

ANDROID STATIC ANALYSIS REPORT



HeaterRC (1.3)

File Name:	installer221.apk
Package Name:	com.dynamite.heaterrc
Scan Date:	May 31, 2022, 4:27 p.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	≪ HOTSPOT
1	9	1	1	1

FILE INFORMATION

File Name: installer221.apk

Size: 0.11MB

MD5: 5743aaa63e74cbf81a2adc4766536b6e

SHA1: 67deea718dca66ee8d895e97cf86f4162f1e94a7

SHA256: dd5c1d4ad1e04801928152c24df4b8265199f1f0ea5cab67642ee5b876387bef

i APP INFORMATION

App Name: HeaterRC

Package Name: com.dynamite.heaterrc

Main Activity: .SHtabWidget

Target SDK: 8 Min SDK: 8 Max SDK:

Android Version Name: 1.3
Android Version Code: 13

B APP COMPONENTS

Activities: 7 Services: 0 Receivers: 3 Providers: 0

Exported Activities: 6 Exported Services: 0 Exported Receivers: 2 Exported Providers: 0



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: 2015-07-25 19:24:29+00:00 Valid To: 2042-12-10 19:24:29+00:00

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

Serial Number: 0x717b46d1 Hash Algorithm: sha256

md5: 0e61f1cfe4f76aaef75a2b17402db4a3

sha1: 0c3c5e323a1daaed229bccd7d6a0770afdd93fb4

sha256: 3188902a6ce1598d0829b2359ee52300895a35563b31a971480c7b6a7622bd33

sha512: c4aa82abd735e63c932132dcff6e6a0a467308d3c9c5f32776d7fc1aae37b6e37a91af01a39151a1fb85a6f54f8f2569e43fdb1f7a62992961d2fb8debe2c648

TITLE SEVERITY DESCRIPTION		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.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
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.

命 APKID ANALYSIS

FILE	DETAILS

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

△ NETWORK SECURITY

		NO	SCOPE	SEVERITY	DESCRIPTION
--	--	----	-------	----------	-------------

Q 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.

NO	ISSUE	SEVERITY	DESCRIPTION	
2	Broadcast Receiver (.SMSreceiver) 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 (.BootReceiver) 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.	
4	Activity (.StandHeizungActivity) is not Protected. An intent-filter exists.	warning	An Activity 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 Activity is explicitly exported.	
5	Activity (.ConfigActivity) is not Protected. An intent-filter exists.	warning	An Activity 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 Activity is explicitly exported.	
6	Activity (.ProgramActivity) is not Protected. An intent-filter exists.	warning	An Activity 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 Activity is explicitly exported.	
7	Activity (.GPStrackerActivity) is not Protected. An intent-filter exists.	warning	An Activity 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 Activity is explicitly exported.	
8	Activity (.DisplayNotifications) is not Protected. An intent-filter exists.	warning	An Activity 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 Activity is explicitly exported.	

NO	ISSUE	SEVERITY	DESCRIPTION
9	Activity (.AlarmDetails) is not Protected. An intent-filter exists.	warning	An Activity 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 Activity 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	com/dynamite/heaterrc/BootReceiver .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 no hardware resources.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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	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.