

## ANDROID STATIC ANALYSIS REPORT



WebRadio (1.3)

File Name:	installer298.apk
Package Name:	starcom.snd
Scan Date:	May 31, 2022, 9:10 a.m.
App Security Score:	56/100 (MEDIUM RISK)
Grade:	

### **FINDINGS SEVERITY**

<del>派</del> HIGH	▲ MEDIUM	i INFO	✓ SECURE	ℚ HOTSPOT
1	1	0	1	1

#### FILE INFORMATION

File Name: installer298.apk

Size: 0.16MB

MD5: 1f3d5213114ca9ae07413a5b920562e4

**SHA1**: 4e55f96d0ac496af2c75a8e4193eed1061557f3b

SHA256: 2a5930c0171d10ba9a68bd4fc1d618025cb63755f95fc77536e4e2dfe5260715

## **i** APP INFORMATION

App Name: WebRadio

Package Name: starcom.snd

Main Activity: starcom.snd.WebRadio

Target SDK: 27 Min SDK: 19 Max SDK:

Android Version Name: 1.3 Android Version Code: 3

#### **APP COMPONENTS**

Activities: 1 Services: 0 Receivers: 0 Providers: 0

Exported Activities: O Exported Services: O Exported Receivers: O Exported Providers: O



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 16:42:31+00:00 Valid To: 2043-06-13 16:42:31+00:00

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

Serial Number: 0x2f3e9784 Hash Algorithm: sha256

md5: ad35fb48978503913ca1a255ec0b8de8

sha1: b010334d4bfd3c4712e83933e4bfcf4251aa1d8c

sha256: 99fa50edab51c312dcc438b207e9826ca6145410961167a22674dd4ca5b8a122

sha512: 7959bd0b5634fe3b49258594da7a2b24d041ca67937fe48384f8898ed5de5218acf8707bf1296cd1b2bbf1b9447f6fe2adcf6831309453563a60c033e6a0c4f8

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.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.

# **M** APKID ANALYSIS

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
Classes.acx	Compiler	dx

## **△** NETWORK SECURITY

|--|

## **Q** MANIFEST ANALYSIS

Ν	10	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	
--	----------	----------	-----------	-------	--

# ■ 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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 user/application initiated 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	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.

#### 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.