APP SCORES

Security Score **46/100**

Trackers Detection **1/432**

FILE INFORMATION

File Name lyft-15-4-3-1682489344.apk

Size 127.74MB

MD5 6dc728aa585023deac6f6f9ba04bd6a3

SHA1 3d9354eb6738702be0c3e045aace8037f8f4cfc0

SHA256 8f09ae770b726a7189d879a414ad17eb6e6b1f73f6fb21cef4798576699246b9

APP INFORMATION

App Name Lyft

Package Name me.lyft.android

Main Activity me.lyft.android.ui.MainActivity

Target SDK 31 Min SDK 23 Max SDK

Android Version Name 15.4.3.1682489344

Android Version Code 1682489344

PLAYSTORE INFORMATION

Title Lyft

Score 4.289602 Installs 50,000,000+ Price 0 Android Version Support Category Maps & Navigation Play Store URL me.lyft.android

Developer Lyft, Inc., Developer ID 6629245766506578153

Developer Address None

Developer Website http://www.lyft.com

Developer Email support@lyft.com

Release Date Aug 28, 2012 Privacy Policy Privacy link

Description

Get where you’re going with Lyft.

Whether you’re catching a flight, going out for the night, commuting to the office, or running errands in a rush, the Lyft app offers you multiple ways to get there.

EASY TO USE
Enter your destination. See your route and ride cost up front. Choose Priority Pickup to get going quick. Boom. Done. Simple

CHOOSE YOUR WHEELS
Choose from Wait & Save, Priority Pickup, Bikes & Scooters, Lyft XL, Lyft Lux, Transit, or even Rentals.

AFFORDABLE RIDES
Our Wait & Save option helps you get around for less. And you can find the fastest public transit routes, too.

* Lyft ride types may vary by region. Check the app to see what is available in your city.
—
Prices vary based on market condition.

By downloading the app, you agree to allow Lyft to collect your device's language settings.

