MOBSF

ANDROID STATIC ANALYSIS REPORT

Musicolet (6.7.3 build422)

File Name:	Musicolet-Music-Player-Final-Pro-6.7.3-Arm64-v8a(www.Farsroid.com).apk
Package Name:	in.krosbits.musicolet
Scan Date:	July 6, 2023, 10:43 a.m.
App Security Score:	32/100 (HIGH RISK)
Grade:	
Trackers Detection:	1/421

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
16	19	2	2	3

FILE INFORMATION

File Name: Musicolet-Music-Player-Final-Pro-6.7.3-Arm64-v8a(www.Farsroid.com).apk
Size: 15.01MB
MD5: fa6184228d41a94cdb8939e60a82f9da
SHA1: 862a1b79e1834994aa8ba27bc2983acae703af8c
SHA256: 08b1a60cfc21e3f450b15275c7b5ce086d6ec0b1c9b58091063062259a4a03a2

APP INFORMATION

App Name: Musicolet
Package Name: in.krosbits.musicolet
Main Activity: in.krosbits.musicolet.MusicActivity
Target SDK: 33
Min SDK: 16
Max SDK:
Android Version Name: 6.7.3 build422
Android Version Code: 42200

APP COMPONENTS

Activities: 32
Services: 19
Receivers: 21
Providers: 2
Exported Activities: 2
Exported Services: 5
Exported Receivers: 10
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=BN, ST=Bangladesh, L=Dhaka, O=Telegram, OU=Modder, CN=ANiK555
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-05-09 12:43:40+00:00
Valid To: 3020-09-09 12:43:40+00:00
Issuer: C=BN, ST=Bangladesh, L=Dhaka, O=Telegram, OU=Modder, CN=ANiK555
Serial Number: 0x46416312
Hash Algorithm: sha1
md5: be441d86c46bbeef9a02f67ecfdaa3be
sha1: 88bd159bbba46f627b8bff9f3a2c7f49b1f897d4
sha256: e151ef865c9b9df84cf17a04a7073eec40951fa3757abf4ba8b7f32a00970d5f
sha512: a3c30c32a79fcbd40019df7f4ccc31390491cb1d92b2a6aa6d516c63d3321bd2460f1eb96bb082e89e9910da291aa853c4321d870b78571e39876c91efdb0ce3
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 04b01bb57241560de607d80d13be31240a47f1d9c80aa83fdcf39babb74ecb47

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.READ_MEDIA_AUDIO	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_IMAGES	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	unknown	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	unknown	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_CONNECT	unknown	Unknown permission	Unknown permission from android reference
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.android.launcher.permission.INSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.USE_FULL_SCREEN_INTENT	normal		Required for apps targeting Build.VERSION_CODES.Q that want to

			use notification full screen intents.
android.permission.EXPAND_STATUS_BAR	normal	expand/collapse status bar	Allows application to expand or collapse the status bar.
in.krosbits.musicolet.ALLOW_CAST_AUDIO	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
assets/SignatureKiller/origin.apk!classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.TAGS check FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)
assets/SignatureKiller/origin.apk!classes2.dex	FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)
	FINDINGS / DETAILS

classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.TAGS check
	Compiler	dexlib 2.x

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
in.krosbits.musicolet.GhostSearchActivity	Schemes: musicolet://, Hosts: dl,
in.krosbits.musicolet.EqualizerActivity2	Schemes: musicolet://, Hosts: eq,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 1 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 15 | WARNING: 10 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version [minSdk=16]	warning	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8, API 26 to receive reasonable security updates.
2	Launch Mode of activity (in.krosbits.musicolet.MusicActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
3	TaskAffinity is set for activity (in.krosbits.musicolet.MiniPlayerActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
4	Launch Mode of activity (in.krosbits.musicolet.SearchActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

