MOBSF

ANDROID STATIC ANALYSIS REPORT

Musify (9.0.0)

File Name:	Musify-arm64-v8a_1.apk
Package Name:	com.gokadzev.musify
Scan Date:	May 4, 2025, 8:39 p.m.
App Security Score:	47/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	9	2	1	1

FILE INFORMATION

File Name: Musify-arm64-v8a_1.apk
Size: 11.28MB
MD5: e8b8327ac78d4204c5eb76797810f50b
SHA1: 608e8689a8cb20334284d99d9199c53cfeceb25b
SHA256: 8ea438e1cfd3c88a1b4b87d2fe2382966236a52fcd98d62c91ee7559e09ab169

APP INFORMATION

App Name: Musify
Package Name: com.gokadzev.musify
Main Activity: com.ryanheise.audioservice.AudioServiceActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 9.0.0
Android Version Code: 2107

APP COMPONENTS

Activities: 2
Services: 1
Receivers: 2
Providers: 1
Exported Activities: 0
Exported Services: 1
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: CN=Valeri Gokadze
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-06-22 12:25:46+00:00
Valid To: 2047-06-16 12:25:46+00:00
Issuer: CN=Valeri Gokadze
Serial Number: 0x226f29cb
Hash Algorithm: sha256
md5: 64cdca3eece63a955d553e2b7afdfb14
sha1: c7c581dc1e50e208a721c78a7edd8871b849699e
sha256: a3fdd79dae938381b8582553b1382f96f1bc78a3b7028ffd07ec061c1842823a
sha512: de21e4e14aeb7c968f6f492403993667bb5a215ae45342e2c5c14382400effa55743697b53b0069ceea8b51e46e2157de300f5d41b64e300fdf48f38f3e147c2
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: c2330805a355816aad2176cdd3bceab59b02e0dda2914a9ebfd256eea91125c1
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	normal	enables foreground services for media playback.	Allows a regular application to use Service.startForeground with the type "mediaPlayback".
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.gokadzev.musify.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **0** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **4** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	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.
3	Service (com.ryanheise.audioservice.AudioService) is not Protected. [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.
4	Broadcast Receiver (com.ryanheise.audioservice.MediaButtonReceiver) is not Protected. [android:exported=true]	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.
5	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	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. 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.

</> CODE ANALYSIS

HIGH: **1** | WARNING: **4** | INFO: **2** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A/c.java B0/a.java B1/d.java B1/q.java C/d.java C1/d.java D/d.java D1/a.java F1/e.java F1/g.java G/A.java G/C0026b.java G/C0036l.java G/K.java G/O.java G/Q.java G/S.java G/X.java K0/d.java L/s.java M/d.java N1/c.java N1/e.java N1/f.java N1/g.java O/e.java P1/f.java P1/m.java Q1/a.java R1/e.java R1/l.java R1/n.java T/d.java T/k.java U1/c.java U1/d.java U1/g.java

