ANDROID STATIC ANALYSIS REPORT

Rumble (1.0.2)

File Name:	installer64.apk
Package Name:	org.disrupted.rumble
Scan Date:	May 31, 2022, 8:59 a.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	13	1	2	2

FILE INFORMATION

File Name: installer64.apk
Size: 2.74MB
MD5: 0e72ffcb0a4d928de57cdd2b3e4cf5a3
SHA1: 24d40d9bc469e561e1f91ea5ad553ff6243a978b
SHA256: 5f317ef2b3eb534294e154371b0c755a5bbc33f092b4d688176ff0285fb4afa9

APP INFORMATION

App Name: Rumble
Package Name: org.disrupted.rumble
Main Activity: org.disrupted.rumble.userinterface.activity.RoutingActivity
Target SDK: 24
Min SDK: 16
Max SDK:
Android Version Name: 1.0.2
Android Version Code: 15

APP COMPONENTS

Activities: 23
Services: 1
Receivers: 1
Providers: 0
Exported Activities: 3
Exported Services: 0
Exported Receivers: 1
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: 2015-12-12 08:19:29+00:00
Valid To: 2043-04-29 08:19:29+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x5375a9c7
Hash Algorithm: sha256
md5: f5ebf80a17ceb6d8da409014f700fd5d
sha1: 10653479a124fc2b6091f96c2570c2f2fc829505
sha256: f1bb37e9ce65e9948e593ba580d3b96f683f0194575aa708795522c4d2530b19
sha512: 913fa1c830eac2442c68e3a5194a545c87201342dfdf1e99651d8b138b368678b79c2c0b54018100bb175f84ca99d38c725631369c2ee21292bcf170657ac274
```

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.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
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.CHANGE_WIFI_MULTICAST_STATE	normal	allow Wi-Fi Multicast reception	Allows an application to receive packets not directly addressed to your device. This can be useful when discovering services offered nearby. It uses more power than the non-multicast mode.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.PRODUCT check</td></tr>
<tr><td>Compiler</td><td>dx (possible dexmerge)</td></tr>
<tr><td>Manipulator Found</td><td>dexmerge</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION

NO	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.
2	Activity (org.disrupted.rumble.userinterface.activity.DisplayQRCode) 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.
3	Activity (org.disrupted.rumble.userinterface.activity.DisplayImage) 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.
4	Activity (org.disrupted.rumble.userinterface.activity.DisplayStatusActivity) 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	Broadcast Receiver (org.disrupted.rumble.app.StartOnBoot) 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
				org/disrupted/rumble/network/protocols/rumble/workers/RumbleOverUDPMulticast.jav

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a org/disrupted/rumble/network/protocols/firechat/workers/FirechatBTServer.java info/vividcode/android/zxing/camera/CameraManager.java info/vividcode/android/zxing/DecodeThread.java org/disrupted/rumble/network/protocols/rumble/workers/RumbleUDPMulticastScanner.java org/disrupted/rumble/network/linklayer/wifi/WifiLinkLayerAdapter.java de/greenrobot/event/util/AsyncExecutor.java org/disrupted/rumble/userinterface/adapter/ChatMessageRecyclerAdapter.java org/disrupted/rumble/network/WorkerPool.java org/disrupted/rumble/util/Log.java de/greenrobot/event/EventBus.java org/disrupted/rumble/network/linklayer/bluetooth/BluetoothServer.java com/github/amlcurran/showcaseview/targets/ActionBarViewWrapper.java org/disrupted/rumble/userinterface/activity/DisplayStatusActivity.java de/greenrobot/event/util/ErrorDialogManager.java de/greenrobot/event/util/ExceptionToResourceMapping.java org/disrupted/rumble/network/linklayer/bluetooth/BluetoothScanner.java org/disrupted/rumble/network/services/chat/ChatService.java org/disrupted/rumble/network/protocols/firechat/workers/FirechatOverUDPMulticast.java org/disrupted/rumble/network/linklayer/wifi/TCP/TCPServer.java com/github/amlcurran/showcaseview/ShowcaseAreaCalculator.java info/vividcode/android/zxing/CaptureActivit

NO	ISSUE	SEVERITY	STANDARDS	FILES
				yHandler.java org/disrupted/rumble/network/linklayer/wifi/WifiScanner.java
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	org/disrupted/rumble/database/PushStatusDatabase.java org/disrupted/rumble/userinterface/activity/PopupInputGroupKey.java de/greenrobot/event/SubscriberMethodFinder.java org/disrupted/rumble/database/statistics/StatisticManager.java org/disrupted/rumble/userinterface/adapter/StatusRecyclerAdapter.java org/disrupted/rumble/network/NetworkCoordinator.java org/disrupted/rumble/network/services/push/PushService.java com/jeremyfeinstein/slidingmenu/lib/SlidingMenu.java org/disrupted/rumble/network/protocols/rumble/workers/RumbleTCPServer.java info/vividcode/android/zxing/camera/CameraConfigurationManager.java org/disrupted/rumble/network/linklayer/wifi/UDP/UDPMulticastConnection.java info/vividcode/android/zxing/camera/open/OpenCameraInterface.java org/disrupted/rumble/app/EventLogger.java org/disrupted/rumble/network/protocols/rumble/RumbleStateMachine.java de/greenrobot/event/util/ErrorDialogConfig.java org/disrupted/rumble/network/linklayer/wifi/WifiUtil.java org/disrupted/rumble/network/services/push/ReplicationDensityWatcher.java org/disrupted/rumble/userinterface/activity/PopupCreateGroup.java org/disrupted/rumble/database/CacheManager.java org/disrupted/rumble/network/linklayer/blu

