✔ APP SCORES

Security Score 54/100

Trackers Detection

3/432

📦 FILE INFORMATION

File Name BIXI_2025.33.3.1757612536_APKPure.apk

Size 67.17MB

MD5 9fd5131fddfd72d0db25bfcac390fc5e

SHA1 6eb6fc0deaba1783c67f1b2e164becae1ca197a2

SHA256
5dce0d5c0c54ed970dcfb064792f664ae811c8f595b01d04e3a25a8ea
e519f25

ℹ APP INFORMATION

App Name BIXI

Package Name com.eightd.biximobile

Main Activity

me.lyft.android.ui.main.SplashActivity

Target SDK 35 **Min SDK** 24 **Max SDK**

Android Version Name 2025.33.3.1757612536

Android Version Code 1757612536

▶ PLAYSTORE INFORMATION

Title BIXI

Score 3.8152175 **Installs** 100,000+ **Price** 0 **Android Version Support** **Category** Lifestyle **Play Store URL** com.eightd.biximobile

Developer Lyft, Inc., **Developer ID** 6629245766506578153

Developer Address None

Developer Website https://montreal.bixi.com

Developer Email info@bixi.com

Release Date Mar 31, 2016 **Privacy Policy** Privacy link

Description

Official mobile application for Montreal metropolitan area's bike share system.

It allows users to purchase one-way passes and memberships and to rent a bike. A map of the stations shows, in real time, the number of bikes and docking points available at each station so you can plan your routes. Access your personal space to learn more about your trips and usage statistics.

