MOBSF

ANDROID STATIC ANALYSIS REPORT

WiFiAnalyzer (2.1.2)

File Name:	installer215.apk
Package Name:	com.vrem.wifianalyzer
Scan Date:	May 31, 2022, 5:49 a.m.
App Security Score:	53/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	4	1	1	0

FILE INFORMATION

File Name: installer215.apk
Size: 2.41MB
MD5: dc44475d71cc0238bf7fcb5d9746b277
SHA1: a854d177e9e1ac4c3bbaf83c70d5837a24d340e1
SHA256: b265d5131c15ae860aeee979df3fcbaea35ed217fbe40b2c143697bcf599526f

APP INFORMATION

App Name: WiFiAnalyzer
Package Name: com.vrem.wifianalyzer
Main Activity: com.vrem.wifianalyzer.SplashActivity
Target SDK: 29
Min SDK: 19
Max SDK:
Android Version Name: 2.1.2
Android Version Code: 52

APP COMPONENTS

Activities: 2
Services: 0
Receivers: 0
Providers: 0
Exported Activities: 1
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: 2016-04-17 08:14:31+00:00
Valid To: 2043-09-03 08:14:31+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x7f1d2b5c
Hash Algorithm: sha256
md5: 1e0afdf1c994f1cef76a1ea127aca455
sha1: f226e68b68f52316c33aeb35a28bbd7fdfc9313a
sha256: 3a14f8bbead3d530ae0aa0b578b945bdd7667b6e2e27da30cd46349356998f3e
sha512: 377fad69f18200005a2050dba33ba3cfc77ebdde14fd1604f7b03434913fcb4489b43e31ab8a44243069316f4ad28cf06c9e5d570a1ac966e7e8218d9229044a

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.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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: DETAILS Anti-VM Code: Build.MANUFACTURER check Compiler: unknown (please file detection issue!)

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	Activity (com.vrem.wifianalyzer.MainActivity) is not Protected. An intent-filter exists.	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.

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	b/f/h/a.java b/h/b/c.java c/b/a/c.java b/f/d/c/f.java b/a/k/a/a.java b/f/d/c/a.java b/f/l/x.java b/f/l/u.java b/f/l/b.java b/f/e/b.java b/f/l/d0/c.java c/a/a/a/z/b.java b/l/i0.java b/f/j/b.java c/b/a/i.java b/f/e/f.java c/a/a/a/y/d.java b/f/k/b.java b/f/e/j.java c/a/a/a/m/h.java b/f/l/e.java b/m/a/a/i.java b/f/l/g.java b/f/l/v.java b/f/e/i.java b/f/e/e.java b/f/e/d.java b/l/y.java b/a/o/g.java b/f/d/c/b.java b/j/a/b.java
2	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/vrem/wifianalyzer/l/g/h.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 ['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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
9	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 142.250.179.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.android-graphview.org	ok	**IP:** 81.169.145.156 **Country:** Germany **Region:** Berlin **City:** Berlin **Latitude:** 52.524368 **Longitude:** 13.410530 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
design.google.com	ok	**IP:** 142.251.39.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
en.wikipedia.org	ok	**IP:** 91.198.174.192 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
vremsoftwaredevelopment.github.io	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.gnu.org	ok	**IP:** 209.51.188.116 **Country:** United States of America **Region:** Massachusetts **City:** Boston **Latitude:** 42.358429 **Longitude:** -71.059769 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.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:** Google Map
schemas.android.com	ok	No Geolocation information available.
commons.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:** Google Map

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"ap_view_key" : "view"
"channel_graph_legend_key" : "channel_graph_legend"
"connection_view_key" : "connection"
"country_code_key" : "country_code"

POSSIBLE SECRETS
"experimental_key" : "experimental_key"
"filter_security_key" : "filter_security"
"filter_ssid_key" : "filter_ssid"
"filter_strength_key" : "filter_strength"
"filter_wifi_band_key" : "filter_wifi_band"
"graph_maximum_y_key" : "graph_maximum_y"
"group_by_key" : "group_by"
"keep_screen_on_key" : "keep_screen_on"
"language_key" : "language"
"scan_speed_key" : "scan_speed"
"selected_menu_key" : "selected_menu"
"sort_by_key" : "sort_by"
"theme_key" : "theme"
"time_graph_legend_key" : "time_graph_legend"
"wifi_band_key" : "wifi_band"

POSSIBLE SECRETS
"wifi_off_on_exit_key" : "wifi_off_on_exit"
"wifi_throttle_disabled_key" : "wifi_throttle_disabled_key"

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.