



ANDROID STATIC ANALYSIS REPORT



 WIFI_EAP_SIM_Conf (1.0)

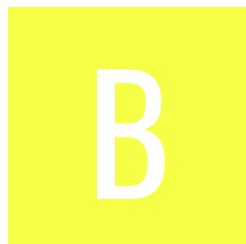
File Name: installer84.apk

Package Name: net.loeuillet.wifi_eap_sim_conf






Scan Date: May 31, 2022, 11:51 a.m.

App Security Score: 56/100 (MEDIUM RISK)

Grade:



FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
1	1	0	1	1

FILE INFORMATION

File Name: installer84.apk

Size: 0.05MB

MD5: 64da82927e21c66f06623c75682b0b84

SHA1: 0afaa529fdb30c22e5e6d03d0699f48c4cb61bbc

SHA256: 971113d6d36ba6c78ebd79afb86d975caa3a76350a7a847926ad8cef43bb078d

APP INFORMATION

App Name: WIFI_EAP_SIM_Conf

Package Name: net.loeuillet.wifi_eap_sim_conf

Main Activity: net.loeuillet.wifi_eap_sim_conf.MyActivity

Target SDK: 21

Min SDK: 21

Max SDK:

Android Version Name: 1.0

Android Version Code: 1

APP COMPONENTS

Activities: 1

Services: 0

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: 2015-11-24 20:41:23+00:00

Valid To: 2043-04-11 20:41:23+00:00

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

Serial Number: 0x279d4da3

Hash Algorithm: sha256

md5: 346ea3e946de948e58bb23f4ac588094

sha1: 8f54faf3ff34dd11558a96fe6bf95712a416cbc8

sha256: 52d50a343a3e5f72d24c91883103c4b8977fa99f6ea6ca805986f90a84692b0f

sha512: 99711a1cef62c8505e91311e3689a8d0297aecaa0bdc759660b835c0a83d021965f234bed80867ce2f4600ebe9501a1ee6b0b8c8cd8686dec2e03cd92749802f

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.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
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
	Compiler	dx

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.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
----	-------	----------	-----------	-------

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 no hardware resources.
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 does not encrypt files in non-volatile memory.
7	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.

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.