2 / 9

EXPORTED ACTIVITIES

View All

3 / 14

EXPORTED SERVICES

View All

3 / 12

EXPORTED RECEIVERS

View All

0 / 5

EXPORTED PROVIDERS

View All

SCAN OPTIONS

DECOMPILED CODE

SIGNER CERTIFICATE

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: O=Zimride Inc.
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-08-06 06:52:35+00:00
Valid To: 2037-07-31 06:52:35+00:00
Issuer: O=Zimride Inc.
Serial Number: 0x501f69b3
Hash Algorithm: sha1
md5: 204377075b1d9909ca6b466b01b3e221
sha1: 17d96c0e43a75b58a440f103a3abd18652f5a292
sha256: fa9a37543634357be088ee7e4f8cfdd13b5907b22e921a3d47453e66c45f3e04
sha512: 0bd1d0231e7187cace2184e1f93610d68a1e30bb2f5706911ddc6b8ba15b6f23c985441aa663c98685af245be45b876d1b952aa2226abb973e8e81b6baf64ff6
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 2430a017181ee559fd4324be07c2042188122895d5b836cd4cb9fa42876f2253
Found 1 unique certificates
```

APPLICATION PERMISSIONS

Search:

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.	
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.	
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.	
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.	
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.	
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.	

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.CHANGE_WIFI_MULTICAST_STATE	normal	allow Wi-Fi Multicast reception	Allows an application to receive packets not directly addressed to your device. This can be useful when discovering services offered nearby. It uses more power than the non-multicast mode.	
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.	

Showing 1 to 10 of 36 entries

Previous 1 2 3 4 Next

ANDROID API

Search:

API	FILES
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

BROWSABLE ACTIVITIES

Search:

ACTIVITY	INTENT
me.lyft.android.ui.MainActivity	**Schemes**: lyft://, geo://, https://, http://, me.lyft.android.braintree://, **Hosts:** lyft.bttn.io, lyft.com, www.lyft.com, account.lyft.com, ride.lyft.com, lyft.baywheels.com, lyft.biketownpdx.com, lyft.capitalbikeshare.com, lyft.citibikenyc.com, lyft.divvybikes.com, lyft.niceridemn.com, help.lyft.com, **Paths:** /ride, /round-up, /round-up/causes, /business-profile/complete, /business-profile, /business, /business-rewards-program, /debt, /organization-invite/accept, /rpw, /ride-program-welcome, /lastmile_qr_scan, /add-venmo, /manage-subscriptions, /gift-a-ride/invite, /bike-scooter-invite, /get-the-app, **Path Prefixes:** /invited/, /invite/, /i/, /dotw/, /deal-of-the-week/, /ride?, /ride-pass/, /memberships/, /manage-subscriptions/, /sbr/, /lastmile_station/, /lyftpass/, /lp/, /accept-membership-referral/, /cr/rides/, /authchallenge/passenger, /persistedchallenge, /family, /recover, /csl, /d/, /lostitem/, **Path Patterns:** /hc/.*/rider/.*,

Showing 1 to 1 of 1 entries

Previous 1 Next

NETWORK SECURITY

Search:

NO	SCOPE	SEVERITY	DESCRIPTION
No data available in table			

Showing 0 to 0 of 0 entries

Previous Next

CERTIFICATE ANALYSIS

HIGH	WARNING	INFO
0	2	1

Search:

TITLE	SEVERITY	DESCRIPTION
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 might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.
Signed Application	info	Application is signed with a code signing certificate

Showing 1 to 3 of 3 entries

Previous 1 Next

MANIFEST ANALYSIS

HIGH	WARNING	INFO	SUPPRESSED
1	9	0	0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable unpatched Android version Android 6.0-6.0.1, [minSdk=23]	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=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.	
3	**Activity-Alias** (me.lyft.android.ui.MainActivity_Share) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
4	**Service** (com.lyft.auth.RemoteAuthAndroidService) is Protected by a permission. **Permission:** com.lyft.android.prod.permission.auth.REQUEST_AUTHORIZATION_CODE **protectionLevel:** signature [android:exported=true]	info	A Service is found to be exported, but is protected by permission.	