5	Launch Mode of activity (in.krosbits.musicolet.IapActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
6	Launch Mode of activity (in.krosbits.musicolet.SettingsActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
7	Launch Mode of activity (in.krosbits.musicolet.Tag2Activity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
8	TaskAffinity is set for activity (in.krosbits.musicolet.LockScreenActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
9	Launch Mode of activity (in.krosbits.musicolet.LockScreenActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
10	Launch Mode of activity (in.krosbits.musicolet.FileUtilsActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
11	Launch Mode of activity (in.krosbits.musicolet.PlaylistActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling

			Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
12	Launch Mode of activity (in.krosbits.musicolet.EqualizerActivity2) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
13	Launch Mode of activity (in.krosbits.musicolet.RestoreActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
14	Launch Mode of activity (in.krosbits.musicolet.WelcomeActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
15	Launch Mode of activity (in.krosbits.musicolet.DbCleanActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
16	Launch Mode of activity (in.krosbits.musicolet.RGReadCalcActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
17	Launch Mode of activity (in.krosbits.musicolet.MostPlayedActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

18	Service (in.krosbits.musicolet.WidgetService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_REMOTEVIEWS [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.
19	Service (in.krosbits.musicolet.MediaBrowserServiceImpl) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Service is explicitly exported.
20	Service (in.krosbits.musicolet.QsService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_QUICK_SETTINGS_TILE [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.
21	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_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.
	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission		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. 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

22	should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	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.
23	Launch Mode of activity (com.google.android.play.core.missingsplits.PlayCoreMissingSplitsActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
24	High Intent Priority (2147483647) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
25	High Intent Priority (2147483647) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: 0 | WARNING: 6 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a1/c.java a2/g.java a2/q.java a2/r.java a6/h.java a6/l.java b0/f.java b0/g.java b0/o.java b0/r.java b0/z.java b2/z.java b5/c.java

				b8/a.java bin/mt/signature/KillerApplication.java com/pavelsikun/seekbarpreference/SeekBarPreferenceCompat.java d3/a.java d3/e.java d3/g.java e0/n.java e0/q.java e1/b.java f/i.java f/j0.java f/o0.java f/p.java f/u.java f/w0.java f/z.java f0/d.java f0/e.java f0/f.java f0/g.java f0/h.java f1/e.java f4/d.java f4/e.java f4/h.java f4/j.java f4/l.java f4/p.java f7/a.java g0/d.java g0/k.java h1/a.java h4/c.java h4/e.java h4/t.java h7/q0.java i2/d.java i2/g.java i3/g0.java i3/s.java i3/w.java

			CWE: CWE-532: Insertion of Sensitive Information into	i6/q0.java ia/k.java in/krosbits/android/widgets/swipetoloadlayout/SwipeToLoadLayout.java in/krosbits/musicolet/EqualizerActivity2.java in/krosbits/musicolet/LockScreenActivity.java in/krosbits/musicolet/MusicService.java in/krosbits/musicolet/SettingsActivity.java in/krosbits/musicolet/m6.java in/krosbits/musicolet/n3.java in/krosbits/musicolet/y1.java in/krosbits/musicolet/z1.java j/i.java j/j.java j0/l.java j1/b1.java j1/c.java j1/c0.java j1/d.java j1/d1.java j1/g.java j1/h.java j1/j0.java j1/l1.java j1/m1.java j1/q0.java j1/s0.java j1/u0.java j1/v0.java j1/y0.java j2/c.java j2/e.java j2/n.java j2/t.java j4/b0.java j4/d0.java j4/e.java j4/f.java j4/m.java j4/p.java

1	The App logs information. Sensitive information should never be logged.	info	Log File OWASP MASVS: MSTG-STORAGE-3	j4/v.java j4/w.java j4/y.java ja/a.java k/g.java k/i.java k/o.java k0/a.java k1/b.java k1/c.java k1/f.java k2/f.java k2/l.java k2/m.java k7/d.java l0/f.java l1/d.java l6/g.java l6/i.java l7/b.java m1/g0.java m1/j0.java m1/y.java m4/a.java me/zhanghai/android/materialprogressbar/HorizontalProgressDrawable.java me/zhanghai/android/materialprogressbar/MaterialProgressBar.java n0/c.java n0/d.java n0/h1.java n0/k1.java n0/t0.java n0/u1.java n0/v.java n0/v1.java n0/z1.java n6/a.java n6/g.java n6/h.java n6/l.java n6/p.java

