

ANDROID STATIC ANALYSIS REPORT

app_icon

EvaluacionMapas-CMS (1.0)

File Name:	app-debug.apk
Package Name:	com.cms_dev.evaluacionmapas_cms
Scan Date:	Oct. 23, 2024, 3:45 p.m.
App Security Score:	36/100 (HIGH RISK)
Grade:	C

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	ℚ HOTSPOT
3	2	0	1	1

FILE INFORMATION

File Name: app-debug.apk

Size: 6.15MB

MD5: 4db804d6cc9b16bede1f19b5ea41c8ce

SHA1: c90bf9e2c84eb51395f158064b8f6155079ff381

SHA256: d09332e2896a2839dce38256f5dc9c5b9c60cea4f2b63cf8fbae9f1aef39f5b8

i APP INFORMATION

App Name: EvaluacionMapas-CMS

 $\begin{picture}(100,00) \put(0,0){\line(1,0){100}} \put(0,0){\line(1,0){1$

Main Activity: com.cms_dev.evaluacionmapas_cms.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: 2024-09-11 15:38:51+00:00 Valid To: 2054-09-04 15:38:51+00:00

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

Serial Number: 0x1 Hash Algorithm: sha256

md5: 5a062797f5d686dabd868a7bfbb8d776

sha1: 1b00737b2ac0bcbbad811ba9687983b5675b67b3

sha256: 88dd833be5fc5ae35c0a6d77e97f4474c51c4caefc7647db474500fb639be3e6

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 03bd3d8fd6681315d1b0fe7096bcb197d5bdd374e87ed987e826a6bc6e022ece

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.cms_dev.evaluacionmapas_cms.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference



FILE	DETAILS		
classes3.dex	FINDINGS DETAILS		
Classess.uex	Compiler	r8 without marker (suspicious)	
classes4.dex	FINDINGS DETAILS		
classes nack	Compiler r8 without marker (sus		picious)
classes2.dex	FINDINGS		DETAILS
classesziack	Compiler		dx
classes5.dex	FINDINGS DETAILS		
Classessiack	Compiler r8 without marker (sus		picious)

FILE	DETAILS	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

TITLE	SEVERITY	DESCRIPTION
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]	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.



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	Error
-----------	-------

2024-10-23 17:37:12	Generating Hashes	ОК
2024-10-23 17:37:12	Extracting APK	ОК
2024-10-23 17:37:12	Unzipping	ОК
2024-10-23 17:37:14	Getting Hardcoded Certificates/Keystores	ОК
2024-10-23 17:37:14	Parsing AndroidManifest.xml	ОК
2024-10-23 17:37:14	Parsing APK with androguard	ОК
2024-10-23 17:37:15	Detecting Trackers	ОК
2024-10-23 17:37:17	Extracting Manifest Data	ОК
2024-10-23 17:37:17	Performing Static Analysis on: EvaluacionMapas-CMS (com.cms_dev.evaluacionmapas_cms)	ОК
2024-10-23 17:37:17	Fetching Details from Play Store: com.cms_dev.evaluacionmapas_cms	ОК
2024-10-23 17:37:18	Manifest Analysis Started	ОК

2024-10-23 17:37:18	Checking for Malware Permissions	ОК
2024-10-23 17:37:18	Fetching icon path	ОК
2024-10-23 17:37:18	Library Binary Analysis Started	ОК
2024-10-23 17:37:22	Decompiling APK to Java with jadx	ОК
2024-10-23 17:37:22	Reading Code Signing Certificate	ОК
2024-10-23 17:37:26	Running APKiD 2.1.5	ОК
2024-10-23 17:37:39	Detecting Trackers	ОК
2024-10-23 17:37:52	Decompiling APK to Java with jadx	ОК
2024-10-23 17:38:00	Converting DEX to Smali	ОК
2024-10-23 17:38:00	Code Analysis Started on - java_source	OK
2024-10-23 17:38:01	Android SAST Completed	ОК

2024-10-23 17:38:01	Android API Analysis Started	ОК
2024-10-23 17:38:11	Android Permission Mapping Started	ОК
2024-10-23 17:38:16	Android Permission Mapping Completed	ОК
2024-10-23 17:38:16	Finished Code Analysis, Email and URL Extraction	ОК
2024-10-23 17:38:16	Extracting String data from APK	ОК
2024-10-23 17:38:18	Extracting String data from Code	ОК
2024-10-23 17:38:18	Extracting String values and entropies from Code	ОК
2024-10-23 17:38:19	Performing Malware check on extracted domains	OK
2024-10-23 17:38:19	Saving to Database	ОК
2024-10-23 17:38:34	Converting DEX to Smali	ОК
2024-10-23 17:38:34	Code Analysis Started on - java_source	ОК

2024-10-23 17:43:00	Android SAST Completed	ОК
2024-10-23 17:43:00	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.