5	**Service** (com.lyft.android.gcm.services.GcmService) 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	OPTIONS
6	**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.	
7	**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.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
8	**Broadcast Receiver** (androidx.work.impl.diagnostics.DiagnosticsReceiver) 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.	
9	**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 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	OPTIONS
10	**Broadcast Receiver** (com.google.firebase.iid.FirebaseInstanceIdReceiver) 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 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.	

Showing 1 to 10 of 11 entries

Previous 1 2 Next

</> CODE ANALYSIS

Search:

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
No data available in table					

Showing 0 to 0 of 0 entries

Previous Next

SHARED LIBRARY BINARY ANALYSIS

Search:

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libbugsnag-ndk.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.	**True** info The binary has the following fortified functions: ['__vsprintf_chk', '__read_chk', '__strcpy_chk', '__strlen_chk', '__strchr_chk', '__vsnprintf_chk', '__memmove_chk']	**True** info Symbols a stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	arm64-v8a/libbugsnag-plugin-android-anr.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.	**False** warning 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 a stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	arm64-v8a/libbugsnag-root-detection.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.	**False** warning 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 a stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	arm64-v8a/libclientlocalization.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.	**True** info The binary has the following fortified functions: ['__memmove_chk', '__strlen_chk', '__vsnprintf_chk']	**False** warning Symbols a available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64-v8a/libenvoy_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.	**True** info The binary has the following fortified functions: ['__strlen_chk', '__FD_SET_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__vsnprintf_chk', '__memmove_chk', '__read_chk']	**True** info Symbols a stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	arm64-v8a/libloop.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.	**True** info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	**True** info Symbols a stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	arm64-v8a/libmapbox-gl.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.	**True** info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__memset_chk', '__vsnprintf_chk', '__memmove_chk']	**True** info Symbols a stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
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.	**Partial RELRO** warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**False** warning 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 a stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	arm64-v8a/libTMXProfiling-6.3-81-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.	**True** info The binary has the following fortified functions: ['__memmove_chk', '__strchr_chk', '__strncpy_chk', '__fgets_chk', '__memcpy_chk', '__vsnprintf_chk', '__strlcpy_chk', '__read_chk', '__strlen_chk']	**True** info Symbols a stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	armeabi-v7a/libbugsnag-ndk.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.	**False** warning 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 a stripped.

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
App talks to a Firebase database	info	The app talks to Firebase database at https://lyftapp.firebaseio.com

Showing 1 to 1 of 1 entries

Previous 1 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.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.TAGS check SIM operator check possible ro.secure check