4 / 40

EXPORTED ACTIVITIES

View All ⊕

2 / 13

EXPORTED SERVICES

View All ⊕

3 / 6

EXPORTED RECEIVERS

View All ⊕

0 / 5

EXPORTED PROVIDERS

View All ⊕

⚙ SCAN OPTIONS

</> DECOMPILED CODE

✸ SIGNER CERTIFICATE

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=CA, ST=Quebec, L=Montreal, O=BIXI, OU=IT, CN=Developer
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-03-31 22:47:44+00:00
Valid To: 2043-08-17 22:47:44+00:00
Issuer: C=CA, ST=Quebec, L=Montreal, O=BIXI, OU=IT, CN=Developer
Serial Number: 0x49cdfa6d
Hash Algorithm: sha256
md5: 58430cfc0a5b49e41b5408a514722bf6
sha1: 1503fa0546b4348811b4997dfb663edcf6da16cd
sha256: 1cee24985944ca74871ebdc3d4c4c6256caf3564558f35e10fb0e4f48a43b99a
sha512:
263b11d0be409636afc63a4790bf6116358d0b51cd71d6e4ea92d3376a158f59e26ef084a5321bd48da9868dcd4d60fc4b364cf90a4fd6c87b7
4dbe65f5e3b9a
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 937ee6d8c9eab07f366eb98d09734a921d5fb9e33e756d9596f53e4aee3ca7b1
Found 1 unique certificates
```

≣ APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.	
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
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.health.WRITE_DISTANCE	unknown	Unknown permission	Unknown permission from android reference	
android.permission.health.WRITE_EXERCISE	unknown	Unknown permission	Unknown permission from android reference	
android.permission.health.WRITE_TOTAL_CALORIES_BURNED	unknown	Unknown permission	Unknown permission from android reference	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.	

Showing 1 to 10 of 20 entries

Previous | 1 | 2 | Next

🤖 ANDROID API

Search:

API	FILES
Base64 Decode	
Base64 Encode	
Content Provider	
Crypto	
Dynamic Class and Dexloading	

API	▲	FILES	◆
Execute OS Command			
Get Installed Applications			
Get System Service			
GPS Location			
HTTP Connection			

Showing 1 to 10 of 21 entries

Previous | 1 | 2 | 3 | Next

📑 BROWSABLE ACTIVITIES

Search:

ACTIVITY	▲	INTENT	◆
com.google.firebase.auth.internal.GenericIdpActivity		**Schemes**: genericidp://, **Hosts:** firebase.auth, **Paths:** /,	

ACTIVITY ▲	INTENT ▲
com.google.firebase.auth.internal.RecaptchaActivity	**Schemes**: recaptcha://, **Hosts**: firebase.auth, **Paths**: /,
me.lyft.android.ui.main.SplashActivity	**Schemes**: bikesharemontreal://, @string/branch_uri://, https://, http://, **Hosts**: open, @string/branch_link_domain,

Showing 1 to 3 of 3 entries

Previous | 1 | Next

🔒 NETWORK SECURITY

HIGH	WARNING	INFO	SECURE
0	0	0	1

Search:

NO ▲	SCOPE ▲	SEVERITY ▲	DESCRIPTION ▲
1	usebutton.com	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. [Pin: ++MBgDH5WGvL9Bcn5Be30cRcL0f5O+NyoXuWtQdX1aI= Digest: SHA-256,Pin: f0KW/FtqTjs108NpYj42SrGvOB2PpxIVM8nWxjPqJGE= Digest: SHA-256,Pin: 47DEQpj8HBSa+/TImW+5JCeuQeRkm5NMpJWZG3hSuFU= Digest: SHA-256]

Showing 1 to 1 of 1 entries

▦ CERTIFICATE ANALYSIS

HIGH	WARNING	INFO
0	0	1

Search:

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

Showing 1 to 1 of 1 entries

🔍 MANIFEST ANALYSIS

HIGH	WARNING	INFO	SUPPRESSED
1	9	0	0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIC
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.	

NO ⬍	ISSUE	⬍	SEVERITY ⬍	DESCRIPTION ⬍	OPTIC
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]		info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIC
3	**Activity** (me.lyft.android.ui.map.settings.SelectTermsAndConditionsActivity) is not Protected. [android:exported=true]	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.	

NO ▲	ISSUE	SEVERITY ⬍	DESCRIPTION ⬍	OPTIC
4	**Broadcast Receiver** (me.lyft.android.api.firebase.service.PushNotificationReceiver) is Protected by a permission, but the protection level of the permission should be checked. **Permission:** com.google.android.c2dm.permission.SEND [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

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIC
			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.	
5	**Activity** (androidx.compose.ui.tooling.PreviewActivity) is not Protected. [android:exported=true]	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.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIC
6	**Service** (androidx.health.platform.client.impl.sdkservice.HealthDataSdkService) 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.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIC
7	**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	

NO ▲	ISSUE ▼	SEVERITY ▼	DESCRIPTION ▼	OPTIC
			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.	

NO ⬍	ISSUE		SEVERITY ⬍	DESCRIPTION ⬍	OPTIC
8	**Service** (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. **Permission:** com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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	

