

ANDROID STATIC ANALYSIS REPORT



• Wifi Fixer (1.0.3.5)

File Name:	installer124.apk
Package Name:	org.wahtod.wififixer
Scan Date:	May 31, 2022, 11:51 a.m.
App Security Score:	41/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

兼 HIGH	▲ MEDIUM	i INFO	✓ SECURE	ℚ HOTSPOT
4	10	1	1	1

FILE INFORMATION

File Name: installer124.apk

Size: 0.81MB

MD5: 8486addda85fa0ca3929c8c58b7bde7e

SHA1: 0b85bb5cdc74ce2eba481a0e92eaea3898ce806d

SHA256: c7af357054a9133d62000142185a2f9741e727998b00abf5524f52e02f228556

i APP INFORMATION

App Name: Wifi Fixer

Package Name: org.wahtod.wififixer

Main Activity: org.wahtod.wififixer.ui.MainActivity

Target SDK: 19 Min SDK: 7 Max SDK: 19

Android Version Name: 1.0.3.5 Android Version Code: 1118

B APP COMPONENTS

Activities: 4
Services: 6
Receivers: 6
Providers: 1

Exported Activities: O Exported Services: O Exported Receivers: 5 Exported Providers: O



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: 2011-01-25 09:27:33+00:00 Valid To: 2038-06-12 09:27:33+00:00

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

Serial Number: 0x4d3e9785 Hash Algorithm: sha1

md5: 09001492cef34e3f7d537e1ac514174c

sha1: d2c8ec4010e82ee1d9b45323064c8e16b2fac2cd

sha256: ae9a5dc52e45b8e7196996bb0eb613c9cbaa278d53e7a4c1a1d2b7b88ea6751b

sha512: af 002180147f84 abdc11482 efaee 417c1c1 dec7c3b5517bd1059c4f774204f73 da0f7ea5b411 fecb3ec9f062dc30a22e8d0d38b182c3de39a3498dcb8a3f2d98a2de3b411fecb3ec9f062dc30a22e8d0d38b182c3de39a3498dcb8a3f2d98a2de3b411fecb3ec9f062dc30a22e8d0d38b182c3de39a3498dcb8a3f2d98a2de3b411fecb3ec9f062dc30a22e8d0d38b182c3de39a3498dcb8a3f2d98a2de3b411fecb3ec9f062dc30a22e8d0d38b182c3de39a3498dcb8a3f2d98a2de3b411fecb3ec9f062dc30a22e8d0d38b182c3de39a3498dcb8a3f2d98a2de3b411fecb3ec9f062dc30a22e8d0d38b182c3de39a3498dcb8a3f2d98a2de3b411fecb3ec9f062dc30a22e8d0d38b182c3de39a3498dcb8a3f2d98a2de3b411fecb3ec9f062dc30a22e8d0d38b182c3de39a3498dcb8a3f2d98a2de3b411fecb3ec9f062dc30a22e8d0d38b182c3de39a3498dcb8a3f2d98a2de3b411fecb3ec9f062dc30a22e8d0d38b182c3de39a3498dcb8a3f2d98a2de3b411fecb3ec9f062dc30a22e8d0d38b182c3de39a3498dcb8a3f2d98a2de3b411fecb3ec9f062dc30a22e8d0d38b182c3de3b411fecb3ec9f062dc30a22e8d0d38b182c3de3b411fecb3ec9f062dc30a22e8d0d38b182c3de3b411fecb3ec9f062dc30a22e8d0d38b182c3de3b411fecb3ec9f062dc30a22e8d0d38b182c3de3b411fecb3ec9f062dc30a22e8d0d38b182c3de3b411fecb3ec9f062dc30a22e8d0d38b182c3de3b411fecb3ec9f062dc30a22e8d0d38b182c3de3b411fecb3ec9f062dc30a22e8d0d38b182c3de3b411fecb3ec9f062dc30a22e8d0d38b182c3de3b411fecb3ec9f062dc30a22e8d0d38b182c3de3b411fecb3ec9f062dc30a22e8d0d38b182c3de3b411fecb3ec9f062dc30a22e8d0d38b182c3de3b411fecb3ec9f062dc30a22e8d0d38b182c3de3b411fecb3ec9f062dc30a22e8d0d38b182c3de3b411fecb3ec9f062dc30a22e8d0d38b182c3de4b411fecb3ec9f062dc30a22e8d0d38b182c3de4b411fecb3ec9f062dc30a22e8d0d38b182c3de4b411fecb3ec9f062dc30a22e8d0d38b182c3de4b411fecb3ec9f062dc30a22e8d0d38b182c3de4b411fecb3ec9f062dc30a22e8d0d38b182c3de4b411fecb3ec9f062dc30a22e8d0d38b182c4b411fecb3ec9f062dc30a22e8d0d38b182c4b411fecb3ec9f062dc30a22e8d0d38b182c4b411fecb3ec9f062dc30a22e8d0d38b182c4b411fecb3ec9f062dc30a22e8d0d38b182c4b411fecb3ec9f062dc30a22e8d0d38b182c4b411fecb3ec9f062dc30a26e66d0d26b41166d0d26b41166d0d26b41166d0d26b41166d0d26b41166d0d26b41166d0d26b41166d0d26b4166d0d26b4166d0d26b4166d0d26b4166d0d26b4166d0d26b4166d0d26b4166d0d26b4166d0d26b4