Compiler	r8

Showing 1 to 2 of 2 entries

Previous 1 Next

DEX	DETECTIONS
classes10.dex	Search: **FINDINGS** | **DETAILS** Compiler | r8 Showing 1 to 1 of 1 entries Previous 1 Next
classes2.dex	Search: **FINDINGS** | **DETAILS** Anti-VM Code | Build.FINGERPRINT check Build.MANUFACTURER check possible Build.SERIAL check Build.TAGS check Compiler | r8 Showing 1 to 2 of 2 entries Previous 1 Next

DEX	DETECTIONS
classes3.dex	Search: **FINDINGS** / **DETAILS** Anti-VM Code — Build.MANUFACTURER check Compiler — r8 Showing 1 to 2 of 2 entries Previous 1 Next
classes4.dex	Search: **FINDINGS** / **DETAILS** Compiler — r8 Showing 1 to 1 of 1 entries Previous 1 Next
classes5.dex	Search: **FINDINGS** / **DETAILS** Anti-VM Code — Build.MANUFACTURER check Compiler — r8 Showing 1 to 2 of 2 entries Previous 1 Next

DEX	DETECTIONS
classes6.dex	Search: **FINDINGS** / **DETAILS** 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 emulator file check Compiler: r8 Showing 1 to 2 of 2 entries Previous 1 Next
classes7.dex	Search: **FINDINGS** / **DETAILS** Compiler: r8 Showing 1 to 1 of 1 entries Previous 1 Next

DEX	DETECTIONS
classes8.dex	Search: FINDINGS / DETAILS Compiler / r8 Showing 1 to 1 of 1 entries Previous 1 Next
classes9.dex	Search: FINDINGS / DETAILS Compiler / r8 Showing 1 to 1 of 1 entries Previous 1 Next

Showing 1 to 10 of 12 entries

Previous 1 2 Next

BEHAVIOUR ANALYSIS

Search:

RULE ID	BEHAVIOUR	LABEL	FILES
No data available in table			

Showing 0 to 0 of 0 entries

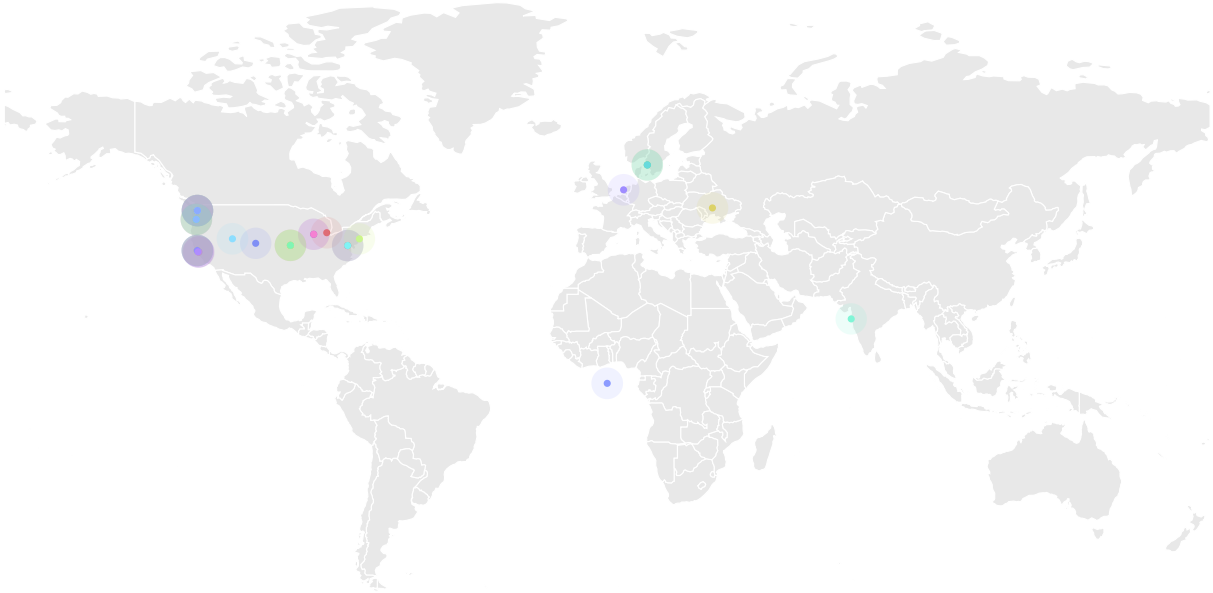
Previous Next

ABUSED PERMISSIONS

Top Malware Permissions	15/25	Other Common Permissions	9/44
android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.INTERNET, android.permission.READ_CONTACTS, android.permission.READ_EXTERNAL_STORAGE, android.permission.READ_PHONE_STATE, android.permission.VIBRATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.GET_ACCOUNTS, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE, android.permission.RECEIVE_BOOT_COMPLETED		android.permission.CALL_PHONE, android.permission.READ_CALENDAR, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, android.permission.CHANGE_WIFI_STATE, android.permission.FOREGROUND_SERVICE	

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:** 18.245.104.107 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api.braintreegateway.com	ok	**IP:** 159.242.242.193 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.888401 **Longitude:** -87.635101 **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:** 18.245.104.98 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api.maptiler.com	ok	**IP:** 104.17.245.40 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.sandbox.braintreegateway.com	ok	**IP:** 159.242.242.129 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.888401 **Longitude:** -87.635101 **View:** Google Map
api.usebutton.com	ok	**IP:** 52.33.174.243 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
apps.mapbox.com	ok	**IP:** 3.164.92.78 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
b.stats.paypal.com	ok	**IP:** 34.106.92.18 **Country:** United States of America **Region:** Utah **City:** Salt Lake City **Latitude:** 40.760780 **Longitude:** -111.891052 **View:** Google Map

Showing 1 to 10 of 52 entries

Previous 1 2 3 4 5 6 Next

URLS

Search:

URL	FILE
data::getsegmentposition(const data::pgraph::getdart(const data::getroadclass(pgraph::edge)	apktool_out/lib/arm64-v8a/libclientlocalization.so
data::getsegmentposition(const data::pgraph::getdart(const data::getroadclass(pgraph::edge)	apktool_out/lib/armeabi-v7a/libclientlocalization.so

URL	FILE
data::getsegmentposition(const data::pgraph::getdart(const data::getroadclass(pgraph::edge)	apktool_out/lib/x86/libclientlocalization.so
data::getsegmentposition(const data::pgraph::getdart(const data::getroadclass(pgraph::edge)	apktool_out/lib/x86_64/libclientlocalization.so
data::getsegmentposition(const data::pgraph::getdart(const data::getroadclass(pgraph::edge)	lib/arm64-v8a/libclientlocalization.so