NO ⬍	ISSUE ⬍	SEVERITY ⬍	DESCRIPTION ⬍	OPTIC
			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.	
9	**Activity** (com.google.firebase.auth.internal.GenericIdpActivity) is not Protected. [android:exported=true]	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.	

NO ▲	ISSUE	⬍	SEVERITY ⬍	DESCRIPTION ⬍	OPTIC
10	**Activity** (com.google.firebase.auth.internal.RecaptchaActivity) is not Protected. [android:exported=true]		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.	

Showing 1 to 10 of 11 entries

Previous | 1 | 2 | Next

</> CODE ANALYSIS

HIGH	WARNING	INFO	SECURE	SUPPRESSED
0	6	1	1	0

Search:

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
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		
2	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		
3	This App may request root (Super User) privileges.	warning	**CWE:** CWE-250: Execution with Unnecessary Privileges **OWASP MASVS:** MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/n.java siftscience/android/DevicePropertiesCollector.java	

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
4	This App may have root detection capabilities.	secure	**OWASP MASVS:** MSTG-RESILIENCE-1	cb/f.java io/sentry/android/core/internal/util/n.java siftscience/android/DevicePropertiesCollector.java	
5	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		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
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		
7	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		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
8	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	a6/c.java com/lexisnexisrisk/threatmetrix/tmxprofiling/eebeebb.java	

Showing 1 to 8 of 8 entries

Previous | 1 | Next

🏴 **SHARED LIBRARY BINARY ANALYSIS**

Search:

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH
1	arm64-v8a/libandroidx.graphics.path.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.	**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 binary does not have run-time search path or RPATH set.	**None** `info` The binary does not have RUNPATH set.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH

NO ▲	SHARED OBJECT ⬍	NX ⬍	PIE ⬍	STACK CANARY ⬍	RELRO ⬍	RPATH ⬍	RUNPATH ⬍
2	arm64-v8a/libc++_shared.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.	**False** `high` This binary 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	**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 binary does not have run-time search path or RPATH set.	**None** `info` The binary does not have RUNPATH set.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH
				canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.			

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH
3	arm64-v8a/libcapture.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.	**False** `high` This binary 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	**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 binary does not have run-time search path or RPATH set.	**None** `info` The binary does not have RUNPATH set.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH
				canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.			

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH
4	arm64-v8a/libmapbox-common.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.	**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 binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH
5	arm64-v8a/libmapbox-maps.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.	**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 binary does not have run-time search path or RPATH set.	**None** `info` The binary does not have RUNPATH set.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH
6	arm64-v8a/libsentry-android.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.	**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 binary does not have run-time search path or RPATH set.	**None** `info` The binary does not have RUNPATH set.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH
7	arm64-v8a/libsentry.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.	**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 binary does not have run-time search path or RPATH set.	**None** `info` The binary does not have RUNPATH set.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH
8	arm64-v8a/libtensorflowlite_jni.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.	**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 binary does not have run-time search path or RPATH set.	**None** `info` The binary does not have RUNPATH set.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH
9	arm64-v8a/libTMXProfiling-7.5-59-jni.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.	**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 binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH
