

#### ANDROID STATIC ANALYSIS REPORT



• Freebloks (1.3.0)

installer205.apk
de.saschahlusiak.freebloks
May 31, 2022, 5:41 a.m.
64/100 (LOW RISK)
A

#### FINDINGS SEVERITY

<b>☆</b> HIGH	▲ MEDIUM	<b>i</b> INFO	✓ SECURE	<b>ℚ</b> HOTSPOT
0	4	1	1	0

#### FILE INFORMATION

File Name: installer205.apk

Size: 5.84MB

MD5: 8c420353f353ef9ba3ba4b54c7f86288

SHA1: 43d67a6d51f8ffa06f0947afbb3abc149d856617

SHA256: ce42ee79a5fa39adfb501f0ed89ae621b413e91ab31eedb19b4951426a017d66

#### **i** APP INFORMATION

App Name: Freebloks

Package Name: de.saschahlusiak.freebloks

Main Activity: de.saschahlusiak.freebloks.game.FreebloksActivity

Target SDK: 30 Min SDK: 21 Max SDK:

Android Version Name: 1.3.0
Android Version Code: 110

#### **B** APP COMPONENTS

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

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

#### **\*** CERTIFICATE INFORMATION

APK is signed v1 signature: True v2 signature: True v3 signature: True

Found 1 unique certificates

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

Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2016-06-18 08:11:03+00:00 Valid To: 2043-11-04 08:11:03+00:00

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

Serial Number: 0x4f81de6 Hash Algorithm: sha256

md5: 2cb6d515dc157a743d99829eae0f76aa

sha1: 275e6ae63109add001bb38a138d1567e22f399d6

sha256: b84ad1afd452a019934fbe6a6b8417d8a278373917b738a6776f4db30214d470

sha512: 1d3615fa5c566aea50e9cd9860556b63b733bb95e66bd557dff397598fc93703f76f5d0a44bd6eec226772272eb715f5af649a7bf165fd6ebc98f427eb0abb1a

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 05671f013f80203384b4e3147548b04c5c1c85c0a216b9f33235046a8f523936

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.

#### **M** APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS					
classes.dex	FINDINGS	DETAILS				
	Anti-VM Code	Build.MANUFACTURER check possible VM check				
	Compiler	r8				

#### **△** 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	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	de/saschahlusiak/freebloks/view/GLConfigC hooser.java de/saschahlusiak/freebloks/view/Freebloks Renderer.java de/saschahlusiak/freebloks/network/Messa geReadThread.java de/saschahlusiak/freebloks/game/Freebloks ActivityViewModel\$connectToBluetooth\$1.j ava de/saschahlusiak/freebloks/game/Freebloks ActivityViewModel.java de/saschahlusiak/freebloks/client/JNIServer. java de/saschahlusiak/freebloks/client/GameClie ntMessageHandler.java de/saschahlusiak/freebloks/network/messa ge/MessageChat\$Companion\$from\$1.java de/saschahlusiak/freebloks/game/dialogs/MultiplayerFragment.java de/saschahlusiak/freebloks/game/Freebloks Activity.java de/saschahlusiak/freebloks/game/Freebloks Activity.java de/saschahlusiak/freebloks/network/Messa geWriter.java de/saschahlusiak/freebloks/network/Messa geWriter.java de/saschahlusiak/freebloks/network/Messa ge.java de/saschahlusiak/freebloks/network/Messa ge.java de/saschahlusiak/freebloks/view/AnimateTh read.java de/saschahlusiak/freebloks/network/blueto oth/BluetoothServerThread.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	de/saschahlusiak/freebloks/database/HighS coreDB.java de/saschahlusiak/freebloks/database/Freebl oksDBOpenHandler.java

#### SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
----	---------------	----	-----------------	-------	-------	---------	---------	---------------------

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/armeabi-v7a/libktx.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/armeabi-v7a/libserver.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['FD_ISSET_chk', 'FD_SET_chk', 'strcpy_chk', 'vsprintf_chk', 'strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/x86/libktx.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	lib/x86/libserver.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['strlen_chk', 'FD_ISSET_chk', 'FD_SET_chk', 'strcpy_chk', 'vsprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	lib/arm64-v8a/libktx.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	lib/arm64-v8a/libserver.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['FD_ISSET_chk', 'strlen_chk', 'FD_SET_chk', 'vsprintf_chk', 'strcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	lib/x86_64/libktx.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	lib/x86_64/libserver.so	True info The shared object has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	True info The shared object has the following fortified functions: ['strlen_chk', 'FD_ISSET_chk', 'FD_SET_chk', 'strcpy_chk', 'vsprintf_chk']	True info Symbols are stripped.

# ■ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application use no DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity', 'bluetooth'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files in non-volatile memory.
8	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.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

### **Q DOMAIN MALWARE CHECK**

DOMAIN	STATUS	GEOLOCATION
www.youtube.com	ok	IP: 142.251.36.46 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
play.google.com	ok	IP: 142.251.36.46 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
paypal.me	ok	IP: 64.4.250.36 Country: United States of America Region: Washington City: Seattle Latitude: 47.606209 Longitude: -122.332069 View: Google Map
f-droid.org	ok	IP: 149.202.95.241 Country: France Region: Hauts-de-France City: Roubaix Latitude: 50.694210 Longitude: 3.174560 View: Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	IP: 140.82.121.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
www.blockchain.com	ok	IP: 104.16.40.77 Country: United States of America Region: Texas City: Dallas Latitude: 32.783058 Longitude: -96.806671 View: Google Map

#### **▶** HARDCODED SECRETS

# POSSIBLE SECRETS "donation\_bitcoin" : "Bitcoin" "donation\_bitcoin" : "Bitcoin"

#### 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.