MOBSF

ANDROID STATIC ANALYSIS REPORT

GPSMapApp (1.0)

File Name:	app-debug.apk
Package Name:	com.example.gpsmapapp
Scan Date:	Oct. 22, 2025, 6:54 p.m.
App Security Score:	48/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	3	0	2	1

FILE INFORMATION

File Name: app-debug.apk
Size: 4.03MB
MD5: c70da776c5dd709ce34248593e00adef
SHA1: 2247695871d2a6435782af9711f47d9681161b15
SHA256: 35dafa7a59794d4c4a1d7bd091b45b1e5ad286642ef988b5c28fec24be60ee4c

APP INFORMATION

App Name: GPSMapApp
Package Name: com.example.gpsmapapp
Main Activity: com.example.gpsmapapp.MapsActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 2
Services: 0
Receivers: 1
Providers: 2
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: 2025-07-14 22:15:13+00:00
Valid To: 2055-07-07 22:15:13+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha256
md5: cee14d6e1c901c3701c8fb402e9dfb37
sha1: 44f11eb33399dd21a3c451741a76b10f0014e8dd
sha256: 9b66115dfe389bd413925a29274d337e33fada483bf9da70fa712332d1668567
sha512: 695d1421a934cfa72832d349921b85960c2a8ae8709f173013ad0c94080561c79eb4ce6ec3cdddc5f34f8e319899df5d170bdd32f6f2d5269630f1641710955a
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: c4549acc105af134f474a931ba90cf58b13a963f1948f32ad33bc39c3e29bb0e
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.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.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

<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>unknown (please file detection issue!)</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>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

HIGH: **0** | WARNING: **0** | INFO: **0** | SECURE: **1**

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	secure	Base config is configured to disallow clear text traffic to all domains.

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: 2 | WARNING: 2 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	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.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	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
4	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.
5	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

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/example/gpsmapapp/MapsActivity.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/example/gpsmapapp/MapsActivity.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/example/gpsmapapp/MapsActivity.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/25	android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.CAMERA, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET
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.

HARDCODED SECRETS

POSSIBLE SECRETS
"google_maps_key" : "REEMPLAZA_AQUI_TU_API_KEY"

SCAN LOGS

Timestamp	Event	Error
2025-10-22 18:54:17	Generating Hashes	OK
2025-10-22 18:54:17	Extracting APK	OK
2025-10-22 18:54:17	Unzipping	OK
2025-10-22 18:54:17	Parsing APK with androguard	OK
2025-10-22 18:54:17	Extracting APK features using aapt/aapt2	OK
2025-10-22 18:54:17	Getting Hardcoded Certificates/Keystores	OK
2025-10-22 18:54:19	Parsing AndroidManifest.xml	OK

2025-10-22 18:54:19	Extracting Manifest Data	OK
2025-10-22 18:54:19	Manifest Analysis Started	OK
2025-10-22 18:54:19	Reading Network Security config from network_security_config.xml	OK
2025-10-22 18:54:19	Parsing Network Security config	OK
2025-10-22 18:54:19	Performing Static Analysis on: GPSMapApp (com.example.gpsmapapp)	OK
2025-10-22 18:54:20	Fetching Details from Play Store: com.example.gpsmapapp	OK
2025-10-22 18:54:20	Checking for Malware Permissions	OK
2025-10-22 18:54:20	Fetching icon path	OK
2025-10-22 18:54:20	Library Binary Analysis Started	OK
2025-10-22 18:54:20	Reading Code Signing Certificate	OK

2025-10-22 18:54:20	Running APKiD 3.0.0	OK
2025-10-22 18:54:24	Detecting Trackers	OK
2025-10-22 18:54:25	Decompiling APK to Java with JADX	OK
2025-10-22 18:54:33	Converting DEX to Smali	OK
2025-10-22 18:54:33	Code Analysis Started on - java_source	OK
2025-10-22 18:54:34	Android SBOM Analysis Completed	OK
2025-10-22 18:54:34	Android SAST Completed	OK
2025-10-22 18:54:34	Android API Analysis Started	OK
2025-10-22 18:54:35	Android API Analysis Completed	OK
2025-10-22 18:54:35	Android Permission Mapping Started	OK
2025-10-22 18:54:36	Android Permission Mapping Completed	OK

2025-10-22 18:54:36	Android Behaviour Analysis Started	OK
2025-10-22 18:54:36	Android Behaviour Analysis Completed	OK
2025-10-22 18:54:36	Extracting Emails and URLs from Source Code	OK
2025-10-22 18:54:36	Email and URL Extraction Completed	OK
2025-10-22 18:54:36	Extracting String data from APK	OK
2025-10-22 18:54:36	Extracting String data from Code	OK
2025-10-22 18:54:36	Extracting String values and entropies from Code	OK
2025-10-22 18:54:37	Performing Malware check on extracted domains	OK
2025-10-22 18:54:37	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.