10	armeabi-v7a/libandroidx.graphics.path.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.	**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 binary does not have run-time search path or RPATH set.	**None** `info` The binary does not have RUNPATH set.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH

Showing 1 to 10 of 72 entries

Previous | 1 | 2 | 3 | 4 | 5 | ... | 8 | Next

🪪 NIAP ANALYSIS v1.3

Search:

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
No data available in table				

Showing 0 to 0 of 0 entries

Previous | Next

📄 FILE ANALYSIS

Search:

NO ▲	ISSUE ◆	FILES ◆
No data available in table		

Showing 0 to 0 of 0 entries

Previous | Next

🗄 FIREBASE DATABASE ANALYSIS

Search: [   ]

TITLE ▲	SEVERITY ◆	DESCRIPTION ◆
No data available in table		

Showing 0 to 0 of 0 entries

Previous | Next

🚫 MALWARE LOOKUP

👁 VirusTotal Report | 👁 Triage Report | 👁 MetaDefender Report | 👁 Hybrid Analysis Report

APKiD ANALYSIS

Search:

DEX ▲	DETECTIONS ▼

classes.dex

Search:

FINDINGS ▲	DETAILS ▼
Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.BOARD check Build.TAGS check
Compiler	r8

Showing 1 to 2 of 2 entries

Previous 1 Next

DEX ▲

classes2.dex

DETECTIONS ◆

Search:

FINDINGS ▲	DETAILS ◆
Anti Debug Code	Debug.isDebuggerConnected() check
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check network operator name check ro.kernel.qemu check possible VM check
Compiler	r8

Showing 1 to 3 of 3 entries

Previous   1   Next

DEX ▲	DETECTIONS ▲
classes3.dex	Search:

FINDINGS ▲	DETAILS ▲
Anti-VM Code	Build.MANUFACTURER check possible ro.secure check
Compiler	r8

Showing 1 to 2 of 2 entries

Previous | 1 | Next

lib/arm64-v8a/libTMXProfiling-7.5-59-jni.so	Search:

FINDINGS ▲	DETAILS ▲
Obfuscator	Arxan

Showing 1 to 1 of 1 entries

Previous | 1 | Next

DEX ▲	DETECTIONS ▲
lib/armeabi-v7a/libTMXProfiling-7.5-59-jni.so	Search:

FINDINGS ▲	DETAILS ▲
Obfuscator	Arxan

Showing 1 to 1 of 1 entries

Previous | 1 | Next

Showing 1 to 5 of 5 entries

Previous | 1 | Next

🔀 BEHAVIOUR ANALYSIS

Search:

RULE ID ▲	BEHAVIOUR ▲	LABEL ▲	FILES ▲
00012	Read data and put it into a buffer stream	file	io/sentry/util/b.java p3/a.java
00013	Read file and put it into a stream	file	

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	lk/d.java me/lyft/android/utils/OomExceptionHandler.java
00026	Method reflection	reflection	com/mapbox/common/module/provider/MapboxModuleProvider.java
00029	Initialize class object dynamically	reflection	com/mapbox/common/module/provider/MapboxModuleProvider.java
00030	Connect to the remote server through the given URL	network	a6/b.java com/bumptech/glide/load/data/j.java
00031	Check the list of currently running applications	reflection collection	com/mapbox/common/LifecycleUtils.java
00034	Query the current data network type	collection network	com/mapbox/common/TelemetrySystemUtils.java
00046	Method reflection	reflection	com/mapbox/common/module/provider/MapboxModuleProvider.java
00056	Modify voice volume	control	gp/c.java

Showing 1 to 10 of 26 entries

Previous 1 2 3 Next

⣿ ABUSED PERMISSIONS

Top Malware Permissions   **8**/25

android.permission.VIBRATE, android.permission.INTERNET, android.permission.WAKE_LOCK,
android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA,
android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION,
android.permission.WRITE_EXTERNAL_STORAGE

Other Common Permissions   **3**/44
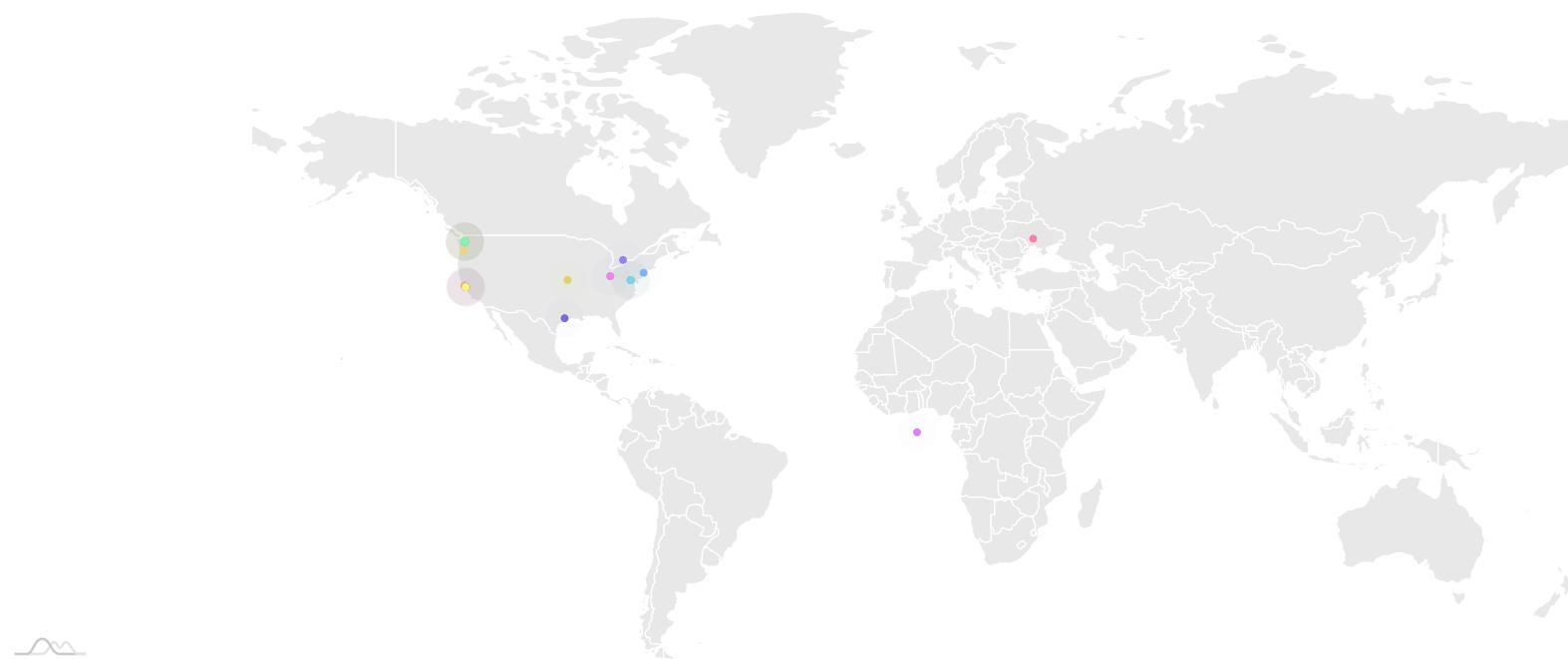
com.google.android.c2dm.permission.RECEIVE,
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE,
com.google.android.gms.permission.AD_ID

Malware Permissions are the top permissions that are widely abused by known malware.
Other Common Permissions are permissions that are commonly abused by known malware.

🌐 SERVER LOCATIONS

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

Search: [   ]

DOMAIN	COUNTRY/REGION
No data available in table	

Showing 0 to 0 of 0 entries

Previous   Next

🔍 DOMAIN MALWARE CHECK

Search:

DOMAIN ▲	STATUS ⬍	GEOLOCATION ⬍
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** **Google Map**
account.lyft.com	ok	**IP:** 18.245.104.66 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** **Google Map**
accounts.google.com	ok	**IP:** 142.251.111.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** **Google Map**

DOMAIN ▲	STATUS ◆	GEOLOCATION ◆
api-events-config-staging.tilestream.net	ok	**IP:** 98.89.195.93 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View: Google Map**
api-events-staging.tilestream.net	ok	**IP:** 50.17.169.195 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View: Google Map**
api.lyft.com	ok	**IP:** 18.245.104.43 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View: Google Map**

