ANDROID STATIC ANALYSIS REPORT

app_icon

CODIGO_PRUEVA (1.0)

File Name:	app-debug.apk
Package Name:	com.example.codigo_prueva
Scan Date:	Oct. 22, 2024, 3:13 p.m.
App Security Score:	31/100 (HIGH RISK)
Grade:	C

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	2	0	1	0

FILE INFORMATION

File Name: app-debug.apk
Size: 16.54MB
MD5: e9e8b21d78f5f8aacf6277338199800c
SHA1: ebf68b4c4f2c39f5cb3d34878580ab04e7f2c037
SHA256: f979a2fea708b64f7097b3cb0e94fa3ff1fe04017cb5d659de6d77810c2b8f80

APP INFORMATION

App Name: CODIGO_PRUEVA
Package Name: com.example.codigo_prueva
Main Activity: com.example.codigo_prueva.MainActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 2
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: 2024-08-27 16:16:50+00:00
Valid To: 2054-08-20 16:16:50+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha1
md5: b03b9683e16112eb285af5b81fa2a349
sha1: 753aad7805a7cf28fb97b62db40e24db67c65765
sha256: 1414a778ce9de3306ace9974d073c9a4d362908105e7c3a7ece607132c56c4a5
sha512: cde76954d470b41c58d7f1d420bd84dc5a2aa9f534af1f90dd38223ea683788b6977c6d3eda073897082ff189be3b9670963258cedac85ac67d7e7c956453bba
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: ebb19f94cf36c21f052e9e16c228912cd2840fc21903dd9e3e9f9cd84f8acc99
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.example.codigo_prueva.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes3.dex	FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)
classes2.dex	FINDINGS: Compiler — DETAILS: dx

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
2024-10-22 15:54:50	Generating Hashes	OK
2024-10-22 15:54:51	Extracting APK	OK
2024-10-22 15:54:51	Unzipping	OK
2024-10-22 15:54:52	Getting Hardcoded Certificates/Keystores	OK
2024-10-22 15:54:53	Parsing AndroidManifest.xml	OK
2024-10-22 15:54:53	Parsing APK with androguard	OK
2024-10-22 15:54:55	Extracting Manifest Data	OK
2024-10-22 15:54:55	Performing Static Analysis on: CODIGO_PRUEVA (com.example.codigo_prueva)	OK
2024-10-22 15:54:55	Fetching Details from Play Store: com.example.codigo_prueva	OK
2024-10-22 15:54:55	Manifest Analysis Started	OK

2024-10-22 15:54:55	Checking for Malware Permissions	OK
2024-10-22 15:54:55	Fetching icon path	OK
2024-10-22 15:54:55	Library Binary Analysis Started	OK
2024-10-22 15:54:56	Reading Code Signing Certificate	OK
2024-10-22 15:54:58	Running APKiD 2.1.5	OK
2024-10-22 15:55:11	Detecting Trackers	OK
2024-10-22 15:55:29	Decompiling APK to Java with jadx	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.