MOBSF

ANDROID STATIC ANALYSIS REPORT

No icon

app-debug-androidTest.apk

File Name:	app-debug-androidTest.apk
Package Name:	com.example.gpsmapapp.test
Scan Date:	Oct. 30, 2024, 1:39 a.m.
App Security Score:	41/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
3	5	1	1	0

FILE INFORMATION

File Name: app-debug-androidTest.apk
Size: 0.53MB
MD5: 24c4f92aff9fd70b25160a2b79ae9a85
SHA1: ff342aeb7f3b6ce91ade18c8fc8f4489ec0400fe
SHA256: d7c2bd223e77019fc8bedc318e1132ba61f072a408dbed18aa6c568d2f039ff0

APP INFORMATION

App Name:
Package Name: com.example.gpsmapapp.test
Main Activity: androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name:
Android Version Code:

APP COMPONENTS

Activities: 3
Services: 0
Receivers: 0
Providers: 0
Exported Activities: 2
Exported Services: 0
Exported Receivers: 0
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: 2024-08-29 04:27:29+00:00
Valid To: 2054-08-22 04:27:29+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha256
md5: 87e9a6aa9a437f6131ab870f05a90a34
sha1: a1271a984db30d8ff94b23c560ecda13e0bb3f52
sha256: db8e3e37b79ec283596bc72323e7521070b669cc94d475bf68bd2038aad499c1
sha512: 3c314d6463fcaa4de0ad0af091a9472a92e590acb303098aec842853374e7c0d6ae956fafe20d87f10faea8b7d6ef8969a514ae762e375167849ab21b0c679a9
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 4807eede4a150166250776537915 1af7f38fb3b8d5942d09ddd80716d53357c8
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.REORDER_TASKS	normal	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.

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>dx</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>unknown (please file detection issue!)</td></tr></table></td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></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.HARDWARE check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</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
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: **3** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched 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	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] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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	Activity (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

CODE ANALYSIS

HIGH: **0** | WARNING: **2** | INFO: **1** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	junit/runner/BaseTestRunner.java junit/runner/Version.java junit/textui/TestRunner.java
2	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	org/junit/runner/manipulation/Ordering.java
3	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	org/junit/rules/TemporaryFolder.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	0/24	
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
2024-10-30 01:39:50	Generating Hashes	OK
2024-10-30 01:39:50	Extracting APK	OK
2024-10-30 01:39:50	Unzipping	OK
2024-10-30 01:39:50	Getting Hardcoded Certificates/Keystores	OK

2024-10-30 01:39:53	Parsing AndroidManifest.xml	OK
2024-10-30 01:39:53	Parsing APK with androguard	OK
2024-10-30 01:39:53	Extracting Manifest Data	OK
2024-10-30 01:39:53	Performing Static Analysis on: com.example.gpsmapapp.test	OK
2024-10-30 01:39:53	Fetching Details from Play Store: com.example.gpsmapapp.test	OK
2024-10-30 01:39:53	Manifest Analysis Started	OK
2024-10-30 01:39:53	Checking for Malware Permissions	OK
2024-10-30 01:39:53	Fetching icon path	OK
2024-10-30 01:39:53	Library Binary Analysis Started	OK
2024-10-30 01:39:53	Reading Code Signing Certificate	OK
2024-10-30 01:39:54	Running APKiD 2.1.5	OK

2024-10-30 01:39:55	Detecting Trackers	OK
2024-10-30 01:39:56	Decompiling APK to Java with jadx	OK
2024-10-30 01:40:06	Converting DEX to Smali	OK
2024-10-30 01:40:06	Code Analysis Started on - java_source	OK
2024-10-30 01:40:08	Android SAST Completed	OK
2024-10-30 01:40:08	Android API Analysis Started	OK
2024-10-30 01:40:10	Android Permission Mapping Started	OK
2024-10-30 01:40:11	Android Permission Mapping Completed	OK
2024-10-30 01:40:11	Finished Code Analysis, Email and URL Extraction	OK
2024-10-30 01:40:11	Extracting String data from APK	OK
2024-10-30 01:40:11	Extracting String data from Code	OK

2024-10-30 01:40:11	Extracting String values and entropies from Code	OK
2024-10-30 01:40:12	Performing Malware check on extracted domains	OK
2024-10-30 01:40:12	Saving to Database	OK

Report Generated by - MobSF v4.1.1

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.