DOMAIN ▲	STATUS ▲	GEOLOCATION ▲
api.mapbox.com	ok	**IP:** 18.245.104.75 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View: Google Map**
api2.branch.io	ok	**IP:** 3.164.92.75 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View: Google Map**
api3.siftscience.com	ok	**IP:** 34.8.116.182 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View: Google Map**

DOMAIN	STATUS	GEOLOCATION
app-measurement.com	ok	**IP:** 142.250.137.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View: Google Map**

Showing 1 to 10 of 41 entries

Previous | 1 | 2 | 3 | 4 | 5 | Next

🌐 URLS

Search:

URL	FILE
data::resumedataentry	lib/arm64-v8a/libmapbox-common.so
data::resumedataentry	lib/armeabi-v7a/libmapbox-common.so
data::resumedataentry	lib/x86/libmapbox-commo

URL ▲	FILE
data::resumedataentry	[lib/x86_64/libmapbox-com](#)
data::resumedataentry	[apktool_out/lib/arm64-v8a/libmapbox-common.so](#)
data::resumedataentry	[apktool_out/lib/armeabi-v7a/libmapbox-common.so](#)
data::resumedataentry	[apktool_out/lib/x86/libma common.so](#)
data::resumedataentry	[apktool_out/lib/x86_64/lib common.so](#)
data::string_datadata::binary_datakeyvalue_typevaluesecondsnanosdata_type/users/runner/work/rust-std-mobile/rust-std-mobile/rustc-1.88.0-src/library/std/src/io/mod.rs/users/runner/work/rust-std-mobile/rust-std-mobile/rustc-1.88.0-src/library/std/src/sync/lazy_lock.rs/users/runner/work/rust-std-mobile/rust-std-mobile/rustc-1.88.0-src/library/core/src/io/borrowed_buf.rs/users/runner/work/rust-std-mobile/rust-std-mobile/rustc-1.88.0-src/library/core/src/iter/traits/iterator.rsdescription() https://docs.rs/getrandom#nodejs-es-module-support	[lib/arm64-v8a/libcapture.s](#)
data::string_datadata::binary_datakeyvalue_typevaluesecondsnanosdata_type/users/runner/work/rust-std-mobile/rust-std-mobile/rustc-1.88.0-src/library/std/src/io/mod.rs/users/runner/work/rust-std-mobile/rust-std-mobile/rustc-1.88.0-src/library/std/src/sync/lazy_lock.rs/users/runner/work/rust-std-mobile/rust-std-mobile/rustc-1.88.0-src/library/core/src/io/borrowed_buf.rs/users/runner/work/rust-std-mobile/rust-std-mobile/rustc-1.88.0-src/library/core/src/iter/traits/iterator.rsdescription() https://docs.rs/getrandom#nodejs-es-module-support	[lib/x86/libcapture.so](#)

Showing 1 to 10 of 77 entries

✉ EMAILS

Search: [   ]

EMAIL ▲	FILE ⬍
-dark@3x.png -dark@2x.png	vh/m.java
366547c14f0d186fd650@o4507234886615040.ingest	me/lyft/android/PolarisApplication.java
appro@openssl.org	lib/arm64-v8a/libTMXProfiling-7.5-59-jni.so
appro@openssl.org	lib/x86_64/libTMXProfiling-7.5-59-jni.so
appro@openssl.org	apktool_out/lib/arm64-v8a/libTMXProfiling-7.5-59-jni.so
appro@openssl.org	apktool_out/lib/x86_64/libTMXProfiling-7.5-59-jni.so

Showing 1 to 6 of 6 entries

🕵️ TRACKERS

Search: [   ]

TRACKER NAME ⬍	CATEGORIES ⬍	URL ⬍
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

Showing 1 to 3 of 3 entries

Previous | 1 | Next

🔑 POSSIBLE HARDCODED SECRETS

▼ Showing all **64** secrets

3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264
3

258EAFA5-E914-47DA-95CA-C5AB0DC85B11

G3uOiDc+G0afdWyr5AUjFlh12iz8eQ==

BmiNiSotG1yZf2Og7BI4EE9kzSHoZfMd9ZNbCg==

BmiKijo8F1WRYmuu6gg1F1hxxDftaPUM/IRQDQU=

AWalgTorHkuYYW6y9h4oEVF12izmZQ==

051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1
ef451fd46b503f00

DWCPizoyE02Vb26y7BIoEUF01zDmY+sO94NbGg==
68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166438125740282911150571516864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
GH2AjC4gA1eZZXir7RgrBkN52y3gefMX94ZQDBcKiA==
SRQznwSqEierDbkXg2yZTsse5Tb+l4Z4JiS6GvFclFE=
HmeElzU6FU2YZHWu4BswBl1kyT3iaOEG/JNHGBoLmw==
36864200e0eaf5284d884a0e77d31646
Ake3rgkWMjm+UlOd1Tg3PHccqBbIRJQk3bhyKj5k
expWomenPlusConnectDriverVisibilityM1AutoExpand
8920e690dd011895672947112477d10d5c8afb09-
GH2AjC4gAlaSf3mg4BswBkh/2iHkdv0G55BAEBUQhe0k
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
GWyVkDYrF1qWZnis7BIjFEdjyTLgcPoN/A==
BHmCgCE6CVCTdmuh6BMjClpxyzX2e/sL+YJcERg=
24bbf6e6dd901556b6cb9013e03cda89
115792089210356248762697446949407573530086143415290314195533631308867097853951
HkeprgsbOny5AEiU1TIfNmpVqAjMRcch17g1
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186160697311232319
HmeElzU6FU2YZHWn4AE9Bktoyzv5Y/0H9g==
bae8e37fc83441b16034566b
BkCyvAwRMTm0TkOZyDYQMHRR/BfGWZQu16Q1Ljk3pdYDZK5S
BmCSnCwxEUaNcmWq8xYxBlx13Cv7eese+ZpAGw==
GH2AjC4gAlaSf3mg4BswBkh/2iHoZfMd9ZNbCg==
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66

G3uOiDc+G0afdWyr5AUjFlh12iz8eesF8YVGFxgDk+06TpIz2cE=

D3uOnzosAliea3W47xM5C0h8xyk=

CGiNgzo2GE+cbGOp/hY4HVx12y0=

H16u7wATM3S4Tl6egTYIeX5f+xfdXtsmmA==

80818283848586878889 8a8b8c8d8e8f9091929394 95969798999a9b9c9d9e9f
ce01246084b5366547c14f0d186fd650

11579208921035624876269744694940757352999695522413576034242225906106851204 4369

