MOBSF

ANDROID STATIC ANALYSIS REPORT

Location Share (1.2)

File Name:	installer358.apk
Package Name:	ca.cmetcalfe.locationshare
Scan Date:	May 30, 2022, 4:15 p.m.
App Security Score:	56/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	1	1	1	1

FILE INFORMATION

File Name: installer358.apk
Size: 0.79MB
MD5: a1164c4d686e2bb174b7d1072049aa11
SHA1: c3ee4a587b729496a1732d6a4bbf898a988bec9a
SHA256: b77bdddb616fb5a5889ff2d96b3264f4814428a832df2b998df7b0c3e6354db2

APP INFORMATION

App Name: Location Share
Package Name: ca.cmetcalfe.locationshare
Main Activity: ca.cmetcalfe.locationshare.MainActivity
Target SDK: 25
Min SDK: 9
Max SDK:
Android Version Name: 1.2
Android Version Code: 3

APP COMPONENTS

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

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-11-04 20:31:47+00:00
Valid To: 2044-03-22 20:31:47+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x1872ec9c
Hash Algorithm: sha256
md5: 198cc173b4b36dd72e773bfe0632e293
sha1: 4abfca4bf0292fb248fcf09fb7a9df6871a9266b
sha256: afbe444805ef95598d568ba9d24f9389109f8b293227a7a38a9fbe60f0c3dba1
sha512: 0752e25c961f3c7ae7dc7f911d9d5d07b9f85e8931542b1c6842c59406307faf29bd4c6999941c325d026a38cbe84153022d01e27b16cb9a55add8340581af6d

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

TITLE	SEVERITY	DESCRIPTION
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 PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Compiler — DETAILS: dx

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

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.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	ca/cmetcalfe/locationshare/MainActivity.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
2	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['location'].
4	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
5	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has no network communications.
6	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files in non-volatile memory.
7	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does not encrypt any data in traffic or does not transmit any data between itself and another trusted IT product.

Report Generated by - MobSF v3.5.2 Beta

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.