

## ANDROID STATIC ANALYSIS REPORT

app\_icon

EvaluacionMapas-LB (1.0)

File Name:	mapsAPP.apk
Package Name:	com.lucianobl.evaluacionmapas_lb
Scan Date:	Oct. 23, 2024, 10:58 p.m.
App Security Score:	36/100 (HIGH RISK)
Grade:	C

### FINDINGS SEVERITY

<del>派</del> HIGH	▲ MEDIUM	i INFO	✓ SECURE	<b>◎</b> HOTSPOT
3	2	0	1	1

### FILE INFORMATION

File Name: mapsAPP.apk

Size: 6.29MB

MD5: 5c659595cdff24590e222fc3892ccea7

**SHA1:** b2c2e601ab11e28a33fcfbcc06b9a292bd4c54b7

**SHA256**: 57d4bef36602a4f10a0492b4e06d48c7f59e70acbff0c77e8b8ac7406a812db1

# **i** APP INFORMATION

App Name: EvaluacionMapas-LB

**Package Name:** com.lucianobl.evaluacionmapas\_lb

Main Activity: com.lucianobl.evaluacionmapas\_lb.MainActivity

Target SDK: 34 Min SDK: 24 Max SDK:

**Android Version Name:** 1.0 **Android Version Code:** 1

### **B** 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: 2024-09-25 15:34:32+00:00 Valid To: 2054-09-18 15:34:32+00:00

Issuer: CN=Android Debug, O=Android, C=US

Serial Number: 0x1 Hash Algorithm: sha256

md5: 69740e5d26d8f99d125b6e0b43e26e02

sha1: 6a4557f137c66999f723f00e52a5dd516aaf8bd5

sha256: 09913fb9974c35313f3eb1533469e8624896fbf7bc98cb0771dbb359d8c70e24

sha512: efe96624a2d75a4ee4919b2934ec52fbd8ed30184c9291819029c560340d2527eb1c1a80d65b4db7b895e550043ffcc40a695b307f016d069490b9a81852bfb2

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: d2ab8d8a0 fac 549c6433d4 fa 02ddc3 bef8a950508a5ec1b262aaedeffd7d6006abef8a950508abef8a9508abeff8a9508abef8a9508abe

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.lucianobl.evaluacionmapas_lb.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference



FILE	DETAILS		
classes4.dex	FINDINGS DETAILS		
Classes4.dex	Compiler r8 without marker (susp		picious)
	FINDINGS DETAILS		
classes3.dex	Compiler r8 without marker (sus		picious)
classes2.dex	FINDINGS		DETAILS
classes2.dex	Compiler		dx
classes5.dex	FINDINGS DETAILS		
Classessiuck	Compiler r8 without marker (sus		picious)

FILE	DETAILS	
	FINDINGS	DETAILS
classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check
	Compiler	r8 without marker (suspicious)

# **△** 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.

# **Q** 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]		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]		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

ТҮРЕ	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
2024-10-23 23:02:18	Generating Hashes	ОК

2024-10-23 23:02:18	Extracting APK	ОК
2024-10-23 23:02:18	Unzipping	OK
2024-10-23 23:02:19	Getting Hardcoded Certificates/Keystores	ОК
2024-10-23 23:02:19	Parsing AndroidManifest.xml	ОК
2024-10-23 23:02:19	Parsing APK with androguard	ОК
2024-10-23 23:02:20	Extracting Manifest Data	ОК
2024-10-23 23:02:20	Performing Static Analysis on: EvaluacionMapas-LB (com.lucianobl.evaluacionmapas_lb)	ОК
2024-10-23 23:02:20	Fetching Details from Play Store: com.lucianobl.evaluacionmapas_lb	ОК
2024-10-23 23:02:20	Manifest Analysis Started	ОК
2024-10-23 23:02:20	Checking for Malware Permissions	ОК

2024-10-23 23:02:20	Fetching icon path	ОК
2024-10-23 23:02:20	Library Binary Analysis Started	OK
2024-10-23 23:02:21	Reading Code Signing Certificate	ОК
2024-10-23 23:02:23	Running APKiD 2.1.5	OK
2024-10-23 23:02:29	Detecting Trackers	ОК
2024-10-23 23:02:39	Decompiling APK to Java with jadx	OK
2024-10-23 23:04:10	Android SAST Completed	ОК
2024-10-23 23:04:10	Android API Analysis Started	ОК

#### 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.

© 2024 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.