ANDROID STATIC ANALYSIS REPORT

Wi-Fi Privacy Police (2.2.4)
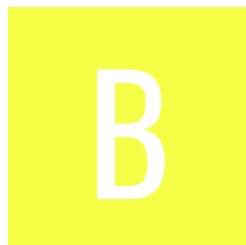
File Name:	installer210.apk
Package Name:	be.uhasselt.privacypolice
Scan Date:	May 30, 2022, 4:02 p.m.
App Security Score:	**56/100 (MEDIUM RISK)**
Grade:	**B**

⬤ FINDINGS SEVERITY

🐞 HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	🔍 HOTSPOT
1	1	1	1	1

📦 FILE INFORMATION

File Name: installer210.apk
Size: 0.13MB
MD5: d841845348f89174e8ba1db099b6d4a2
SHA1: 38cc99a8f5ab870a751e8e7d96d432d55e867943
SHA256: b6d286329ca6eed9c86c9da1054a677531d8a96088c1559fe0f7b2742d3f16c4

ℹ APP INFORMATION

App Name: Wi-Fi Privacy Police
Package Name: be.uhasselt.privacypolice
Main Activity: be.uhasselt.privacypolice.PreferencesActivity
Target SDK: 22
Min SDK: 14
Max SDK:
Android Version Name: 2.2.4
Android Version Code: 13

⬛ APP COMPONENTS

Activities: 5
Services: 0
Receivers: 4
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: 2015-02-17 08:33:00+00:00
Valid To: 2042-07-05 08:33:00+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x2f0ea9a3
Hash Algorithm: sha256
md5: a62ba7aab8580012747df5de85386782
sha1: 82deb8a3c029bb07bd604b10e4d12b8afcc9583e
sha256: d13302a39fbac1269ccd4f0c50414c17f879abae57603ed09d698559cd5d933d
sha512: acc8e7b8bbc8963b3c270644d1e0abde0629ef83b75bec11b7ec5ad4da0db3fdb5b19e788011e8d08aaa81946d725a890f70b95f5c2f9d72fc352fa5f692ec6f

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_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
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.

ᯤ APKID ANALYSIS

FILE	DETAILS	
classes.dex	**FINDINGS**	**DETAILS**
	Compiler	dx

🔒 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

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	be/uhasselt/privacypolice/l.java be/uhasselt/privacypolice/ScanResultsChecker.java be/uhasselt/privacypolice/m.java be/uhasselt/privacypolice/SSIDManagerActivity.java be/uhasselt/privacypolice/h.java be/uhasselt/privacypolice/MACManagerActivity.java be/uhasselt/privacypolice/r.java be/uhasselt/privacypolice/k.java be/uhasselt/privacypolice/PermissionChangeReceiver.java be/uhasselt/privacypolice/WakelockHandler.java be/uhasselt/privacypolice/LocationAccess.java be/uhasselt/privacypolice/s.java be/uhasselt/privacypolice/o.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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['location', 'network connectivity'].
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 not encrypt any data in traffic or does not transmit any data between itself and another trusted IT product.

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.