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	U1/h.java U1/j.java U1/l.java U1/o.java U1/t.java V1/b.java V1/d.java W/f.java W/o.java W/q.java W/r.java W/s.java W1/b.java W1/j.java Z/f.java Z0/u.java a/AbstractC0110a.java com/ryanheise/audioservice/AudioService.java com/ryanheise/audioservice/MediaButtonReceiver.java e2/C0187a.java g/C0221d.java g/C0222e.java g2/C0225b.java h/MenuC0233h.java h/ViewOnKeyListenerC0230e.java h0/AbstractC0245a.java i/AbstractC0269g0.java i/AbstractC0291s.java i/C0281m0.java i/E0.java i/F0.java i/J.java i/N.java i/Q0.java i/U0.java i/r.java io/flutter/embedding/engine/FlutterJNI.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/flutter/embedding/engine/renderer/FlutterRenderer$ImageTextureRegistryEntry.java io/flutter/embedding/engine/renderer/f.java io/flutter/plugin/editing/e.java io/flutter/plugin/editing/i.java io/flutter/plugin/platform/g.java io/flutter/plugin/platform/o.java io/flutter/plugins/GeneratedPluginRegistrant.java io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/l.java j0/C0311f.java j2/C0322d.java k2/C0338g.java m0/n.java o1/AbstractC0394a.java o2/f.java o2/q.java p0/i.java q/e.java s/b.java s/f.java s/h.java s/l.java s1/C0448b.java w/C0530d.java y/m.java z/AbstractC0587f.java z/C0588g.java z/C0589h.java z/C0590l.java
2	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	a1/C0112a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	N1/c.java a/AbstractC0110a.java j2/C0322d.java
4	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	P/s.java Q1/a.java R1/g.java V0/a0.java u0/f.java y2/a.java y2/b.java y2/c.java z2/a.java
5	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	Z0/u.java io/flutter/plugin/editing/b.java
6	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	R1/e.java
7	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	a/AbstractC0110a.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	arm64-v8a/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary 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. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	arm64-v8a/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	arm64-v8a/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary 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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary 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. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00028	Read file from assets directory	file	n1/C0369c.java
00161	Perform accessibility service action on accessibility node info	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/k.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	N1/c.java N1/g.java com/ryanheise/audioservice/AudioService.java
00022	Open a file from given absolute path of the file	file	N1/c.java Y1/b.java a/AbstractC0110a.java io/flutter/embedding/engine/FlutterJNI.java j2/C0322d.java
00013	Read file and put it into a stream	file	A/c.java Z/b.java Z/f.java Z/l.java a/AbstractC0110a.java n1/C0375i.java n1/S.java o2/q.java z/C0588g.java z/C0589h.java
00024	Write file after Base64 decoding	reflection file	o2/q.java

RULE ID	BEHAVIOUR	LABEL	FILES
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java
00056	Modify voice volume	control	O1/f.java
00209	Get pixels from the latest rendered image	collection	U1/h.java
00210	Copy pixels from the latest rendered image into a Bitmap	collection	U1/h.java
00132	Query The ISO country code	telephony collection	K0/c.java
00015	Put buffer stream (data) to JSON object	file	a/AbstractC0110a.java
00003	Put the compressed bitmap data into JSON object	camera	a/AbstractC0110a.java
00014	Read file into a stream and put it into a JSON object	file	a/AbstractC0110a.java
00005	Get absolute path of file and put it to JSON object	file	a/AbstractC0110a.java
00009	Put data in cursor to JSON object	file	a/AbstractC0110a.java
00004	Get filename and put it to JSON object	file collection	a/AbstractC0110a.java com/ryanheise/audioservice/AudioService.java

RULE ID	BEHAVIOUR	LABEL	FILES
00012	Read data and put it into a buffer stream	file	a/AbstractC0110a.java
00096	Connect to a URL and set request method	command network	n1/C0389x.java
00089	Connect to a URL and receive input stream from the server	command network	n1/C0389x.java
00030	Connect to the remote server through the given URL	network	n1/C0389x.java
00109	Connect to a URL and get the response code	network command	n1/C0389x.java
00094	Connect to a URL and read data from it	command network	n1/C0389x.java
00108	Read the input stream from given URL	network command	n1/C0389x.java
00036	Get resource file from res/raw directory	reflection	Q1/a.java com/ryanheise/audioservice/AudioService.java i/E0.java n1/S.java
00191	Get messages in the SMS inbox	sms	i/E0.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	4/25	android.permission.INTERNET, android.permission.WAKE_LOCK, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE
Other Common Permissions	1/44	android.permission.FOREGROUND_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
developer.apple.com	ok	No Geolocation information available.
docs.flutter.dev	ok	No Geolocation information available.
www.unicode.org	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
api.flutter.dev	ok	No Geolocation information available.
developer.android.com	ok	No Geolocation information available.
i.scdn.co	ok	No Geolocation information available.
github.com	ok	No Geolocation information available.
www.w3.org	ok	No Geolocation information available.
dashif.org	ok	No Geolocation information available.
ns.adobe.com	ok	No Geolocation information available.
aomedia.org	ok	No Geolocation information available.
dartbug.com	ok	No Geolocation information available.

