ANDROID STATIC ANALYSIS REPORT

app_icon

EvaluacionACG-A0P
(1.0)

File Name:	app-debug.apk
Package Name:	com.example.evaluacionacg_a0p
Scan Date:	Oct. 24, 2024, 3:42 p.m.
App Security Score:	31/100 (HIGH RISK)
Grade:	

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	2	0	1	0

FILE INFORMATION

File Name: app-debug.apk
Size: 19.28MB
MD5: 10b4af7a4f38817ba3f163a6826e509b
SHA1: 02c267d97428c2b7abe18190716915be6cb38a8f
SHA256: 41e9794df082a95b53ad6890429f4cf058d76783837ca033ba6ed4dea4bb1675

APP INFORMATION

App Name: MapasACG-A0P
Package Name: com.example.evaluacionacg_a0p
Main Activity: com.example.evaluacionacg_a0p.MainActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 1
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 13:17:41+00:00
Valid To: 2054-08-12 13:17:41+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha1
md5: af16694b27d61f6a715c62f59d979e4a
sha1: 28db58488c692c4e86f3a35c0fb5f6962f828fd4
sha256: 381c8b9a5a0cff49fafea60166e662f44b841e6e6baad3aad712dfe4b53f0aa3
sha512: 0a2e31b84b130a2eaa1f2f7a400dad0fb90c77d57d25090e0e1c7f15908e8a3795b14a850280530a935fcf743d121e7d49a2cfecc700398c159ce1d65c61fdd9
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: ee417d3d1bfdcd37bb5a4ef4b3ee863dba662efa04bc6706c5fa8fd85b65a433
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.example.evaluacionacg_a0p.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>
</table>

FILE	DETAILS
classes.dex	<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</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 2 | 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.
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

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	0/24	
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
2024-10-24 15:43:54	Generating Hashes	OK
2024-10-24 15:43:54	Extracting APK	OK
2024-10-24 15:43:54	Unzipping	OK
2024-10-24 15:43:55	Getting Hardcoded Certificates/Keystores	OK
2024-10-24 15:43:55	Parsing AndroidManifest.xml	OK
2024-10-24 15:43:55	Parsing APK with androguard	OK
2024-10-24 15:43:56	Extracting Manifest Data	OK
2024-10-24 15:43:56	Performing Static Analysis on: EvaluacionACG-A0P (com.example.evaluacionacg_a0p)	OK
2024-10-24 15:43:56	Fetching Details from Play Store: com.example.evaluacionacg_a0p	OK
2024-10-24 15:43:56	Manifest Analysis Started	OK

2024-10-24 15:43:56	Checking for Malware Permissions	OK
2024-10-24 15:43:56	Fetching icon path	OK
2024-10-24 15:43:56	Library Binary Analysis Started	OK
2024-10-24 15:43:56	Reading Code Signing Certificate	OK
2024-10-24 15:43:57	Running APKiD 2.1.5	OK
2024-10-24 15:44:01	Detecting Trackers	OK
2024-10-24 15:44:05	Decompiling APK to Java with jadx	OK
2024-10-24 15:45:57	Converting DEX to Smali	OK
2024-10-24 15:45:57	Code Analysis Started on - java_source	OK
2024-10-24 15:48:37	Converting DEX to Smali	OK

2024-10-24 15:48:37	Code Analysis Started on - java_source	OK
2024-10-24 15:55:02	Android SAST Completed	OK
2024-10-24 15:55:02	Android API Analysis Started	OK
2024-10-24 15:55:37	Android SAST Completed	OK
2024-10-24 15:55:37	Android API Analysis Started	OK
2024-10-24 15:58:52	Android Permission Mapping Started	OK
2024-10-24 15:58:52	libsast scan failed	AttributeError("'NoneType' object has no attribute 'values'")
2024-10-24 15:58:52	Android Permission Mapping Completed	OK
2024-10-24 15:58:52	Finished Code Analysis, Email and URL Extraction	OK
2024-10-24 15:58:52	Extracting String data from APK	OK

2024-10-24 15:58:53	Extracting String data from Code	OK
2024-10-24 15:58:53	Extracting String values and entropies from Code	OK
2024-10-24 15:58:57	Performing Malware check on extracted domains	OK
2024-10-24 15:58:57	Saving to Database	OK
2024-10-24 16:02:14	Android Permission Mapping Started	OK
2024-10-24 16:02:15	libsast scan failed	AttributeError("'NoneType' object has no attribute 'values'")
2024-10-24 16:02:15	Android Permission Mapping Completed	OK
2024-10-24 16:02:17	Finished Code Analysis, Email and URL Extraction	OK
2024-10-24 16:02:17	Extracting String data from APK	OK
2024-10-24 16:02:19	Extracting String data from Code	OK

2024-10-24 16:02:19	Extracting String values and entropies from Code	OK
2024-10-24 16:02:34	Performing Malware check on extracted domains	OK
2024-10-24 16:02:34	Saving to Database	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.