

ANDROID STATIC ANALYSIS REPORT



WiFiKeyShare (1.2.0)

File Name:	installer208.apk
Package Name:	be.brunoparmentier.wifikeyshare
Scan Date:	May 31, 2022, 3:54 p.m.
App Security Score:	46/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	≪ HOTSPOT
2	6	1	1	0

FILE INFORMATION

File Name: installer208.apk

Size: 1.91MB

MD5: a8de68c2d6c05153132011051db6a441

SHA1: b0091507a293f92bdf0012999ae0aa9b0f64933e

SHA256: daf561050b0c1d84497bbfdd776b2e39073ac91d99fed110b7c0825a1aedb01e

i APP INFORMATION

App Name: WiFiKeyShare

Package Name: be.brunoparmentier.wifikeyshare

 $\textbf{\textit{Main Activity}}: be. brun oparmentier. wifikey share. ui. activities. Wifi List Activity$

Target SDK: 28 Min SDK: 15 Max SDK:

Android Version Name: 1.2.0 Android Version Code: 4

EE APP COMPONENTS

Activities: 6 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: 2016-01-26 13:59:36+00:00 Valid To: 2043-06-13 13:59:36+00:00

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

Serial Number: 0xa9ec115 Hash Algorithm: sha256

md5: 190b0e9a5f1a732634ef57d3efadb7b2

sha1: bc0e82ae4c7dbe1b0c5ba6e220c09ca52e867796

sha256: 78f2e4fcffa7338dad554c73765e6876c5e8b383fd494d4e7d0b96c959fa0bad

sha512: 78a3d1da1b2ae3172d7441eb9968c936243eb8f3b0af06f287cce2eebcae09769d5841d67ed80e8afc4f340d49c6722d3f05fc86487491cfb79ecd8d35ca3c95

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.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.

命 APKID ANALYSIS

FILE	DETAILS
------	---------

FILE	DETAILS		
	FINDINGS	DETAILS	
classes.dex	Compiler	r8 without marker (suspicious)	

△ NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

Q MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Activity (be.brunoparmentier.wifikeyshare.ui.activities.ConfirmConnectToWifiNetworkActivity) 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	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	eu/chainfire/libsuperuser/ShellNotClosedEx ception.java eu/chainfire/libsuperuser/BuildConfig.java eu/chainfire/libsuperuser/Shell.java eu/chainfire/libsuperuser/Application.java eu/chainfire/libsuperuser/R.java eu/chainfire/libsuperuser/ShellOnMainThre adException.java eu/chainfire/libsuperuser/HideOverlaysRec eiver.java eu/chainfire/libsuperuser/Policy.java eu/chainfire/libsuperuser/Debug.java eu/chainfire/libsuperuser/Toolbox.java be/brunoparmentier/wifikeyshare/ui/activiti es/WifiListActivity.java eu/chainfire/libsuperuser/StreamGobbler.ja va
2	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	org/wordpress/passcodelock/AbstractAppL ock.java org/wordpress/passcodelock/BuildConfig.ja va org/wordpress/passcodelock/DefaultAppLo ck.java be/brunoparmentier/wifikeyshare/utils/Nfc Utils.java be/brunoparmentier/wifikeyshare/model/W ifiNetwork.java be/brunoparmentier/wifikeyshare/db/WifiK eysContract.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/brunoparmentier/wifikeyshare/ui/activiti es/WifiNetworkActivity.java be/brunoparmentier/wifikeyshare/utils/Wifi ConfigStoreParser.java be/brunoparmentier/wifikeyshare/utils/Nfc Utils.java eu/chainfire/libsuperuser/Debug.java be/brunoparmentier/wifikeyshare/ui/activiti es/ConfirmConnectToWifiNetworkActivity.ja va org/wordpress/passcodelock/StringUtils.jav a be/brunoparmentier/wifikeyshare/ui/activiti es/WifiListActivity.java
4	Weak Encryption algorithm used	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	org/wordpress/passcodelock/DefaultAppLo ck.java
5	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	org/wordpress/passcodelock/StringUtils.jav a
6	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	be/brunoparmentier/wifikeyshare/db/WifiK eysDbHelper.java

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 ['NFC'].
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.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data 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 not encrypt any data in traffic or does not transmit any data between itself and another trusted IT product.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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
xmlpull.org	ok	IP: 74.50.61.58 Country: United States of America Region: Texas City: Dallas Latitude: 32.814899 Longitude: -96.879204 View: Google Map

DOMAIN	STATUS	GEOLOCATION
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
wifikeysha.re	ok	IP: 185.199.111.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map
github.com	ok	IP: 140.82.121.4 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

HARDCODED SECRETS

POSSIBLE SECRETS	POS:	SIBLE	SECF	RETS
------------------	------	-------	------	------

"password": "Password"

POSSIBLE SECRETS
"pref_key_passcode_toggle" : "turn_passcode_on_off"
"wifi_dialog_view_password" : ""
"wifilist_dialog_view_password" : ""
"password" : "Passwort"
"wifi_dialog_view_password" : ""
"wifilist_dialog_view_password" : ""

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.