MOBSF

ANDROID STATIC ANALYSIS REPORT

WiFi Walkie Talkie (1.10)

File Name:	installer214.apk
Package Name:	org.jsl.wfwt
Scan Date:	May 31, 2022, 7:47 a.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	3	1	1	1

FILE INFORMATION

File Name: installer214.apk
Size: 0.12MB
MD5: 487f267ae7a9b91483a04a0653f570bf
SHA1: c1c76ec42d6bc92004c97d13958d338b943b0c7b
SHA256: 1f6b91f14739eb734204010c8cb754754a626c483164eb077c536d4cb8832701

APP INFORMATION

App Name: WiFi Walkie Talkie
Package Name: org.jsl.wfwt
Main Activity: org.jsl.wfwt.MainActivity
Target SDK: 16
Min SDK: 16
Max SDK:
Android Version Name: 1.10
Android Version Code: 11

APP COMPONENTS

Activities: 1
Services: 1
Receivers: 0
Providers: 0
Exported Activities: 0
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: 2015-12-31 12:50:07+00:00
Valid To: 2043-05-18 12:50:07+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x1a9b398c
Hash Algorithm: sha256
md5: cd8aafa40a1ac3bee1379028aeab258e
sha1: 9866b378aa7622fa94cdaab10cd835060aff3eb7
sha256: 8bd9ded0fbc77f3a7975d75c7b35c4276a84f1d566e084eb61a873ea8fb6c495
sha512: a9bb7e3ddb81d6e5629618fd1141f9111b80aff8ae5d65259b0ebfbf419201649f26a1aa8869746940df0113eae0d7cebd1381d55e2f7460e8c1ca8eb952d422

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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Compiler — DETAILS: dx (possible dexmerge) FINDINGS: Manipulator Found — DETAILS: dexmerge

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.

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	org/jsl/wfwt/AudioRecorder.java org/jsl/wfwt/SwitchButton.java org/jsl/wfwt/ChannelSession.java org/jsl/wfwt/HandshakeClientSession.java org/jsl/wfwt/Channel.java org/jsl/wfwt/MainActivity.java org/jsl/wfwt/HandshakeServerSession.java org/jsl/wfwt/WalkieService.java org/jsl/wfwt/AudioPlayer.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	org/jsl/wfwt/WalkieService.java
3	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	org/jsl/collider/ShMemClient.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 ['network connectivity', 'microphone'].
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 user/application initiated 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 not encrypt any data in traffic or does not transmit any data between itself and another trusted IT product.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
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

---

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.