ANDROID STATIC ANALYSIS REPORT

app_icon

POEPart2Example

File Name:	TicTrack.zip
Package Name:	
Scan Date:	Aug. 30, 2024, 5:14 p.m.
App Security Score:	44/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	2	1	1	1

FILE INFORMATION

File Name: TicTrack.zip
Size: 45.17MB
MD5: 55133884963244fddc9c338f558ce9cf
SHA1: 95dfab373e849143085db9994589f8891441c617
SHA256: 31ef26f8b32e3c2fc64662f25d1f488be06a7c6024cea6b1b9cc849b28712f70

APP INFORMATION

App Name: POEPart2Example
Package Name:
Main Activity: .SplashActivity
Target SDK:
Min SDK:
Max SDK:
Android Version Name:
Android Version Code:

APP COMPONENTS

Activities: 15
Services: 0
Receivers: 0
Providers: 0
Exported Activities: 1
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

Failed to read Code Signing Certificate or none available.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

TITLE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

HIGH: 2 | WARNING: 2 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	Activity (.SplashActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (26) of the app to 29 or higher to fix this issue at platform level.
3	Activity (.MainActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (26) of the app to 29 or higher to fix this issue at platform level.
4	Activity (.MainActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

CODE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1 | SECURE: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/example/poepart2example/fragments/SettingsFragment.kt

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	1/24	android.permission.READ_EXTERNAL_STORAGE
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
2024-08-30 17:14:04	Extracting ZIP	OK
2024-08-30 17:14:04	Unzipping	OK
2024-08-30 17:14:05	Detecting source code type	OK
2024-08-30 17:14:05	Source code type - studio	OK
2024-08-30 17:14:05	Generating Hashes	OK
2024-08-30 17:14:05	Getting Hardcoded Certificates/Keystores	OK
2024-08-30 17:14:05	Parsing AndroidManifest.xml	OK
2024-08-30 17:14:05	Extracting Manifest Data	OK
2024-08-30 17:14:05	Fetching Details from Play Store:	OK

2024-08-30 17:14:05	Manifest Analysis Started	OK
2024-08-30 17:14:05	Checking for Malware Permissions	OK
2024-08-30 17:14:05	Guessing icon path	OK
2024-08-30 17:14:05	Code Analysis Started on - java	OK
2024-08-30 17:14:06	Android SAST Completed	OK
2024-08-30 17:14:06	Android API Analysis Started	OK
2024-08-30 17:14:06	Android Permission Mapping Started	OK
2024-08-30 17:14:06	Android Permission Mapping Completed	OK
2024-08-30 17:14:06	Finished Code Analysis, Email and URL Extraction	OK
2024-08-30 17:14:06	Extracting String data from Code	OK
2024-08-30 17:14:07	Extracting String values and entropies from Code	OK

2024-08-30 17:14:07	Performing Malware check on extracted domains	OK
2024-08-30 17:14:07	Detecting Trackers from Domains	OK
2024-08-30 17:14:07	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.