

ANDROID STATIC ANALYSIS REPORT



AndrOBD GpsProvider (V1.0.3)

File Name:	installer169.apk
Package Name:	com.fr3tsOn.androbd.plugin.gpsprovider
Scan Date:	May 31, 2022, 4:35 p.m.
App Security Score:	28/100 (CRITICAL RISK)
Grade:	F

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	≪ HOTSPOT
4	1	1	1	1

FILE INFORMATION

File Name: installer169.apk

Size: 0.03MB

MD5: 6ae07869492275889fa92f4cccdf2d8f

SHA1: 35595e0ad6bb9b1dd841c77243a29eb2969a774d

SHA256: 67742925aabd1a6d581914488bad25e903fa3aced26b7708ec50d4524d15f274

i APP INFORMATION

App Name: AndrOBD GpsProvider

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

 ${\it Main\ Activity:} com. fr 3 ts 0 n. and robd. plugin. gps provider. Settings Activity$

Target SDK: 28 Min SDK: 16 Max SDK:

Android Version Name: V1.0.3 Android Version Code: 10003

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: 2019-09-19 06:41:09+00:00 Valid To: 2047-02-04 06:41:09+00:00

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

Serial Number: 0x3a96444b Hash Algorithm: sha256

md5: b576d92942eb979a9bf9e1608298beb2 sha1: 24c1a4060b4a9046ff9f6b9f342f5bf008915a4c

sha256: 7dd282b1609ffd9054d7a8534d985da0d556309aabd58f42869003a4f98fd87e

sha512: 348bb3e4fc4e45e00ca4508693d89ada9a3f9dcb2c1c579d5ec668b62fcf31a4d8ef060d7f738b6940a490d3f386162fcc0a68882862c22cb75c48666f6563e6

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_COARSE_LOCATION	dangerous	coarse (network- based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
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.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

ক্ল APKID ANALYSIS

TILE	DETAILS
------	---------

FILE	DETAILS		
	FINDINGS	DETAILS	
classes.dex	Compiler	r8	

△ NETWORK SECURITY

NO SCOPE SEVERITY DESCRIPTION	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.
2	Broadcast Receiver (com.fr3ts0n.androbd.plugin.gpsprovider.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.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Service (com.fr3ts0n.androbd.plugin.gpsprovider.GpsProvider) 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
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/mgr/PluginHan dler.java com/fr3ts0n/androbd/plugin/gpsprovider/Gp sProvider.java com/fr3ts0n/androbd/plugin/Plugin.java com/fr3ts0n/androbd/plugin/PluginReceiver.j ava

■ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

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	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.

Q 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

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 | Ajin Abraham | OpenSecurity.