MOBSF

ANDROID STATIC ANALYSIS REPORT

WiFiKeyShare (1.1.1)

File Name:	installer279.apk
Package Name:	be.brunoparmentier.wifikeyshare
Scan Date:	May 31, 2022, 10:54 a.m.
App Security Score:	46/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	6	1	1	0

FILE INFORMATION

File Name: installer279.apk
Size: 1.78MB
MD5: 6fbfe4ce2cec8423942b98f1cf4e3373
SHA1: 7622464decc11e2cb54d5a2e42885b24e6c5c5b2
SHA256: 9af11713ab2f369d48914919bf7bae3ee6830f2d55b659985b37ad5a8d3f2331

APP INFORMATION

App Name: WiFiKeyShare
Package Name: be.brunoparmentier.wifikeyshare
Main Activity: be.brunoparmentier.wifikeyshare.ui.activities.WifiListActivity
Target SDK: 23
Min SDK: 15
Max SDK:
Android Version Name: 1.1.1
Android Version Code: 3

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.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dx (possible dexmerge)</td></tr><tr><td>Manipulator Found</td><td>dexmerge</td></tr></table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

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/Toolbox.java eu/chainfire/libsuperuser/StreamGobbler.java eu/chainfire/libsuperuser/ShellNotClosedException.java eu/chainfire/libsuperuser/BuildConfig.java eu/chainfire/libsuperuser/Shell.java be/brunoparmentier/wifikeyshare/ui/activities/WifiListActivity.java eu/chainfire/libsuperuser/Application.java eu/chainfire/libsuperuser/ShellOnMainThreadException.java eu/chainfire/libsuperuser/HideOverlaysReceiver.java eu/chainfire/libsuperuser/Policy.java eu/chainfire/libsuperuser/Debug.java
2	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/DefaultAppLock.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/DefaultAppLock.java be/brunoparmentier/wifikeyshare/utils/NfcUtils.java be/brunoparmentier/wifikeyshare/model/WifiNetwork.java org/wordpress/passcodelock/AbstractAppLock.java be/brunoparmentier/wifikeyshare/db/WifiKeysContract.java org/wordpress/passcodelock/BuildConfig.java
4	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/utils/NfcUtils.java org/wordpress/passcodelock/StringUtils.java be/brunoparmentier/wifikeyshare/ui/activities/ConfirmConnectToWifiNetworkActivity.java be/brunoparmentier/wifikeyshare/ui/activities/WifiListActivity.java eu/chainfire/libsuperuser/Debug.java be/brunoparmentier/wifikeyshare/ui/activities/WifiNetworkActivity.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.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/WifiKeysDbHelper.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 ['NFC'].
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 implement functionality to encrypt sensitive data 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.
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
wifikeysha.re	ok	**IP:** 185.199.109.153 **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

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.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

🔑 HARDCODED SECRETS

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

POSSIBLE SECRETS
"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.