ANDROID STATIC ANALYSIS REPORT

app_icon

js (1.0)

File Name:	app-debug.apk
Package Name:	com.mapagps.js
Scan Date:	Oct. 22, 2024, 3:41 p.m.
App Security Score:	38/100 (HIGH RISK)
Grade:	C

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
3	3	0	1	1

FILE INFORMATION

File Name: app-debug.apk
Size: 5.49MB
MD5: 91d96c31a3dcbd6cf1b7f7fe1e1374fe
SHA1: 18dc558020e7fc20150e9b15a6ad12284faec045
SHA256: c723420a87b69b6040c4a5654f32df92e0cc0a2d133633e8ebaea46f05ebb680

APP INFORMATION

App Name: js
Package Name: com.mapagps.js
Main Activity: com.mapagps.js.MainActivity
Target SDK: 34
Min SDK: 21
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

▦ APP COMPONENTS

Activities: 2
Services: 0
Receivers: 0
Providers: 1
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

✹ CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: True
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: 2024-08-12 13:19:39+00:00
Valid To: 2054-08-05 13:19:39+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha1
md5: 1b3d9a9a4bb7e3cca94df2700097e203
sha1: 1c8ca4daf80b5338ca8256d1e8ad23efee0738ff
sha256: f66cd8597ae4161526359810ef18baff92c5c014bafc37aab720ba40417664e3
sha512: 572b107c1dcf8c36da9e44096d4283344c0a3c41129786afb2b7d3c53bdbcf37212049c03d166128efb8302f17cf78e4f843b25c984e2c1913548a0071310eb8
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 8f5ec535f367f5b8d5601d236859f61cfce95e5c7ec0655b7f50b4c2455bc4fc
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.mapagps.js.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<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>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>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **1** | WARNING: **2** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.0-5.0.2, [minSdk=21]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
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.

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

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.

HARDCODED SECRETS

POSSIBLE SECRETS
"google_maps_key" : ""

SCAN LOGS

Timestamp	Event	Error
2024-10-22 15:50:40	Generating Hashes	OK
2024-10-22 15:50:40	Extracting APK	OK

2024-10-22 15:50:41	Unzipping	OK
2024-10-22 15:50:41	Getting Hardcoded Certificates/Keystores	OK
2024-10-22 15:50:41	Parsing AndroidManifest.xml	OK
2024-10-22 15:50:41	Parsing APK with androguard	OK
2024-10-22 15:50:44	Extracting Manifest Data	OK
2024-10-22 15:50:44	Performing Static Analysis on: js (com.mapagps.js)	OK
2024-10-22 15:50:44	Fetching Details from Play Store: com.mapagps.js	OK
2024-10-22 15:50:44	Manifest Analysis Started	OK
2024-10-22 15:50:44	Checking for Malware Permissions	OK
2024-10-22 15:50:44	Fetching icon path	OK
2024-10-22 15:50:44	Library Binary Analysis Started	OK

2024-10-22 15:50:45	Reading Code Signing Certificate	OK
2024-10-22 15:50:48	Running APKiD 2.1.5	OK
2024-10-22 15:50:53	Detecting Trackers	OK
2024-10-22 15:51:01	Decompiling APK to Java with jadx	OK
2024-10-22 15:53:14	Converting DEX to Smali	OK
2024-10-22 15:53:14	Code Analysis Started on - java_source	OK
2024-10-22 15:53:26	Android SAST Completed	OK
2024-10-22 15:53:26	Android API Analysis Started	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.