				o1/k.java o1/m.java o1/p.java o1/q.java o1/y.java o4/a.java org/jaudiotagger/audio/mp4/atom/Mp4StcoBox.java org/lsposed/hiddenapibypass/HiddenApiBypass.java q/d.java q0/b.java q4/d.java q4/f.java q6/a.java q6/d.java q6/i.java q6/j.java q6/l.java r0/w.java s5/b.java s9/g.java ss/com/bannerslider/Slider.java t1/f.java t6/a.java u0/e.java u1/a.java u5/e.java v0/i.java v0/j.java v0/k.java v5/d.java v6/h.java v6/j.java w4/i.java x/b.java x/d.java x/e.java x/f.java x/i.java x/m.java x/o.java

				x1/f.java x1/q.java x5/e.java x5/h.java y0/b.java y0/c.java y0/g.java y3/a.java y4/a.java y7/b.java z1/g.java z3/b.java z3/g.java z5/e.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	c9/a.java c9/b.java d4/a.java d9/a.java h4/k0.java in/krosbits/musicolet/n9.java j$/util/concurrent/ThreadLocalRandom.java j1/c1.java r6/r.java
3	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	c8/k.java c8/q0.java e3/f.java e3/g.java e3/h.java e3/i.java e3/j.java e3/l.java in/krosbits/musicolet/b0.java in/krosbits/musicolet/m9.java j2/c.java t1/c.java
				j2/d.java

4	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/jaudiotagger/tag/id3/ID3v22Frames.java org/jaudiotagger/tag/id3/ID3v23Frames.java org/jaudiotagger/tag/id3/ID3v24Frames.java s7/e.java
5	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	bin/mt/signature/KillerApplication.java c8/e.java c8/e1.java i6/b1.java i6/k1.java in/krosbits/musicolet/b5.java in/krosbits/musicolet/n3.java
6	MD5 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	c8/k.java
7	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	m1/n.java
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	m9/j.java
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	l6/i.java n6/v.java
10	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	k1/f.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/arm64-v8a/lib_x86_arm_mapping.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	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.
2	lib/arm64-v8a/libstub.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.	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: ['__memmove_chk', '__strlen_chk', '__vsnprintf_chk']	True info Symbols are stripped.
		True info The shared object has NX	False high This shared object does not have a stack canary value	None info The shared	None info The shared object does	False warning The shared object does not have any fortified	True info Symbols are stripped.

3	lib/arm64-v8a/libavfilter.so	bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	object does not have run-time search path or RPATH set.	not have RUNPATH set.	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.	
4	lib/arm64-v8a/libavcodec.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	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.
5	lib/arm64-v8a/libSignatureKiller.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	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.
		True info The shared	False high This shared object does not	None info The	None info The shared	False warning The shared object does	True info Symbols are

6	lib/arm64-v8a/libavutil.so	object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	shared object does not have run-time search path or RPATH set.	object does not have RUNPATH set.	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.	stripped.
7	lib/arm64-v8a/libswresample.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	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.
8	lib/arm64-v8a/libavformat.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	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.
		True info	True info	None info	None info	True info	True info

9	lib/arm64-v8a/lib_musicolet.so	The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	The shared object does not have run-time search path or RPATH set.	The shared object does not have RUNPATH set.	The shared object has the following fortified functions: ['__strlen_chk', '__vsprintf_chk', '__read_chk', '__vsnprintf_chk', '__memmove_chk']	Symbols are stripped.
10	lib/arm64-v8a/libz.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	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.
11	lib/arm64-v8a/liblog.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	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.

12	lib/arm64-v8a/libandroid.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.	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.

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 ['USB', 'bluetooth'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform	The application has access to no sensitive information repositories.

