APK	OK
2024-10-22 02:17:23	Extracting String data from Code	OK
2024-10-22 02:17:23	Extracting String values and entropies from Code	OK
2024-10-22 02:17:24	Performing Malware check on extracted domains	OK
2024-10-22 02:17:24	Updating Database...	OK
2024-10-22 02:17:46	Android Permission Mapping Completed	OK
2024-10-22 02:17:47	Finished Code Analysis, Email and URL Extraction	OK
2024-10-22 02:17:47	Extracting String data from APK	OK
2024-10-22 02:17:53	Extracting String data from Code	OK

2024-10-22 02:17:53	Extracting String values and entropies from Code	OK
2024-10-22 02:17:58	Performing Malware check on extracted domains	OK
2024-10-22 02:17:58	Saving to Database	OK
2024-10-22 02:18:17	Android SAST Completed	OK
2024-10-22 02:18:17	Android API Analysis Started	OK
2024-10-22 02:18:29	Android Permission Mapping Started	OK
2024-10-22 02:19:05	Converting DEX to Smali	OK
2024-10-22 02:19:05	Code Analysis Started on - java_source	OK
2024-10-22 02:19:14	Android SAST Completed	OK
2024-10-22 02:19:14	Android API Analysis Started	OK
2024-10-22 02:19:30	Android Permission Mapping Completed	OK

2024-10-22 02:19:31	Finished Code Analysis, Email and URL Extraction	OK
2024-10-22 02:19:31	Extracting String data from APK	OK
2024-10-22 02:19:32	Extracting String data from Code	OK
2024-10-22 02:19:32	Extracting String values and entropies from Code	OK
2024-10-22 02:19:37	Performing Malware check on extracted domains	OK
2024-10-22 02:19:37	Saving to Database	OK
2024-10-22 02:20:02	Android SAST Completed	OK
2024-10-22 02:20:02	Android API Analysis Started	OK
2024-10-22 02:21:16	Android SAST Completed	OK
2024-10-22 02:21:16	Android API Analysis Started	OK
2024-10-22 02:23:11	Android SAST Completed	OK

2024-10-22 02:23:11	Android API Analysis Started	OK
2024-10-22 02:23:19	Android Permission Mapping Started	OK
2024-10-22 02:23:55	Android Permission Mapping Completed	OK
2024-10-22 02:23:55	Finished Code Analysis, Email and URL Extraction	OK
2024-10-22 02:23:55	Extracting String data from APK	OK
2024-10-22 02:23:55	Extracting String data from Code	OK
2024-10-22 02:23:55	Extracting String values and entropies from Code	OK
2024-10-22 02:23:58	Performing Malware check on extracted domains	OK
2024-10-22 02:23:58	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.