

ANDROID STATIC ANALYSIS REPORT



\Pi Botifier (1.4.1)

File Name:	installer97.apk
Package Name:	com.github.grimpy.botifier
Scan Date:	May 31, 2022, 2:07 p.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	≪ HOTSPOT
1	6	1	1	1

FILE INFORMATION

File Name: installer97.apk

Size: 0.29MB

MD5: b84a778152d511d56a5dfae0541299f4

SHA1: b7e1d23d05491ae8dae053a6b466b77ce6c31a6e

SHA256: fbc537c6bbb88b414cc4b337646e2c6ed5f517d55c0b893e6d9e2a13713d87c7

i APP INFORMATION

App Name: Botifier

Package Name: com.github.grimpy.botifier

Main Activity: com.github.grimpy.botifier.MainActivity

Target SDK: 23 Min SDK: 14 Max SDK:

Android Version Name: 1.4.1 Android Version Code: 16

EE APP COMPONENTS

Activities: 1 Services: 5 Receivers: 3 Providers: 0

Exported Activities: 0 Exported Services: 2 Exported Receivers: 3 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: 2013-12-11 00:12:55+00:00 Valid To: 2041-04-28 00:12:55+00:00

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

Serial Number: 0x5ba565e3 Hash Algorithm: sha256

md5: 982fd79bf50f0681f23975d99579547b

sha1: d9ba1e96f74c772cd668eeb43d7fde30c87539eb

sha256: 704749482ab892162def98ed7e7b1fbce6fe87852fa3bd1aa708b7317ef8d0e6

sha512: 2a1a337c823f824596cc8da47ca6e4efc6bf66efdcd913b3a436ccfe9d2abf396c124a714a0d9ccc4e66158aef7fef8001411d91bec9b2aec947e538cb5dc1f3

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.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.
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.
com.sonyericsson.extras.liveware.aef.EXTENSION_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

ক্ল APKID ANALYSIS

FILE	DETAILS
------	---------

FILE	DETAILS		
	FINDINGS	DETAILS	
classes.dex	Compiler	dx (possible dexmerge)	
	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	Service (com.github.grimpy.botifier.receivers.BotifierNotificationService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NOTIFICATION_LISTENER_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
3	Service (com.github.grimpy.botifier.receivers.BotifierAccessibilityService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_ACCESSIBILITY_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
4	Broadcast Receiver (com.github.grimpy.botifier.plugins.liveware.SWExtensionReceiver) 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.
5	Broadcast Receiver (com.github.grimpy.botifier.receivers.NotificationReceiver) 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.
6	Broadcast Receiver (com.github.grimpy.botifier.plugins.avrcp.MediaButtonIntentReceiver) 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	com/github/grimpy/botifier/plugins/avrcp/AvrcpSe rvice.java com/github/grimpy/botifier/receivers/BotifierNotifi cationService.java com/github/grimpy/botifier/plugins/avrcp/MediaB uttonIntentReceiver.java com/github/grimpy/botifier/plugins/PluginPreferen ce.java com/github/grimpy/botifier/Botification.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.
4	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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 | <u>Ajin Abraham</u> | <u>OpenSecurity.</u>