



ANDROID STATIC ANALYSIS REPORT



 adbWireless (1.5.4)

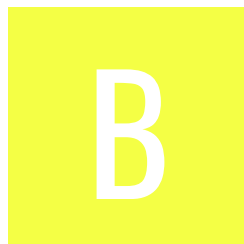
File Name: installer120.apk

Package Name: siir.es.adbWireless






Scan Date: May 31, 2022, 1:04 p.m.

App Security Score: 45/100 (MEDIUM RISK)

Grade:



FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
2	4	1	1	0

FILE INFORMATION

File Name: installer120.apk

Size: 0.37MB

MD5: ef29c2e880b9df98cf42b10292850385

SHA1: 881d0abfafc7042f714b2b6252663802e81c74b0

SHA256: c42a48cd12fb453105c93e2af25ed4d5ac181e74fcf6f2a21c063e4ec210923c

APP INFORMATION

App Name: adbWireless

Package Name: siir.es.adbWireless

Main Activity: .adbWireless

Target SDK: 17

Min SDK: 4

Max SDK:

Android Version Name: 1.5.4

Android Version Code: 12

APP COMPONENTS

Activities: 2

Services: 0

Receivers: 2

Providers: 0

Exported Activities: 0

Exported Services: 0

Exported Receivers: 2

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: 2013-03-12 09:19:39+00:00

Valid To: 2040-07-28 09:19:39+00:00

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

Serial Number: 0x513ef32b

Hash Algorithm: sha1

md5: df69de352889c34817be5b85aae1bf7c

sha1: 1c5d3902857d02ad41e1cbe3c05f7057e11e8f54

sha256: cc2db16d8e16a2e34052dc39dc41cac5cdd2bb92dd87dd1ec406651a15087971

sha512: 6ecd49f06631d0f0cd63673aa27e1ff287af7aa8894d95842c4bd34dad63a2c4cec57df409089ef5ab9c0f06fd706e7c7938eceb212e1ff01d540bf48a158399

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.
Certificate algorithm might be vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

≡ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.



APKID ANALYSIS

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



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 (.TrackShutdown) 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.
3	Broadcast Receiver (.adbWidgetProvider) 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	siir/es/adbWireless/Debug.java

👤 NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

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 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.

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

EMAILS

EMAIL	FILE
mrsiir@gmail.com	Android String Resource

HARDCODED SECRETS

POSSIBLE SECRETS
"pref_vibrate_key" : "key_vibrate"
"pref_sound_key" : "key_sound"
"pref_noti_key" : "key_noti"
"pref_haptic_key" : "key_haptic"

POSSIBLE SECRETS
"pref_wifi_on_key" : "key_wifi_on"
"pref_wifi_off_key" : "key_wifi_off"
"pref_onboot_key" : "key_onboot"
"pref_autocon_key" : "key_autocon"
"pref_autoconip_key" : "key_autoconip"
"pref_autoconport_key" : "key_autoconport"
"pref_screenon_key" : "key_screenon"
"pref_vibrate_key" : "key_vibrate"
"pref_sound_key" : "key_sound"
"pref_noti_key" : "key_noti"
"pref_haptic_key" : "key_haptic"
"pref_wifi_on_key" : "key_wifi_on"
"pref_wifi_off_key" : "key_wifi_off"
"pref_autocon_key" : "key_autocon"
"pref_autoconip_key" : "key_autoconip"

POSSIBLE SECRETS
"pref_autoconport_key" : "key_autoconport"
"pref_screenon_key" : "key_screenon"

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](#).