data::getsegmentposition(const data::pgraph::getdart(const data::getroadclass(pgraph::edge)	lib/armeabi-v7a/libclientlocalization.so
data::getsegmentposition(const data::pgraph::getdart(const data::getroadclass(pgraph::edge)	lib/x86/libclientlocalization.so
data::getsegmentposition(const data::pgraph::getdart(const data::getroadclass(pgraph::edge)	lib/x86_64/libclientlocalization.so
data:text/html;charset=utf-8;base64,	com/lyft/android/payment/processors/services/chase/js/b.java
file:///android_asset/	com/masabi/justride/sdk/ui/configuration/screens/ticket/e.java

Showing 1 to 10 of 111 entries

Previous 1 2 3 4 5 … 12 Next

EMAILS

Search:

EMAIL	FILE
advisors@gabi.com	Android String Resource
ticket-banner-icon@3x.png	com/lyft/android/transit/visualticketing/services/l.java

Showing 1 to 2 of 2 entries

Previous 1 Next

TRACKERS

Search:

TRACKER NAME	CATEGORIES	URL
Bugsnag	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/207

Showing 1 to 1 of 1 entries

Previous 1 Next

POSSIBLE HARDCODED SECRETS

▼ Showing all **79** secrets

"face_auth_tos_info_menu_button" : "Info"
"profile_edit_screen_private_settings_pronouns_title" : "Pronombres"
"chat_session_failed_retry_button" : "輕點以重試"
"face_auth_selfie_guidance_menu_item" : "Pourboires"
"chat_session_survey_screen_submit_button" : "Envoyer"
"instabug_key" : "8667667c97b39ae4f5b825209e4cc5f2"
"face_auth_selfie_guidance_menu_item" : "Consejos"
"profile_edit_screen_private_settings_pronouns_title" : "Pronomes"

"android_backup_api_key" : "AEdPqrEAAAAIg8ZLhCeZA8kFNITnW3KPOuMExjAdGZsy5D_-Rw"
"firebase_database_url" : "https://lyftapp.firebaseio.com"
"face_auth_dl_info_description" : "Info"
"help_session_cancel" : "Cancel"
"face_auth_tos_info_menu_button" : "Información"
"chat_session_survey_screen_submit_button" : "Enviar"
"face_auth_completed_successfully" : "驗證成功"
"face_auth_camera_permission_alert_primary_button" : "開啟設定"
"face_auth_dl_info_description" : "Informações"
"chat_session_survey_screen_submit_button" : "Submit"
"profile_edit_screen_private_settings_pronouns_title" : "代詞"
"fieldwork_missing_possession_status" : "Missing"
"profile_edit_screen_private_settings_pronouns_title" : "Pronouns"
"face_auth_selfie_guidance_menu_item" : "Tips"
"fieldwork_lost_possession_status" : "Lost"
"fieldwork_unknown_possession_status" : "Desconhecido"
"face_auth_camera_permission_panel_primary_button" : "Allow"
"client_secret" : "ZtvLDz0n1-kJVwkIvxC4iSJ0yMvJydPq"
"face_auth_camera_permission_panel_primary_button" : "Permitir"
"help_session_cancel" : "Cancelar"
"google_maps_api_key" : "AIzaSyAuvqWhbywVvMJ3xoMbJf-FYDiLpoxdoqs"
"face_auth_panel_blurriness_dl_button_retry" : "Reprendre"
"profile_edit_screen_private_settings_pronouns_title" : "Pronoms"
"face_auth_panel_blurriness_dl_button_retry" : "Retake"
"face_auth_selfie_guidance_menu_item" : "Dicas"
"fieldwork_missing_possession_status" : "Manquant"
"face_auth_camera_permission_panel_secondary_button" : "現在還不要"
"face_auth_tos_info_menu_button" : "Informações"
"fieldwork_unknown_possession_status" : "Unknown"
"help_session_retry" : "Retry"
"fieldwork_unknown_possession_status" : "Desconocido"
"passenger_x_r4o_rider_selection_header_tooltip_firt_time_user" : "要變更乘客嗎？"
"fieldwork_lost_possession_status" : "Perdu"
"fieldwork_unknown_possession_status" : "Inconnu"
"fieldwork_lost_possession_status" : "Perdido"
"fieldwork_missing_possession_status" : "Falta"
"face_auth_camera_permission_panel_primary_button" : "Conceder"
"face_auth_camera_permission_panel_primary_button" : "Autoriser"

"face_auth_camera_permission_panel_title" : "要允許取用相機嗎？"
"help_session_cancel" : "Annuler"
"help_session_retry" : "Réessayer"
"face_auth_camera_permission_panel_primary_button" : "允許"
"face_auth_dl_info_description" : "資訊"
db5fce526403c5d0f68f9598eb2e19af57a3a55e
198c8973c0048dffd715fda2665fb73d
95857b61dc98903b2dd13065fa1ed972
c103703e120ae8cc73c9248622f3cd1e
x34mMawEUcCG8l95riWCOK+kAJYejVmdt44l6tzcyUc=
ade0a5b5-b8f3-46f9-a4e4-d92483740614
72b4ec1241a130bf46c35a20e424cbb4
a30b8ba3-f556-4c99-9f71-fdc839f99308