			Resources	
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has no 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.
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 not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
12	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
13	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
14	FIA_X509_EXT.2.1	Selection-Based Security Functional	X.509 Certificate	The application use X.509v3 certificates as defined by RFC 5280 to support

		Requirements	Authentication	authentication for HTTPS , TLS.

! OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION
image.baidu.com	IP: 103.235.46.231 Country: Hong Kong Region: Hong Kong City: Hong Kong
www.baidu.com	IP: 103.235.46.40 Country: Hong Kong Region: Hong Kong City: Hong Kong

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.downloadmp3titelblabla.com	ok	No Geolocation information available.
www.id3.org	ok	**IP:** 167.99.106.11 **Country:** United States of America **Region:** California **City:** Santa Clara **Latitude:** 37.354111 **Longitude:** -121.955238 **View:** Google Map

www.doadlahomasongblabla.com	ok	No Geolocation information available.
reddit.com	ok	IP: 10.10.34.35 Country: - Region: - City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map
play.google.com	ok	IP: 142.250.185.206 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.downloadmp3songblabla.com	ok	No Geolocation information available.
image.baidu.com	ok	IP: 103.235.46.231 Country: Hong Kong Region: Hong Kong City: Hong Kong Latitude: 22.285521 Longitude: 114.157692 View: Google Map
duckduckgo.com	ok	IP: 40.114.177.246 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
schemas.android.com	ok	No Geolocation information available.

www.downloadmp3songblabla.info	ok	No Geolocation information available.
plus.google.com	ok	IP: 10.10.34.35 Country: - Region: - City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map
instagram.com	ok	IP: 10.10.34.35 Country: - Region: - City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map
twitter.com	ok	IP: 10.10.34.35 Country: - Region: - City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map
www.descargarcancionmp3blabla.com	ok	No Geolocation information available.
bing.com	ok	IP: 131.253.33.220 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
ns.adobe.com	ok	No Geolocation information available.

www.изтегленамр3песендръндрън.com	ok	No Geolocation information available.
www.facebook.com	ok	IP: 10.10.34.35 Country: - Region: - City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map
www.pobierzmp3utwórxyz.com	ok	No Geolocation information available.
www.mp3indirblabla.com	ok	No Geolocation information available.
telegram.me	ok	No Geolocation information available.
yandex.com	ok	IP: 213.180.193.56 Country: Russian Federation Region: Moskva City: Moscow Latitude: 55.752220 Longitude: 37.615559 View: Google Map
www.letoltottmp3zeneblabla.com	ok	No Geolocation information available.
en.wikipedia.org	ok	IP: 91.198.174.192 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
musicbrainz.org	ok	IP: 142.132.240.1 Country: Canada Region: Manitoba City: Winnipeg Latitude: 49.889748

		Longitude: -97.153961 **View:** Google Map
krosbits.in	ok	**IP:** 162.241.148.160 **Country:** United States of America **Region:** Utah **City:** Provo **Latitude:** 40.213909 **Longitude:** -111.634071 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.186.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
youtube.com	ok	**IP:** 10.10.34.35 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
www.baidu.com	ok	**IP:** 103.235.46.40 **Country:** Hong Kong **Region:** Hong Kong **City:** Hong Kong **Latitude:** 22.285521 **Longitude:** 114.157692 **View:** Google Map
google.com	ok	**IP:** 216.239.38.120 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991

		Longitude: -122.078514 **View:** Google Map
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

EMAILS

EMAIL	FILE
musicolet@krosbits.in translate.krosbits@gmail.com	in/krosbits/musicolet/AboutActivity.java
u0013android@android.com0 u0013android@android.com	f4/n.java

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312

HARDCODED SECRETS

POSSIBLE SECRETS
"key_album_display_mode" : "CF_ADM"
"key_disconnect_pause" : "ppkdp"
"key_earphone_double_press_behavior" : "k_edpb"
"key_earphone_triple_press_behavior" : "k_etpb"
"key_force_rescan" : "k_f_rscn"
"key_immersive_bg_now_playing" : "k_imbgnp"
"key_lyrics_settings" : "k_lycss"
"key_min_playback_req" : "MINPBR"
"key_previous_button_behaviour" : "PP_PBTNBH"
"key_refresh_songs_info_now" : "k_rsin"
"key_widget_settings" : "k_wids"
"for_xiaomi_miui_user" : "XiaomiのMIUIユーザー向け"

