



## ANDROID STATIC ANALYSIS REPORT



 AndrOBD (V2.1.3)

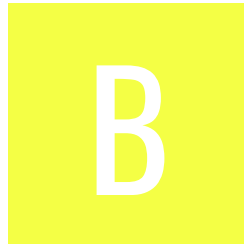
File Name: installer352.apk

Package Name: com.fr3ts0n.ecu.gui.androbd






Scan Date: May 31, 2022, 2:28 p.m.

App Security Score: 45/100 (MEDIUM RISK)

Grade:



## FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
2	3	1	1	1

## FILE INFORMATION

File Name: installer352.apk

Size: 0.58MB

MD5: 40e7d71e76c88babf011af25292a0597

SHA1: 251527759e99afb776d56f80f62d0a9a73de4a7a

SHA256: 9486445700e3231bcb318563b3fbda4317946a0bac3edfcc578af4fe90c90346

## APP INFORMATION

App Name: AndrOBD

Package Name: com.fr3ts0n.ecu.gui.androbd

Main Activity: com.fr3ts0n.ecu.gui.androbd.MainActivity

Target SDK: 25

Min SDK: 15

Max SDK:

Android Version Name: V2.1.3

Android Version Code: 20103

## APP COMPONENTS

Activities: 6

Services: 1

Receivers: 0

Providers: 0

Exported Activities: 0

Exported Services: **1**

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: 2015-05-26 20:34:55+00:00

Valid To: 2042-10-11 20:34:55+00:00

Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid

Serial Number: 0x7bb219bc

Hash Algorithm: sha256

md5: 9b4554664941a3060e7615c8b75dfecd

sha1: 80661616862195b9602a5e138cf1f75098b1a507

sha256: 60d7575f56e8fe0e268365d0f90a8430721a0288f30f191435b12398ec1a3990

sha512: 8c4d7c3da55ca8b91d28f672776b444e891bbd8debd98b432fa74e7f66f7f40f98fc491d9a0cc4dbb5d903f0882acaa976cb56d1e7d136a7b6f263a8531c0a1d

TITLE	SEVERITY	DESCRIPTION
Signed Application	<a href="#">info</a>	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_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.

## APKID ANALYSIS

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Compiler	r8 without marker (suspicious)

## 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	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
1	<a href="#">The App logs information. Sensitive information should never be logged.</a>	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/fr3ts0n/androbd/plugin/PluginReceiver.java com/fr3ts0n/androbd/plugin/mgr/PluginHandler.java com/hoho/android/usbserial/driver/CdcAcmSerialDriver.java com/hoho/android/usbserial/driver/FtdiSerialDriver.java com/hoho/android/usbserial/driver/Cp21xxSerialDriver.java com/fr3ts0n/androbd/plugin/Plugin.java com/hoho/android/usbserial/util/SerialInputOutputManager.java com/hoho/android/usbserial/driver/ProlificSerialDriver.java
2	<a href="#">App can read/write to External Storage. Any App can read data written to External Storage.</a>	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/fr3ts0n/ecu/gui/androbd/Screenshot.java com/fr3ts0n/ecu/gui/androbd/FileHelper.java
3	<a href="#">Files may contain hardcoded sensitive information like usernames, passwords, keys etc.</a>	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/fr3ts0n/pvs/io/PvXMLWriter.java

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 ['network connectivity', 'bluetooth', 'USB'].
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 user/application initiated 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	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
xml.apache.org	ok	IP: 151.101.2.132 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: <a href="#">Google Map</a>
www.makedonov.ru	ok	No Geolocation information available.
hosted.weblate.org	ok	IP: 116.203.108.97 Country: Germany Region: Bayern City: Gunzenhausen Latitude: 48.323330 Longitude: 11.601220 View: <a href="#">Google Map</a>
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: <a href="#">Google Map</a>

---

## 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.