MOBSF

ANDROID STATIC ANALYSIS REPORT

encryptor (1.0)

File Name:	encryptor.apk
Package Name:	com.example.encryptor
Scan Date:	Sept. 6, 2024, 7:54 p.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	2	0	1	0

FILE INFORMATION

File Name: encryptor.apk
Size: 4.39MB
MD5: 83c7d4def6410f6c1b5f1ad38442d51d
SHA1: b4287322161712ff5491b1a677ea5348153df3fa
SHA256: e6ddbbfd133851f355c7ead12cea9f98c2aa20eb21ec865b1cae3926fcb6efb9

APP INFORMATION

App Name: encryptor
Package Name: com.example.encryptor
Main Activity: com.example.encryptor.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=encryptor, OU=encryptor, O=encryptor, L=encryptor, ST=encryptor, C=encryptor
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2024-08-16 11:05:34+00:00
Valid To: 2049-08-10 11:05:34+00:00
Issuer: CN=encryptor, OU=encryptor, O=encryptor, L=encryptor, ST=encryptor, C=encryptor
Serial Number: 0x1
Hash Algorithm: sha256
md5: 61f573be300ea6798f0764e6da7edd5b
sha1: 7bef27d68d52cba52643f3096b8af1ac5d3efc3d
sha256: e6299475c71452b0014540c771aa562c1c20504b0b6bc9330b4f3cd2d1d6a739
sha512: fd12ef2d61d2a6c609235a2439109fd71eeca09bfa8c23ec671dbc79286932cd5e82c5a66e49414de89f0d5bd322fb69607239ce775b1ca328fd700027c7018e
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: b313f255c49e03d7696fad88d856b5fc74d51152ae77b99f026940870e5fe3ad
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION

com.example.encryptor.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

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

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: 1 | 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	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.
3	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
2024-09-06 20:06:33	Generating Hashes	OK
2024-09-06 20:06:33	Extracting APK	OK
2024-09-06 20:06:33	Unzipping	OK
2024-09-06 20:06:34	Getting Hardcoded Certificates/Keystores	OK

2024-09-06 20:06:53	Parsing AndroidManifest.xml	OK
2024-09-06 20:06:53	Parsing APK with androguard	OK
2024-09-06 20:06:55	Extracting Manifest Data	OK
2024-09-06 20:06:55	Performing Static Analysis on: encryptor (com.example.encryptor)	OK
2024-09-06 20:06:55	Fetching Details from Play Store: com.example.encryptor	OK
2024-09-06 20:06:56	Manifest Analysis Started	OK
2024-09-06 20:06:56	Checking for Malware Permissions	OK
2024-09-06 20:06:56	Fetching icon path	OK
2024-09-06 20:06:56	Library Binary Analysis Started	OK
2024-09-06 20:06:56	Reading Code Signing Certificate	OK
2024-09-06 20:06:57	Running APKiD 2.1.5	OK
	Detecting Trackers	OK

2024-09-06 20:07:06		
2024-09-06 20:07:09	Decompiling APK to Java with jadx	OK
2024-09-06 20:09:09	Converting DEX to Smali	OK
2024-09-06 20:09:09	Code Analysis Started on - java_source	OK
2024-09-06 20:13:13	Android SAST Completed	OK
2024-09-06 20:13:13	Android API Analysis Started	OK
2024-09-06 20:17:08	Android Permission Mapping Started	OK
2024-09-06 20:17:09	libsast scan failed	AttributeError("'NoneType' object has no attribute 'values'")
2024-09-06 20:17:09	Android Permission Mapping Completed	OK
2024-09-06 20:17:09	Finished Code Analysis, Email and URL Extraction	OK
2024-09-06 20:17:09	Extracting String data from APK	OK
2024-09-06 20:17:09	Extracting String data from Code	OK

2024-09-06 20:17:09	Extracting String values and entropies from Code	OK
2024-09-06 20:17:13	Performing Malware check on extracted domains	OK
2024-09-06 20:17:13	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.