

ANDROID STATIC ANALYSIS REPORT



WiFiAnalyzer (3.0.1)

File Name:	installer272.apk
Package Name:	com.vrem.wifianalyzer
Scan Date:	May 31, 2022, 9:40 a.m.
App Security Score:	53/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	≪ HOTSPOT
1	4	1	1	0

FILE INFORMATION

File Name: installer272.apk

Size: 2.3MB

MD5: 31e40bfcb6934cc37ec797aa095c136b

SHA1: 3473e894a49fa9d80ff2dfb05552aeebf40632e5

SHA256: ba056efca559544f39ba72fcdcd0e3b4312557172507886373b04730a2b2263e

i 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: 3.0.1
Android Version Code: 53

EE 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.

M 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

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	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/e/e.java b/f/e/g.java b/f/j/b.java b/n/a/a/h.java b/m/i0.java c/b/a/c.java c/a/a/a/co/g.java b/m/y.java c/a/a/a/m/h.java b/f/h/b.java c/b/a/i.java b/f/e/k.java b/f/l/b0.java b/f/l/co/c.java b/f/l/h.java b/f/l/f.java b/f/l/f.java b/f/l/f.java b/f/l/t.java b/f/e/c.java c/a/a/a/z/d.java b/f/l/b.java b/f/l/b.java b/f/l/b.java b/f/l/b.java b/f/l/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/a/e.ja va com/vrem/wifianalyzer/l/g/k.ja va

■ 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.
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 ['location'].
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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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 encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
10	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.

Q DOMAIN MALWARE CHECK

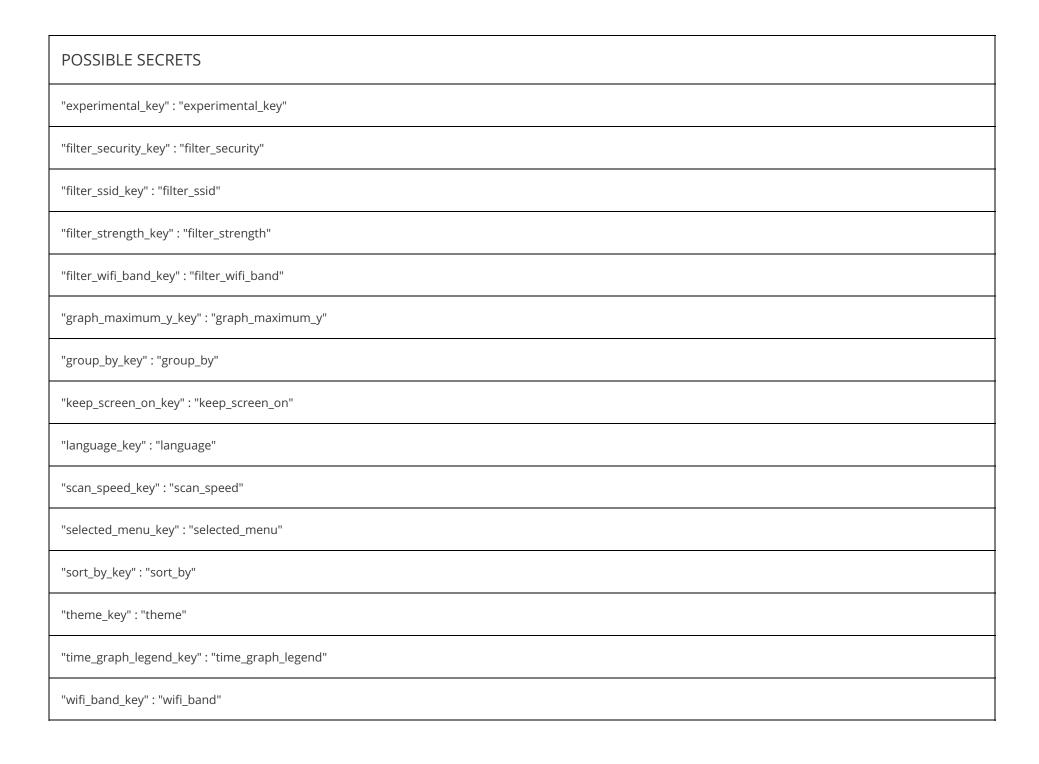
DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	IP: 142.250.179.206 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

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: 185.199.108.153 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.
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

HARDCODED SECRETS

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



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.

© 2022 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.