MOBSF

ANDROID STATIC ANALYSIS REPORT

Rimichka (1.0)

File Name:	sample.apk
Package Name:	com.avtobiografia.rimichka
Scan Date:	Oct. 17, 2025, 11:47 a.m.
App Security Score:	24/100 (CRITICAL RISK)
Grade:	

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
5	1	0	1	0

FILE INFORMATION

File Name: sample.apk
Size: 0.01MB
MD5: ccb79f5b25ce17ede0e94fda4803391f
SHA1: 98282eac31dc1f05bf1a1dca2858f6927c090694
SHA256: 0911689e14684722de61f1102d99f905c76d8069bf00de247888612760ecc091

APP INFORMATION

App Name: Rimichka
Package Name: com.avtobiografia.rimichka
Main Activity: .RimichkaActivity
Target SDK: 8
Min SDK: 8
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 1
Services: 0
Receivers: 0
Providers: 0
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: C=US, O=Android, CN=Android Debug
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-02-04 11:08:39+00:00
Valid To: 2042-01-27 11:08:39+00:00
Issuer: C=US, O=Android, CN=Android Debug
Serial Number: 0x4f2d11b7
Hash Algorithm: sha1
md5: 580443a68bede3414b030a3c98461ddd
sha1: 5ce1d29cac8dd3ca6dc90e4136d1f536b306bcc9
sha256: ca3911dbefb06ab4532c0b7d66b8fb751ac3b5efadaba2dfcd8ba649ea5a1d93
sha512: e123113c47b52a4af370db3da5add2353545a81eea87efa23aa23324f11c37ea34b7375f07d8b2e99233b2e4d1d7ae017b379e7f7f35a2bff154059a160f09fc
Found 1 unique certificates

APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dx</td></tr></table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 3 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	high	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.

TITLE	SEVERITY	DESCRIPTION
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: 1 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 2.2-2.2.3, [minSdk=8]	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] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	0/25	
Other Common Permissions	0/44	

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
2025-10-17 11:47:46	Generating Hashes	OK
2025-10-17 11:47:46	Extracting APK	OK

2025-10-17 11:47:46	Unzipping	OK
2025-10-17 11:47:46	Parsing APK with androguard	OK
2025-10-17 11:47:46	Extracting APK features using aapt/aapt2	OK
2025-10-17 11:47:46	Getting Hardcoded Certificates/Keystores	OK
2025-10-17 11:47:49	Parsing AndroidManifest.xml	OK
2025-10-17 11:47:49	Extracting Manifest Data	OK
2025-10-17 11:47:49	Manifest Analysis Started	OK
2025-10-17 11:47:49	Performing Static Analysis on: Rimichka (com.avtobiografia.rimichka)	OK
2025-10-17 11:47:51	Fetching Details from Play Store: com.avtobiografia.rimichka	OK
2025-10-17 11:47:52	Checking for Malware Permissions	OK
2025-10-17 11:47:52	Fetching icon path	OK

2025-10-17 11:47:52	Library Binary Analysis Started	OK
2025-10-17 11:47:52	Reading Code Signing Certificate	OK
2025-10-17 11:47:52	Running APKiD 3.0.0	OK
2025-10-17 11:47:57	Detecting Trackers	OK
2025-10-17 11:47:58	Decompiling APK to Java with JADX	OK
2025-10-17 11:48:00	Converting DEX to Smali	OK
2025-10-17 11:48:00	Code Analysis Started on - java_source	OK
2025-10-17 11:48:00	Android SBOM Analysis Completed	OK
2025-10-17 11:48:00	Android SAST Completed	OK
2025-10-17 11:48:00	Android API Analysis Started	OK
2025-10-17 11:48:01	Android API Analysis Completed	OK

2025-10-17 11:48:01	Android Behaviour Analysis Started	OK
2025-10-17 11:48:01	Android Behaviour Analysis Completed	OK
2025-10-17 11:48:01	Extracting Emails and URLs from Source Code	OK
2025-10-17 11:48:01	Email and URL Extraction Completed	OK
2025-10-17 11:48:01	Extracting String data from APK	OK
2025-10-17 11:48:01	Extracting String data from Code	OK
2025-10-17 11:48:01	Extracting String values and entropies from Code	OK
2025-10-17 11:48:01	Performing Malware check on extracted domains	OK
2025-10-17 11:48:01	Saving to Database	OK

Report Generated by - MobSF v4.4.3

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.