MOBSF

ANDROID STATIC ANALYSIS REPORT

WiFi Warning (1.5.3)

File Name:	installer365.apk
Package Name:	nu.firetech.android.wifiwarning
Scan Date:	May 30, 2022, 4:23 p.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	3	1	1	0

FILE INFORMATION

File Name: installer365.apk
Size: 0.06MB
MD5: 85b59c8198cc0d373da8031be2f2d498
SHA1: 240bf62242496978b46b7d173bed0f40f8f08bbb
SHA256: 07f9f6bd2dc5946bf1330c14ac4bb0a7e6bfda8ed4177c6239921eca776014a3

APP INFORMATION

App Name: WiFi Warning
Package Name: nu.firetech.android.wifiwarning
Main Activity: .ConfigActivity
Target SDK: 19
Min SDK: 9
Max SDK:
Android Version Name: 1.5.3
Android Version Code: 6

APP COMPONENTS

Activities: 2
Services: 0
Receivers: 2
Providers: 0
Exported Activities: 0
Exported Services: 0
Exported Receivers: 1
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: 2014-11-24 07:04:23+00:00
Valid To: 2042-04-11 07:04:23+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x1798a307
Hash Algorithm: sha256
md5: 414b8cbfebba20d6f3b2caf466441fa5
sha1: e656d13c2b1e797ee57b08be235500530d94a82c
sha256: 8a0e76a3f14931fecd296379c329d3d329d660ec807669e346cb1ca233c66d56
sha512: cb451596579b0879b0b6fbf9e34ab3470d961f600ebd7100142bec9b826bf8e319097d3fa17957b0e3e19ffb99213dedad843ea9092641c6b22a9d3120dab0ed

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.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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dx</td></tr></table>

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.
2	Broadcast Receiver (.StatusListener) 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	nu/firetech/android/wifiwarning/StatusListener.java nu/firetech/android/wifiwarning/ConfigActivity.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 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.

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.

HARDCODED SECRETS

POSSIBLE SECRETS
"key_action" : "intentAction"
"key_clearable" : "ongoing"
"key_notify_sound" : "sound"
"key_notify_vibrate" : "vibrate"
"key_notify_light" : "light"

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.