ANDROID STATIC ANALYSIS REPORT

app_icon

Mapa (1.0)

File Name:	app-debug.apk
Package Name:	com.evi.mapa
Scan Date:	Oct. 21, 2024, 9:45 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: f02395344d7fa987b2d777848d8fb489
SHA1: ba0b669bc041a8640a91cca85b26869816035a66
SHA256: 46c5b7ed7948f1a5c2d42d0654c834e621cafa50348912d74c18029690621f06

APP INFORMATION

App Name: Mapa
Package Name: com.evi.mapa
Main Activity: com.evi.mapa.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: 2024-08-19 13:16:23+00:00
Valid To: 2054-08-12 13:16:23+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha256
md5: 184297a8b22a8931a8148f82645fc8ce
sha1: 93541ec6da08d763312b8f08f7a280a0bc19e181
sha256: b8b0cc96dc49c47eed479bad12e7a8af53301f2ca9cd6804cd46cd5d6df808e9
sha512: 64403fccc4bd0d0ae7bbeca8730e93f0900c07cb40b93dc9ceaeb23d110407bfea8bd2b46dfce3470805642e72279362ae4c316297db5b8ceee0e5a2ac399993
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 5f764d1f4db544b235c5d75be2feb9bb5f5e03e992474de0943076ffcad6c46c
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.evi.mapa.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>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>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>classes4.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>
</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.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: **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	4/24	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.

SCAN LOGS

Timestamp	Event	Error
2024-10-21 21:51:56	Generating Hashes	OK

2024-10-21 21:51:56	Extracting APK	OK
2024-10-21 21:51:56	Unzipping	OK
2024-10-21 21:51:57	Getting Hardcoded Certificates/Keystores	OK
2024-10-21 21:51:57	Parsing AndroidManifest.xml	OK
2024-10-21 21:51:57	Parsing APK with androguard	OK
2024-10-21 21:51:58	Extracting Manifest Data	OK
2024-10-21 21:51:58	Performing Static Analysis on: Mapa (com.evi.mapa)	OK
2024-10-21 21:51:58	Fetching Details from Play Store: com.evi.mapa	OK
2024-10-21 21:51:58	Manifest Analysis Started	OK
2024-10-21 21:51:58	Checking for Malware Permissions	OK

2024-10-21 21:51:58	Fetching icon path	OK
2024-10-21 21:51:58	Library Binary Analysis Started	OK
2024-10-21 21:51:58	Reading Code Signing Certificate	OK
2024-10-21 21:52:00	Running APKiD 2.1.5	OK
2024-10-21 21:52:03	Detecting Trackers	OK
2024-10-21 21:52:05	Converting DEX to Smali	OK
2024-10-21 21:52:06	Code Analysis Started on - java_source	OK
2024-10-21 21:52:12	Decompiling APK to Java with jadx	OK
2024-10-21 21:52:12	libsast scan failed	FileNotFoundError(2, 'No such file or directory')
2024-10-21 21:52:12	Android SAST Completed	OK
2024-10-21 21:52:12	Android API Analysis Started	OK

2024-10-21 21:52:21	Android Permission Mapping Started	OK
2024-10-21 21:52:21	Android Permission Mapping Completed	OK
2024-10-21 21:52:21	Finished Code Analysis, Email and URL Extraction	OK
2024-10-21 21:52:21	Extracting String data from APK	OK
2024-10-21 21:52:24	Extracting String data from Code	OK
2024-10-21 21:52:24	Extracting String values and entropies from Code	OK
2024-10-21 21:52:24	Performing Malware check on extracted domains	OK
2024-10-21 21:52:24	Saving to Database	OK
2024-10-21 21:52:57	Converting DEX to Smali	OK
2024-10-21 21:52:57	Code Analysis Started on - java_source	OK
2024-10-21 21:57:12	Android SAST Completed	OK

2024-10-21 21:57:12	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.