ANDROID STATIC ANALYSIS REPORT

 WiFiAnalyzer (3.0.2)

File Name:	installer98.apk
Package Name:	com.vrem.wifianalyzer
Scan Date:	May 31, 2022, 9:29 a.m.
App Security Score:	**61/100 (LOW RISK)**
Grade:	**A**

📊 FINDINGS SEVERITY

🐛 HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	🔍 HOTSPOT
0	5	1	1	0

📦 FILE INFORMATION

File Name: installer98.apk
Size: 2.3MB
MD5: 6ceff628605b16e3930a7b7e8aefb05d
SHA1: fe4cf4d1a3a1846b62fa7b53eadc14fac697b656
SHA256: fb66858a2dbf79826e55cca86f72088f06fa330a27560609d177366c98e7450a

ℹ APP INFORMATION

App Name: WiFiAnalyzer
Package Name: com.vrem.wifianalyzer
Main Activity: com.vrem.wifianalyzer.SplashActivity
Target SDK: 30
Min SDK: 19
Max SDK:
Android Version Name: 3.0.2
Android Version Code: 54

■■ 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: True
v3 signature: True
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
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 62051a46a5865879387fc4116bf8d51afbe33d1117c80a4bc8a80c99a51f4c65

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	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

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
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	d/f/d/c/a.java d/f/l/w.java d/f/e/e.java d/f/l/f.java d/f/j/b.java d/f/e/g.java e/b/a/c.java d/f/h/b.java e/b/a/i.java e/a/a/a/z/d.java d/f/e/k.java d/a/o/g.java d/n/a/a/h.java e/a/a/a/p/a.java d/f/l/b0.java d/h/b/c.java d/k/a/b.java d/f/l/h.java d/m/i0.java d/f/d/c/b.java e/a/a/a/c0/g.java d/f/l/u.java e/a/a/a/a0/b.java d/f/l/t.java d/f/e/f.java d/m/y.java d/f/e/c.java e/a/a/a/m/h.java d/f/l/b.java d/f/e/j.java d/f/l/c0/c.java d/f/k/b.java d/f/d/c/f.java d/a/k/a/a.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.java com/vrem/wifianalyzer/l/g/k.java

🪪 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.

⚙ 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

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.