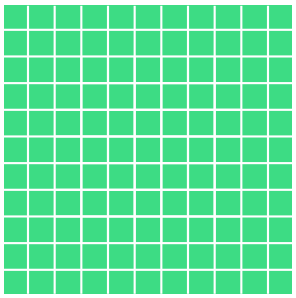
MOBSF

ANDROID STATIC ANALYSIS REPORT



Evaluacion-maps-KS (1.0)

File Name:	app-debug.apk
Package Name:	com.jsh.evaluacion_maps_ks
Scan Date:	Nov. 12, 2024, 9:53 p.m.
App Security Score:	36/100 (HIGH RISK)
Grade:	C

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	2	0	1	1

FILE INFORMATION

File Name: app-debug.apk
Size: 6.16MB
MD5: a40d22ea59db408737d480cfa01b3025
SHA1: a17628ee483051f510f6cbcbe89bf5aaefe6c7ee
SHA256: 5f78147103614e3635c83a371ead7b1c0f6ee0a194f656edc35775c6ae35938c

APP INFORMATION

App Name: Evaluacion-maps-KS
Package Name: com.jsh.evaluacion_maps_ks
Main Activity: com.jsh.evaluacion_maps_ks.MainActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

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: 2024-09-10 21:56:27+00:00
Valid To: 2054-09-03 21:56:27+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha256
md5: e39d6a71f0aafe0387805883efccdb63
sha1: d64d36157480c0e7fc1ab969d7fcc15ccd16b2e2
sha256: e62ef1a124f478d889a5baae65c53ea3a90cdbea5623878536154c3bb92f7c9f
sha512: 3f0b7c29d6e8c6b5767e615a31853090bd6f9f80c462651171fc98b3f05b0932fb952140e7b1cd679b6cae5be58012615a4af66ce9b5bcfc736a054643bf2a96
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: c8b628f4da190497c3d28a049b08dc1fd6858585e2034bca82625e8485e63888
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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_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_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.jsh.evaluacion_maps_ks.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>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>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>classes5.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
Build.BRAND check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes4.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</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: 2 | 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=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.
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	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	4/25	android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, 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.

OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
maps.googleapis.com	ok	**IP:** 216.58.211.234 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

SCAN LOGS

Timestamp	Event	Error
2024-11-12 22:24:51	Generating Hashes	OK
2024-11-12 22:24:51	Extracting APK	OK
2024-11-12 22:24:51	Unzipping	OK
2024-11-12 22:24:57	Getting Hardcoded Certificates/Keystores	OK
2024-11-12 22:24:57	Parsing APK with androguard	OK

2024-11-12 22:25:14	Parsing AndroidManifest.xml	OK
2024-11-12 22:25:14	Extracting Manifest Data	OK
2024-11-12 22:25:14	Performing Static Analysis on: Evaluacion-maps-KS (com.jsh.evaluacion_maps_ks)	OK
2024-11-12 22:25:14	Fetching Details from Play Store: com.jsh.evaluacion_maps_ks	OK
2024-11-12 22:25:15	Manifest Analysis Started	OK
2024-11-12 22:25:15	Checking for Malware Permissions	OK
2024-11-12 22:25:15	Fetching icon path	OK
2024-11-12 22:25:23	Library Binary Analysis Started	OK
2024-11-12 22:25:29	Reading Code Signing Certificate	OK
2024-11-12 22:25:34	Running APKiD 2.1.5	OK
2024-11-12 22:26:00	Detecting Trackers	OK

2024-11-12 22:26:47	Decompiling APK to Java with JADX	OK

Report Generated by - MobSF v4.1.9

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.