NO	ISSUE	SEVERITY	STANDARDS	FILES
				etooth/BluetoothLinkLayerAdapter.java org/disrupted/rumble/network/linklayer/bluetooth/BluetoothConnection.java org/disrupted/rumble/userinterface/fragments/FragmentChatMessageList.java org/disrupted/rumble/util/NetUtil.java org/disrupted/rumble/network/protocols/firechat/FirechatBTState.java org/disrupted/rumble/network/protocols/rumble/workers/RumbleUnicastChannel.java org/disrupted/rumble/userinterface/activity/GroupListActivity.java org/disrupted/rumble/database/ContactDatabase.java org/disrupted/rumble/network/protocols/firechat/FirechatProtocol.java info/vividcode/android/zxing/DecodeHandler.java de/greenrobot/event/BackgroundPoster.java org/disrupted/rumble/database/DatabaseExecutor.java info/vividcode/android/zxing/DecodeHintManager.java org/disrupted/rumble/userinterface/activity/PopupComposeStatus.java org/disrupted/rumble/userinterface/fragments/FragmentNetworkDrawer.java info/vividcode/android/zxing/camera/PreviewCallback.java org/disrupted/rumble/network/protocols/rumble/RumbleProtocol.java org/disrupted/rumble/network/protocols/firechat/workers/FirechatOverBluetooth.java info/vividcode/android/zxing/camera/AutoFocusManager.java info/vividcode/android/zxing/CaptureActivity.java com/jeremyfeinstein/slidingmenu/lib/CustomViewBehind.java org/disrupted/rumble/network/linklayer/bluetooth/BluetoothUtil.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/disrupted/rumble/network/protocols/rumble/workers/RumbleBTServer.java
2	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/amulyakhare/textdrawable/util/ColorGenerator.java org/disrupted/rumble/network/services/push/PushService.java org/disrupted/rumble/util/HashUtil.java org/disrupted/rumble/network/linklayer/bluetooth/BluetoothClientConnection.java org/disrupted/rumble/network/protocols/firechat/FirechatMessageParser.java
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	org/disrupted/rumble/network/protocols/rumble/workers/RumbleUDPMulticastScanner.java org/disrupted/rumble/network/linklayer/wifi/UDP/UDPMulticastNeighbour.java org/disrupted/rumble/network/protocols/firechat/workers/FirechatOverUDPMulticast.java org/disrupted/rumble/network/linklayer/wifi/WifiNeighbour.java org/disrupted/rumble/network/protocols/firechat/FirechatProtocol.java
4	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	org/disrupted/rumble/database/DatabaseFactory.java org/disrupted/rumble/database/PushStatusDatabase.java org/disrupted/rumble/database/ContactDatabase.java org/disrupted/rumble/database/ChatMessageDatabase.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	org/disrupted/rumble/database/GroupDatabase.java org/disrupted/rumble/database/ContactDatabase.java org/disrupted/rumble/database/statistics/StatMessageDatabase.java
6	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	org/disrupted/rumble/util/CryptoUtil.java
7	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	org/disrupted/rumble/util/FileUtil.java
8	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	org/disrupted/rumble/network/protocols/rumble/packetformat/BlockFile.java org/disrupted/rumble/userinterface/activity/PopupComposeStatus.java org/disrupted/rumble/network/protocols/firechat/workers/FirechatOverBluetooth.java
9	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	org/disrupted/rumble/database/statistics/StatisticManager.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided 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', 'camera'].
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 implement functionality to encrypt sensitive data 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1/SHA-256/SHA-384/SHA-512 and message digest sizes 160/256/384/512 bits.
12	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
13	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
marlinski.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
data.disruptedsystems.org	ok	No Geolocation information available.
disruptedsystems.org	ok	No Geolocation information available.

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"login_username" : "Username"
"login_username" : "Benutzername"
"login_username" : "Username"

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.