

ANDROID STATIC ANALYSIS REPORT



• Location Share (1.3.2)

File Name:	installer325.apk
Package Name:	ca.cmetcalfe.locationshare
Scan Date:	May 31, 2022, 11:15 a.m.
App Security Score:	56/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

兼 HIGH	▲ MEDIUM	i INFO	✓ SECURE	≪ HOTSPOT
1	1	2	1	1

FILE INFORMATION

File Name: installer325.apk

Size: 0.91MB

MD5: feeec6d89efb36c4b2037f2bf31ca9a8

SHA1: e616c675346f62bbe2b2101ec1cbc1bc573eb166

SHA256: a9ef5f9ba415c4e4f3555940dff100e8a416063676d3486a930bc1f87bb2a818

i APP INFORMATION

App Name: Location Share

Package Name: ca.cmetcalfe.locationshare

Main Activity: ca.cmetcalfe.locationshare.MainActivity

Target SDK: 28 Min SDK: 14 Max SDK:

Android Version Name: 1.3.2 Android Version Code: 6

EE APP COMPONENTS

Activities: 2 Services: 0 Receivers: 0 Providers: 0

Exported Activities: O Exported Services: O Exported Receivers: O Exported Providers: O

***** 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: afbe 444805 ef 95598 d568 ba 9d24 f 9389109 f 8b 293227 a 7a 38a 9fbe 60 f 0c3 dba 10 february 10 februa

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.

M APKID ANALYSIS

FILE	DETAILS		
classes.dex	FINDINGS	DETAILS	
Classes.uex	Compiler	dx	



NO	SCOPE	SEVERITY	DESCRIPTION	

Q 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	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	ca/cmetcalfe/locationshare/MainActivit y.java
2	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/MainActivit y.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.
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.

@ 2022 Mobile Security Framework - MobSF | $\underline{\mbox{Ajin Abraham}}$ | $\underline{\mbox{OpenSecurity}}.$