PLAYSTORE INFORMATION

Title: Musicolet Music Player

Score: 4.6656394 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support:** **Category:** Music & Audio **Play Store URL:** in.krosbits.musicolet

Developer Details: Krosbits, 8059182133280644587, Rajula-365560 Gujarat, India, http://krosbits.in/musicolet, musicolet@krosbits.in,

Release Date: Jun 24, 2016 **Privacy Policy:** Privacy link

Description:

---------- PLEASE READ THIS BEFORE INSTALLING 1. This app can organise and play only the local audio files which are stored on the internal storage or SD card. 2. This app can not stream/download/search new music online. ---------- Musicolet is simple, light yet powerful music player with all essential music playing features with some advance features like... ✓ Multiple Queues Now it is possible to create/manage one Queue while listening songs from another Queue. Musicolet is the only music player in android market which supports multiple Queues. You can create maximum 20 Queues. ✓ Simple GUI with Minimalistic design & Easy navigation For fast and easy navigation we placed all important components of the app (like Main player, Queues, Folders, Albums, Artists, Playlists) in just one row. So you can access them with just 1-Tap! ✓ Tag editor+: Can edit tags and album-arts of multiple songs at once. ✓ Move/Copy songs, Rename folders directly in app. ✓ Create Synchronized Lyrics. ✓ Save Bookmarks and Notes. ✓ Add/remove a song to >1 playlist, from notifications, widgets and even from lockscreen ✓ Folder browsing 2-types of folder structures: 1) Linear (all folders at once) and 2) Hierarchical(folders within folders) ✓ Powerful Equalizer : Separate presets and settings for Speakers , Headphones , Bluetooth etc. ✓ Gapless playback ✓ Earphone controls Single click for pause/play. Double click for next and Triple click for previous song. On each press >=4 you can Fast-Forward the song. ✓ Embedded Lyrics + LRC support Supports offline lyrics embedded in audio file as ID3 tag. You can edit embedded lyrics from tag editor. Musicolet also support .lrc files for synced lyrics. (Note: Musicolet doesn't fetch lyrics automatically from internet. You have to manually write or paste lyrics in tag editor, if there is no embedded lyrics. It doesn't fetch lrc file automatically. For lrc files, You have to find lrc file from internet, put it in the same folder and rename to exactly match it with audio file name manually.) ✓ Sleep timers 2 types: 1) close app after hh:mm time or 2) close app after N songs. ✓ Add shortcuts of any album/artist/folder/playlist to your HomeScreen (Launcher) app. ✓ Stunning Widgets ✓ Lock Screen (with controls, Queue and Lyrics) ✓ Audio formats supported: mp3, m4a, wma, flac, opus, aac, alac, ape, dsf and many more... ✓ Android Auto support From your 'Android Auto' enabled car, you can control music and access your playlists, queues, folders and whole music library. ✓ Change notifications appearance ✓ You can also enable Fast-Forward and rewind buttons in notifications from settings. ✓ Light and dark themes ✓ Backup and Restore Automatic and Manual backups. Restore settings, playlists, play-counts from any backup anytime on any device. And much more... No Ads Ad-free forever, for all users. No internet permission, Completely offline Musicolet doesn't even use Internet permission (a.k.a. network access permission). (You can check this in 'App permissions' at the bottom of this description in Play Store.) So it cannot send/receive even a single bit of data to/from the internet. Not even in background. Full respect of your privacy. Dedicated to Music lovers all around the world. Created with love ❤, lots of code and sleepless nights. Hope you will like our work. ---------- Our official website: https://krosbits.in/musicolet https://krosbits.in/musicolet/download ---------- To send feedback/suggestions, report bugs or for other queries... Contact us: musicolet@krosbits.in

---

Report Generated by - MobSF v3.6.8 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.