EMAILS

EMAIL	FILE
appro@openssl.org	apktool_out/lib/arm64-v8a/libflutter.so
appro@openssl.org	lib/arm64-v8a/libflutter.so

HARDCODED SECRETS

POSSIBLE SECRETS
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
9a04f079-9840-4286-ab92-e65be0885f95
e2719d58-a985-b3c9-781a-b030af78d30e
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a

SCAN LOGS

Timestamp	Event	Error
2025-05-04 20:39:12	Generating Hashes	OK
2025-05-04 20:39:12	Extracting APK	OK
2025-05-04 20:39:12	Unzipping	OK
2025-05-04 20:39:12	Parsing APK with androguard	OK

2025-05-04 20:39:13	Extracting APK features using aapt/aapt2	OK
2025-05-04 20:39:13	Getting Hardcoded Certificates/Keystores	OK
2025-05-04 20:39:15	Parsing AndroidManifest.xml	OK
2025-05-04 20:39:15	Extracting Manifest Data	OK
2025-05-04 20:39:15	Manifest Analysis Started	OK
2025-05-04 20:39:15	Performing Static Analysis on: Musify (com.gokadzev.musify)	OK
2025-05-04 20:39:15	Fetching Details from Play Store: com.gokadzev.musify	OK
2025-05-04 20:39:35	Checking for Malware Permissions	OK
2025-05-04 20:39:35	Fetching icon path	OK
2025-05-04 20:39:35	Library Binary Analysis Started	OK
2025-05-04 20:39:35	Analyzing apktool_out/lib/arm64-v8a/libflutter.so	OK

2025-05-04 20:39:35	Analyzing apktool_out/lib/arm64-v8a/libapp.so	OK
2025-05-04 20:39:35	Analyzing lib/arm64-v8a/libflutter.so	OK
2025-05-04 20:39:35	Analyzing lib/arm64-v8a/libapp.so	OK
2025-05-04 20:39:35	Reading Code Signing Certificate	OK
2025-05-04 20:39:35	Running APKiD 2.1.5	OK
2025-05-04 20:40:16	Detecting Trackers	OK
2025-05-04 20:40:16	Decompiling APK to Java with JADX	OK
2025-05-04 20:40:31	Converting DEX to Smali	OK
2025-05-04 20:40:31	Code Analysis Started on - java_source	OK
2025-05-04 20:40:33	Android SBOM Analysis Completed	OK
2025-05-04 20:40:38	Android SAST Completed	OK

2025-05-04 20:40:38	Android API Analysis Started	OK
2025-05-04 20:40:40	Android API Analysis Completed	OK
2025-05-04 20:40:40	Android Permission Mapping Started	OK
2025-05-04 20:40:42	Android Permission Mapping Completed	OK
2025-05-04 20:40:42	Android Behaviour Analysis Started	OK
2025-05-04 20:40:46	Android Behaviour Analysis Completed	OK
2025-05-04 20:40:46	Extracting Emails and URLs from Source Code	OK
2025-05-04 20:40:47	Email and URL Extraction Completed	OK
2025-05-04 20:40:47	Extracting String data from APK	OK
2025-05-04 20:40:47	Extracting String data from SO	OK
2025-05-04 20:40:48	Extracting String data from Code	OK

2025-05-04 20:40:48	Extracting String values and entropies from Code	OK
2025-05-04 20:40:48	Performing Malware check on extracted domains	OK
2025-05-04 20:45:29	Saving to Database	OK

Report Generated by - MobSF v4.3.2

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.