MOBSF

ANDROID STATIC ANALYSIS REPORT

Sensors Sandbox (1.7)

File Name:	installer6.apk
Package Name:	com.mustafaali.sensorssandbox
Scan Date:	May 31, 2022, 5:39 a.m.
App Security Score:	56/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	1	0	1	0

FILE INFORMATION

File Name: installer6.apk
Size: 0.25MB
MD5: 96b6927099e58a91bc96b7cd1d827f41
SHA1: 7aa2060c7c6ec56d01420c8156fa9ef4dc83532a
SHA256: cc83fe836f7c98ed97a0212fcfed0f5069878833c5c72090419cdc028b69a68b

APP INFORMATION

App Name: Sensors Sandbox
Package Name: com.mustafaali.sensorssandbox
Main Activity: com.mustafaali.sensorssandbox.MainActivity
Target SDK: 18
Min SDK: 9
Max SDK:
Android Version Name: 1.7
Android Version Code: 7

APP COMPONENTS

Activities: 2
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: 2014-11-10 07:00:27+00:00
Valid To: 2042-03-28 07:00:27+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x651fea54
Hash Algorithm: sha256
md5: 0b36da2064a5adebc815acd05794d079
sha1: f2409e85f6e252ea326e7f8507f262a43dec8c18
sha256: 92caa1d789abee64428a82ba019d607850c46a25ad33f5d60ff4add32f1d6b52
sha512: e73e8ccc2b991d5cfc97ab1f1a39c07f003da309b5fa4e947b20e79edf49bcc94b6204493bdcfda9ae082c35dddbe69dff46650c85f529157d4df16d1c8d03fa

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.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>dx (possible dexmerge)</td></tr>
<tr><td>Manipulator Found</td><td>dexmerge</td></tr>
</table>
</td></tr>
</table>

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

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 no hardware resources.
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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.121.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
play.google.com	ok	**IP:** 142.251.36.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
twitter.com	ok	**IP:** 104.244.42.129 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map

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.