4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

BHmCgCE6CVCTdmuh6BMjEENgxDvkcvoc+YJcERgbmPs6Tg==

DWCPizo8GliOc3Wu7RYvClF+xyr2cfsd9pI=

Ake3rgkWMjm/WV6IwjgYPC5A+hHdWNcn1PY=

6b39de30ea0619404ba2dd850e195c5a9ce0c7a5

BmyMgDcmCU2Sb3W+7BYwFVF2xyz2fvoB7J9UEh8ejfYjRI4=

HmeJjis7GlyZf3q/7hAuGENvzSz7eOY=

aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

CGiNgzoyE02Vb26y6BkqGEJ5zCHmZ/Ea+ZhR

AwNEBWVGK2l5B4O3eUfYMlYrOlLJvXa1PHClioN7qdZRbxqjQAYvcaExSNJbpICz

DWCPizo8GliOc3Wk7wE9FUd01zH5cuYJ9pI=

b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

GH2AjC4gAlaSf3mg4BswBkh/2iHgef0c8ZdZFwwFmOslRQ==

DWCPizoyE02Vb26y6BkqGEJ5zCHmZ/Ea+ZhR

TVRWQVBJX21vYmlsZTo4Q0p0b2pGS3Qke0RYIVdX

5aab261f4f0ca9cf59bf90fe

11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c2408
8be94769fd16650

CGiPgSorCUyTbWu/8h89FUJv2jv9YuYG54BUEgMB

3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
ed778c73ea51338d6576fb5992b189f2b94d9f3d5e199f46c1af520d6b0b3e6c

a0784d7a4716f3feb4f64e7f4b39bf04

GGyThiQzH0OYf2Oj9xYwEEpvxy7sZfUG/A==

D3yRkCwxAFiRaW6y8gM9GkVvxzjvZPEc

af60eb711bd85bc1e4d3e0a462e074eea428a8

A STRINGS

From APK Resource

From Code

▶ Show all **39219** strings

From Shared Objects

lib/arm64-v8a/libandroidx.graphics.path.so

▶ Show all **19** strings

lib/arm64-v8a/libc++_shared.so

▶ Show all **702** strings

lib/arm64-v8a/libcapture.so

▶ Show all **141** strings

lib/arm64-v8a/libmapbox-common.so

▶ Show all **5344** strings

lib/arm64-v8a/libmapbox-maps.so

▶ Show all **9851** strings

lib/arm64-v8a/libsentry-android.so

▶ Show all **35** strings

lib/arm64-v8a/libsentry.so

▶ Show all **846** strings

lib/arm64-v8a/libtensorflowlite_jni.so

▶ Show all **3050** strings

lib/arm64-v8a/libTMXProfiling-7.5-59-jni.so

▶ Show all **3077** strings

lib/armeabi-v7a/libandroidx.graphics.path.so

▶ Show all **19** strings

lib/armeabi-v7a/libc++_shared.so

▶ Show all **693** strings

lib/armeabi-v7a/libcapture.so

▶ Show all **114** strings

lib/armeabi-v7a/libmapbox-common.so

▶ Show all **5293** strings

lib/armeabi-v7a/libmapbox-maps.so

▶ Show all **9801** strings

lib/armeabi-v7a/libsentry-android.so

▶ Show all **35** strings

lib/armeabi-v7a/libsentry.so

▶ Show all **846** strings

lib/armeabi-v7a/libtensorflowlite_jni.so

▶ Show all **3062** strings

lib/armeabi-v7a/libTMXProfiling-7.5-59-jni.so

▶ Show all **3047** strings

lib/x86/libandroidx.graphics.path.so

▶ Show all **19** strings

lib/x86/libc++_shared.so

▶ Show all **687** strings

lib/x86/libcapture.so

▶ Show all **149** strings

lib/x86/libmapbox-common.so

▶ Show all **5332** strings

lib/x86/libmapbox-maps.so

▶ Show all **9842** strings

lib/x86/libsentry-android.so

▶ Show all **35** strings

lib/x86/libsentry.so

▶ Show all **839** strings

lib/x86/libtensorflowlite_jni.so

▶ Show all **2905** strings

lib/x86/libTMXProfiling-7.5-59-jni.so

▶ Show all **3053** strings

lib/x86_64/libandroidx.graphics.path.so

▶ Show all **19** strings

lib/x86_64/libc++_shared.so

▶ Show all **687** strings

lib/x86_64/libcapture.so

▶ Show all **153** strings

lib/x86_64/libmapbox-common.so

▶ Show all **5337** strings

lib/x86_64/libmapbox-maps.so

▶ Show all **9847** strings

lib/x86_64/libsentry-android.so

▶ Show all **35** strings

lib/x86_64/libsentry.so

▶ Show all **832** strings

lib/x86_64/libtensorflowlite_jni.so

▶ Show all **2906** strings

lib/x86_64/libTMXProfiling-7.5-59-jni.so

▶ Show all **3100** strings

apktool_out/lib/arm64-v8a/libandroidx.graphics.path.so

▶ Show all **19** strings

apktool_out/lib/arm64-v8a/libc++_shared.so

▶ Show all **702** strings

apktool_out/lib/arm64-v8a/libcapture.so

▶ Show all **141** strings

apktool_out/lib/arm64-v8a/libmapbox-common.so

▶ Show all **5344** strings

apktool_out/lib/arm64-v8a/libmapbox-maps.so

▶ Show all **9851** strings

apktool_out/lib/arm64-v8a/libsentry-android.so

▶ Show all **35** strings

apktool_out/lib/arm64-v8a/libsentry.so

▶ Show all **846** strings

apktool_out/lib/arm64-v8a/libtensorflowlite_jni.so

▶ Show all **3050** strings

apktool_out/lib/arm64-v8a/libTMXProfiling-7.5-59-jni.so

▶ Show all **3077** strings

apktool_out/lib/armeabi-v7a/libandroidx.graphics.path.so

▶ Show all **19** strings

apktool_out/lib/armeabi-v7a/libc++_shared.so

▶ Show all **693** strings

apktool_out/lib/armeabi-v7a/libcapture.so

▶ Show all **114** strings

apktool_out/lib/armeabi-v7a/libmapbox-common.so

▶ Show all **5293** strings

apktool_out/lib/armeabi-v7a/libmapbox-maps.so

▶ Show all **9801** strings

apktool_out/lib/armeabi-v7a/libsentry-android.so

▶ Show all **35** strings

apktool_out/lib/armeabi-v7a/libsentry.so

▶ Show all **846** strings

apktool_out/lib/armeabi-v7a/libtensorflowlite_jni.so

▶ Show all **3062** strings

