ANDROID STATIC ANALYSIS REPORT

🤖 AndrOBD SensorProvider
(V1.0.4)

File Name: installer31.apk

Package Name: com.fr3ts0n.androbd.plugin.sensorprovider

Scan Date: May 31, 2022, 3:24 p.m.

App Security Score: **28/100 (CRITICAL RISK)**

Grade:

F

⊕ FINDINGS SEVERITY

🐛 HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	🔍 HOTSPOT
4	1	1	1	0

⊟ FILE INFORMATION

File Name: installer31.apk
Size: 0.03MB
MD5: 47e91c0484b4d54b923eec674c4b4a04
SHA1: a18b78d88e3bd1e9b314b9a9f627e7a0e9923b91
SHA256: 76190a13101385798019dc8ed184dbef861d30fe0e0f8dc4d3ea61ec2eb9d8cf

ℹ APP INFORMATION

App Name: AndrOBD SensorProvider
Package Name: com.fr3ts0n.androbd.plugin.sensorprovider
Main Activity: com.fr3ts0n.androbd.plugin.sensorprovider.SettingsActivity
Target SDK: 25
Min SDK: 15
Max SDK:
Android Version Name: V1.0.4
Android Version Code: 10004

▣ APP COMPONENTS

Activities: 1
Services: 2
Receivers: 1
Providers: 0
Exported Activities: 0
Exported Services: 2
Exported Receivers: 1
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: 2019-09-25 16:40:20+00:00
Valid To: 2047-02-10 16:40:20+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x51ab8011
Hash Algorithm: sha256
md5: 3c2f3b80ca66628aa802ea1f23ea3332
sha1: 4eaa188402ea8f940dcd8bdbc9ad20f82048f1f4
sha256: 13b65b25996562343e50ad1e2ba455deff5121ba3678cfcd018524272efb9c63
sha512: 0e1720cd614f3431d968e37467ccd5c4b16f2941256506d9e79460bf7ed8e4292191f43dd4aeee100f8c6e27dd6f8f8b2a7cd5b966edfc3a86cc358b91802df4

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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

🖐 APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><td>FINDINGS</td><td>DETAILS</td></tr><tr><td>Compiler</td><td>r8</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.
2	Broadcast Receiver (com.fr3ts0n.androbd.plugin.sensorprovider.PluginReceiver) is not Protected. [android:exported=true]	high	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.
3	Service (com.fr3ts0n.androbd.plugin.sensorprovider.SensorProvider) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Service (com.fr3ts0n.androbd.plugin.mgr.PluginDataService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

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	com/fr3ts0n/androbd/plugin/sensorprovider/SensorProvider.java com/fr3ts0n/androbd/plugin/mgr/PluginHandler.java com/fr3ts0n/androbd/plugin/Plugin.java com/fr3ts0n/androbd/plugin/PluginReceiver.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 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.
6	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files in non-volatile memory.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
7	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
8	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

⚲ DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **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.