TITLE	SEVERITY	DESCRIPTION	
Signed Application	info	Application is signed with a code signing certificate	

TITLE	SEVERITY	DESCRIPTION		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.			
Certificate algorithm might be vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.			

⋮ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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_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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.

MAPKID ANALYSIS

FILE	DETAILS		
classes.dex	FINDINGS DETAILS		
Classes.uex	Compiler	dx	

△ 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	Launch Mode of Activity (org.wahtod.wififixer.ui.MainActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
3	Broadcast Receiver (org.wahtod.wififixer.boot.BootReceiver) is not Protected. An intent-filter exists. warning		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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
4	Broadcast Receiver (org.wahtod.wififixer.NotificationReceiver) 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.
5	Broadcast Receiver (org.wahtod.wififixer.WFBroadcastReceiver) is not Protected. An intent-filter exists.		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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
6	Broadcast Receiver (org.wahtod.wififixer.widget.FixerWidget) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
7	Broadcast Receiver (org.wahtod.wififixer.widget.FixerWidgetSmall) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Broadcast Receiver 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	com/actionbarsherlock/internal/widget/lcs Toast.java com/actionbarsherlock/internal/widget/Act ionBarView.java com/actionbarsherlock/internal/nineoldan droids/animation/PropertyValuesHolder.ja va org/wahtod/wififixer/utility/r.java com/actionbarsherlock/widget/Suggestions Adapter.java com/actionbarsherlock/view/MenuInflater. java com/actionbarsherlock/internal/ActionBarS herlockCompat.java org/wahtod/wififixer/utility/am.java com/actionbarsherlock/widget/ActivityCho oserModel.java com/actionbarsherlock/internal/view/men u/MenuItemImpl.java com/actionbarsherlock/widget/SearchView .java
2	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	org/wahtod/wififixer/utility/p.java
3	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	org/wahtod/wififixer/a/a.java org/wahtod/wififixer/utility/r.java org/wahtod/wififixer/a/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	org/wahtod/wififixer/utility/m.java
5	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/actionbarsherlock/internal/view/men u/MenuBuilder.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 ['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 user/application initiated 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.baidu.com	ok	IP: 104.193.88.77 Country: United States of America Region: California City: Cupertino Latitude: 37.316605 Longitude: -122.046486 View: Google Map
cyanogenmod.com	ok	IP: 216.168.38.169 Country: United States of America Region: Washington City: Seattle Latitude: 47.620621 Longitude: -122.310959 View: Google Map

DOMAIN	STATUS	GEOLOCATION
wififixer.wordpress.com	ok	IP: 192.0.78.12 Country: United States of America Region: California City: San Francisco Latitude: 37.748425 Longitude: -122.413673 View: Google Map
plus.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
code.google.com	ok	IP: 142.250.179.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 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

Т

DOMAIN	STATUS	GEOLOCATION
www.google.com	ok	IP: 142.250.179.164 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
github.com	ok	IP: 140.82.121.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

EMAILS

EMAIL	FILE
wifi_fixer@gmail.com	Android String Resource



POSSIBLE SECRETS "backup_key": "THISISANEXAMPLEAPIKEYITWILLNOTWORK" "dbmfloor_key": "DBMFLOOR" "dbmfloor_key": "DBMFLOOR"

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.