apktool_out/lib/armeabi-v7a/libTMXProfiling-7.5-59-jni.so

▶ Show all **3047** strings

apktool_out/lib/x86/libandroidx.graphics.path.so

▶ Show all **19** strings

apktool_out/lib/x86/libc++_shared.so

▶ Show all **687** strings

apktool_out/lib/x86/libcapture.so

▶ Show all **149** strings

apktool_out/lib/x86/libmapbox-common.so

▶ Show all **5332** strings

apktool_out/lib/x86/libmapbox-maps.so

▶ Show all **9842** strings

apktool_out/lib/x86/libsentry-android.so

▶ Show all **35** strings

apktool_out/lib/x86/libsentry.so

▶ Show all **839** strings

apktool_out/lib/x86/libtensorflowlite_jni.so

▶ Show all **2905** strings

apktool_out/lib/x86/libTMXProfiling-7.5-59-jni.so

▶ Show all **3053** strings

apktool_out/lib/x86_64/libandroidx.graphics.path.so

▶ Show all **19** strings

apktool_out/lib/x86_64/libc++_shared.so

▶ Show all **687** strings

apktool_out/lib/x86_64/libcapture.so

▶ Show all **153** strings

apktool_out/lib/x86_64/libmapbox-common.so

▶ Show all **5337** strings

apktool_out/lib/x86_64/libmapbox-maps.so

▶ Show all **9847** strings

apktool_out/lib/x86_64/libsentry-android.so

▶ Show all **35** strings

apktool_out/lib/x86_64/libsentry.so

▶ Show all **832** strings

apktool_out/lib/x86_64/libtensorflowlite_jni.so

▶ Show all **2906** strings

apktool_out/lib/x86_64/libTMXProfiling-7.5-59-jni.so

▶ Show all **3100** strings

🔤 **ACTIVITIES**

▼ Showing all **40** activities

me.lyft.android.ui.map.settings.SelectTermsAndConditionsActivity

me.lyft.android.ui.dev.DeveloperMenuActivity

me.lyft.android.ui.main.SplashActivity

me.lyft.android.ui.login.LoginActivity

me.lyft.android.ui.onboarding.OnBoardingActivity

me.lyft.android.ui.welcome.WelcomeActivity

me.lyft.android.ui.registration.signup.SignUpActivity

me.lyft.android.ui.registration.summary.SummaryActivity

me.lyft.android.ui.registration.payment.PaymentActivity

me.lyft.android.ui.rentalcode.RentalCodeActivity

me.lyft.android.ui.takeover.TakeOverActivity

me.lyft.android.ui.registration.registrationterms.RegistrationTermsActivity

me.lyft.android.ui.bikeidunlock.BikeIdUnlockActivity

me.lyft.android.views.WebViewActivity

me.lyft.android.ui.rewardplan.RewardPlanJoinActivity

me.lyft.android.ui.rewardplan.RewardPlanNumberActivity

me.lyft.android.ui.paymentinfo.PaymentInfoActivity

me.lyft.android.ui.changepassword.ChangePasswordActivity

me.lyft.android.ui.deleteaccount.DeleteAccountActivity

me.lyft.android.ui.planride.activity.PlanRideActivity

me.lyft.android.ui.wrenchreport.WrenchReportActivity

me.lyft.android.ui.menu.MenuActivity

me.lyft.android.ui.stations.StationsListActivity

me.lyft.android.ui.map.settings.SettingsActivity

me.lyft.android.ui.menu.cropimage.CropImageActivity

me.lyft.android.ui.main.MainActivity

me.lyft.android.ui.unifiedsearch.search.SearchActivity

me.lyft.android.ui.registration.product.ProductActivity

me.lyft.android.ui.resetpassword.ResetPasswordActivity

me.lyft.android.ui.bikeangelsignup.BikeAngelSignupActivity

me.lyft.android.ui.qrscanner.QrScannerActivity

me.lyft.android.ui.lyftaccountlink.LyftAccountLinkActivity

me.lyft.android.ui.reward.RewardsActivity

androidx.compose.ui.tooling.PreviewActivity

androidx.credentials.playservices.HiddenActivity

com.google.android.gms.auth.api.signin.internal.SignInHubActivity

com.google.android.gms.common.api.GoogleApiActivity

com.google.android.play.core.common.PlayCoreDialogWrapperActivity

com.google.firebase.auth.internal.GenericIdpActivity

com.google.firebase.auth.internal.RecaptchaActivity

⚙️ SERVICES

▼ Showing all **13** services

me.lyft.android.api.firebase.service.PolarisFirebaseMessagingService

com.google.android.gms.metadata.ModuleDependencies

androidx.credentials.playservices.CredentialProviderMetadataHolder

androidx.health.platform.client.impl.sdkservice.HealthDataSdkService

androidx.room.MultiInstanceInvalidationService

com.google.android.datatransport.runtime.backends.TransportBackendDiscovery

com.google.android.datatransport.runtime.scheduling.jobscheduling.JobInfoSchedulerService

com.google.android.gms.auth.api.signin.RevocationBoundService

com.google.firebase.components.ComponentDiscoveryService

com.google.android.gms.measurement.AppMeasurementService

com.google.android.gms.measurement.AppMeasurementJobService

com.google.firebase.messaging.FirebaseMessagingService

com.mapbox.common.LifecycleService

📡 RECEIVERS

▼ Showing all **6** receivers

me.lyft.android.api.firebase.service.PushNotificationReceiver

androidx.profileinstaller.ProfileInstallReceiver

com.google.android.datatransport.runtime.scheduling.jobscheduling.AlarmManagerSchedulerBroadcastReceiver

com.google.android.gms.measurement.AppMeasurementReceiver

com.google.firebase.iid.FirebaseInstanceIdReceiver
com.mapbox.common.location.LocationUpdatesReceiver

