ANDROID STATIC ANALYSIS REPORT

Car Bus Interface (0.9)

File Name:	installer255.apk
Package Name:	com.theksmith.android.car_bus_interface
Scan Date:	May 31, 2022, 2:14 p.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	3	1	1	1

FILE INFORMATION

File Name: installer255.apk
Size: 0.29MB
MD5: dd874ca7b34f2f63ef85757d18928040
SHA1: 94d000c3dc027b3b23eed40421f778b39592102e
SHA256: 2eab7f5c5fe1b19be2f3451cf6356432dcaf6a745168a0d6b6e4156a3b87ec54

APP INFORMATION

App Name: Car Bus Interface
Package Name: com.theksmith.android.car_bus_interface
Main Activity: com.theksmith.android.car_bus_interface.CBIActivityMain
Target SDK: 19
Min SDK: 16
Max SDK:
Android Version Name: 0.9
Android Version Code: 90

APP COMPONENTS

Activities: 3
Services: 1
Receivers: 1
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: 2014-11-24 07:03:10+00:00
Valid To: 2042-04-11 07:03:10+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x69e2ebeb
Hash Algorithm: sha256
md5: 247216c93accef7090e96ad589de4153
sha1: 3592bc9ed63d085872e5d5b65f3a8f530cccec08
sha256: 90eec75727975c85f0419ab03da9c2debb5e699b6d3de8d65e07a15871e9cb7c
sha512: 8f6c13532159b484afc01a0e1f909bf5399c952ba346cd9a8c4a51f3c6d6d7f7ede48ddd3c8167a86618b143115418ec408c3b0000d001ba93e2560b2f890fa7

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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
android.permission.REORDER_TASKS	normal	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.
net.dinglisch.android.tasker.PERMISSION_RUN_TASKS	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_SUPERUSER	unknown	Unknown permission	Unknown permission from android reference

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
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/theksmith/android/car_bus_interface/BusMessageProcessor.java com/theksmith/android/car_bus_interface/AndroidActions.java net/dinglisch/android/tasker/TaskerIntent.java com/theksmith/android/car_bus_interface/CBIServiceMain.java
2	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	net/dinglisch/android/tasker/TaskerIntent.java
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	net/dinglisch/android/tasker/TaskerIntent.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application use no DRBG functionality for its cryptographic operations.
2	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
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['bluetooth'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has no network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files in non-volatile memory.
8	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.
9	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

DOMAIN	STATUS	GEOLOCATION
tasker.dinglisch.net	ok	**IP:** 87.247.244.225 **Country:** Germany **Region:** Nordrhein-Westfalen **City:** Koeln **Latitude:** 50.933331 **Longitude:** 6.950000 **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.