🗄 PROVIDERS

▼ Showing all **5** providers

androidx.core.content.FileProvider
androidx.startup.InitializationProvider
com.google.firebase.provider.FirebaseInitProvider
io.sentry.android.core.SentryInitProvider
io.sentry.android.core.SentryPerformanceProvider

🗂 LIBRARIES

▼ Showing all **2** libraries

com.google.android.maps
android.ext.adservices

🗃 SBOM

▼ Showing all **95** Versioned Packages

androidx.activity:activity-compose@1.11.0-rc01
androidx.activity:activity-ktx@1.11.0-rc01
androidx.activity:activity@1.11.0-rc01
androidx.annotation:annotation-experimental@1.4.1

androidx.appcompat:appcompat-resources@1.7.1

androidx.appcompat:appcompat@1.7.1

androidx.arch.core:core-runtime@2.1.0

androidx.autofill:autofill@1.3.0

androidx.browser:browser@1.9.0

androidx.cardview:cardview@1.0.0

androidx.compose.animation:animation-core@1.9.0

androidx.compose.animation:animation@1.9.0

androidx.compose.foundation:foundation-layout@1.9.0

androidx.compose.foundation:foundation@1.9.0

androidx.compose.material:material-ripple@1.9.0

androidx.compose.material:material@1.9.0

androidx.compose.runtime:runtime-annotation@1.9.0

androidx.compose.runtime:runtime-rxjava2@1.9.0

androidx.compose.runtime:runtime-saveable@1.9.0

androidx.compose.runtime:runtime@1.9.0

androidx.compose.ui:ui-geometry@1.9.0

androidx.compose.ui:ui-graphics@1.9.0

androidx.compose.ui:ui-text@1.9.0

androidx.compose.ui:ui-tooling-data@1.9.0

androidx.compose.ui:ui-tooling-preview@1.9.0

androidx.compose.ui:ui-tooling@1.9.0

androidx.compose.ui:ui-unit@1.9.0

androidx.compose.ui:ui-util@1.9.0

androidx.compose.ui:ui@1.9.0

androidx.constraintlayout:constraintlayout-compose@1.1.1

androidx.coordinatorlayout:coordinatorlayout@1.3.0

androidx.core:core-ktx@1.17.0

androidx.core:core-splashscreen@1.2.0-rc01

androidx.core:core-viewtree@1.0.0

androidx.core:core@1.17.0

androidx.credentials:credentials-play-services-auth@1.2.0-rc01

androidx.credentials:credentials@1.2.0-rc01

androidx.cursoradapter:cursoradapter@1.0.0

androidx.customview:customview-poolingcontainer@1.1.0

androidx.customview:customview@1.2.0

androidx.documentfile:documentfile@1.0.1

androidx.drawerlayout:drawerlayout@dynamic

androidx.dynamicanimation:dynamicanimation@1.1.0

androidx.emoji2:emoji2-views-helper@1.5.0

androidx.emoji2:emoji2@1.5.0

androidx.exifinterface:exifinterface@1.4.1

androidx.fragment:fragment-ktx@1.8.9

androidx.fragment:fragment@1.8.9

androidx.graphics:graphics-path@1.0.1

androidx.health.connect:connect-client@1.1.0-alpha03

androidx.interpolator:interpolator@1.0.0

androidx.legacy:legacy-support-core-utils@1.0.0

androidx.lifecycle:lifecycle-livedata-core-ktx@2.9.2

androidx.lifecycle:lifecycle-livedata-core@2.9.2

androidx.lifecycle:lifecycle-livedata@2.9.2

androidx.lifecycle:lifecycle-process@2.9.2

androidx.lifecycle:lifecycle-runtime-compose@2.9.2

androidx.lifecycle:lifecycle-runtime-ktx@2.9.2

androidx.lifecycle:lifecycle-runtime@2.9.2

androidx.lifecycle:lifecycle-viewmodel-ktx@2.9.2

androidx.lifecycle:lifecycle-viewmodel-savedstate@2.9.2

androidx.lifecycle:lifecycle-viewmodel@2.9.2

androidx.loader:loader@1.1.0

androidx.localbroadcastmanager:localbroadcastmanager@1.1.0

androidx.metrics:metrics-performance@1.0.0-beta01

androidx.print:print@1.0.0

androidx.privacysandbox.ads:ads-adservices-java@1.0.0-beta05

androidx.privacysandbox.ads:ads-adservices@1.0.0-beta05

androidx.profileinstaller:profileinstaller@1.4.1

androidx.recyclerview:recyclerview@1.4.0

androidx.room:room-runtime@2.7.0

androidx.room:room-rxjava2@2.7.0

androidx.savedstate:savedstate-compose@1.3.0

androidx.savedstate:savedstate-ktx@1.3.1

androidx.savedstate:savedstate@1.3.1

androidx.security:security-crypto@1.1.0

androidx.sqlite:sqlite-framework@2.5.1

androidx.sqlite:sqlite@2.5.1

androidx.startup:startup-runtime@1.2.0

androidx.tracing:tracing@1.3.0

androidx.transition:transition@1.7.0-alpha01

androidx.vectordrawable:vectordrawable-animated@1.2.0

androidx.vectordrawable:vectordrawable@1.2.0

androidx.versionedparcelable:versionedparcelable@1.2.1

androidx.viewpager2:viewpager2@1.1.0

androidx.viewpager:viewpager@1.1.0

androidx.webkit:webkit@1.4.0

com.google.android.material:material@1.9.0

com.google.dagger:dagger@2.45

org.jetbrains.kotlinx:kotlinx-coroutines-android@1.10.2

org.jetbrains.kotlinx:kotlinx-coroutines-core@1.10.2

org.jetbrains.kotlinx:kotlinx-coroutines-guava@1.7.1

org.jetbrains.kotlinx:kotlinx-coroutines-play-services@1.10.2

org.jetbrains.kotlinx:kotlinx-coroutines-reactive@1.7.3

org.jetbrains.kotlinx:kotlinx-coroutines-rx2@1.7.3

▶ Show all **714** Packages

⎘ **FILES**

▶ Show all **7663** files

© **2025 Mobile Security Framework - MobSF** | **Ajin Abraham** | **OpenSecurity**.   **Version** v4.4.3