26584d407930d52f3d62ef77e729f1b4
3cedec86a663fb461d9c3a2059cef018
51b55c3d-6fa7-4242-87f9-83dde06bdd58
LoadSubflowV2RequestDTOTypeAdapterFactory
SRQznwSqEierDbkXg2yZTsse5Tb+l4Z4JiS6GvFclFE=
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
b227749a5773894765577ba51c993f70
907c169c-04c2-4ff0-ad21-f16f74e552cb
SubmitSubflowStepV2ResponseDTOTypeAdapterFactory
dd13d176ed9d642560698383cba6a0668ba75b53
ConfirmDockOrderingSessionV2RequestDTOTypeAdapterFactory
bb16099d-145d-43ff-af79-8bc92da0cb3a
e2719d58-a985-b3c9-781a-b030af78d30e
0e085944bd6623888ec8f9d2ad4ccf3e
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
dac079332b1d93a5cf118a2c74174fad
79edc3bcb1abd6e7be3bc5ae290c7319
9a04f079-9840-4286-ab92-e65be0885f95
49f946663a8deb7054212b8adda248c6
SubmitSubflowStepV2RequestDTOTypeAdapterFactory

A STRINGS

From APK Resource

▶ Show all **39329** strings

From Code

▶ Show all **111064** strings

From Shared Objects

apktool_out/lib/arm64-v8a/libbugsnag-ndk.so

▶ Show all **1231** strings

apktool_out/lib/arm64-v8a/libbugsnag-plugin-android-anr.so

▶ Show all **29** strings

apktool_out/lib/arm64-v8a/libbugsnag-root-detection.so

▶ Show all **10** strings

apktool_out/lib/arm64-v8a/libclientlocalization.so

▶ Show all **3257** strings

apktool_out/lib/arm64-v8a/libenvoy_jni.so

▶ Show all **24565** strings

apktool_out/lib/arm64-v8a/libloop.so

▶ Show all **825** strings

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

▶ Show all **4954** strings

apktool_out/lib/arm64-v8a/libtensorflowlite_jni.so

▶ Show all **1938** strings

apktool_out/lib/arm64-v8a/libTMXProfiling-6.3-81-jni.so

▶ Show all **457** strings

apktool_out/lib/armeabi-v7a/libbugsnag-ndk.so

▶ Show all **1226** strings

apktool_out/lib/armeabi-v7a/libbugsnag-plugin-android-anr.so

▶ Show all **29** strings

apktool_out/lib/armeabi-v7a/libbugsnag-root-detection.so

▶ Show all **10** strings

apktool_out/lib/armeabi-v7a/libclientlocalization.so

▶ Show all **3380** strings

apktool_out/lib/armeabi-v7a/libenvoy_jni.so

▶ Show all **25436** strings

apktool_out/lib/armeabi-v7a/libloop.so

▶ Show all **765** strings

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

▶ Show all **4938** strings

apktool_out/lib/armeabi-v7a/libtensorflowlite_jni.so

▶ Show all **2170** strings

apktool_out/lib/armeabi-v7a/libTMXProfiling-6.3-81-jni.so

▶ Show all **497** strings

apktool_out/lib/x86/libbugsnag-ndk.so

▶ Show all **1234** strings

apktool_out/lib/x86/libbugsnag-plugin-android-anr.so

▶ Show all **29** strings

apktool_out/lib/x86/libbugsnag-root-detection.so

▶ Show all **10** strings

apktool_out/lib/x86/libclientlocalization.so

▶ Show all **3353** strings

apktool_out/lib/x86/libenvoy_jni.so

▶ Show all **25408** strings

apktool_out/lib/x86/libloop.so

▶ Show all **793** strings

apktool_out/lib/x86/libmapbox-gl.so

▶ Show all **4892** strings

apktool_out/lib/x86/libtensorflowlite_jni.so

▶ Show all **2025** strings

apktool_out/lib/x86/libTMXProfiling-6.3-81-jni.so

▶ Show all **468** strings

apktool_out/lib/x86_64/libbugsnag-ndk.so

▶ Show all **1233** strings

apktool_out/lib/x86_64/libbugsnag-plugin-android-anr.so

▶ Show all **29** strings

apktool_out/lib/x86_64/libbugsnag-root-detection.so

▶ Show all **10** strings

apktool_out/lib/x86_64/libclientlocalization.so

▶ Show all **3363** strings

apktool_out/lib/x86_64/libenvoy_jni.so

▶ Show all **25430** strings

apktool_out/lib/x86_64/libloop.so

▶ Show all **812** strings

apktool_out/lib/x86_64/libmapbox-gl.so

▶ Show all **4893** strings

apktool_out/lib/x86_64/libtensorflowlite_jni.so

▶ Show all **2019** strings

apktool_out/lib/x86_64/libTMXProfiling-6.3-81-jni.so

▶ Show all **473** strings

lib/arm64-v8a/libbugsnag-ndk.so

▶ Show all **1231** strings

lib/arm64-v8a/libbugsnag-plugin-android-anr.so

▶ Show all **29** strings

lib/arm64-v8a/libbugsnag-root-detection.so

▶ Show all **10** strings

lib/arm64-v8a/libclientlocalization.so

▶ Show all **3257** strings

lib/arm64-v8a/libenvoy_jni.so

▶ Show all **24565** strings

lib/arm64-v8a/libloop.so

▶ Show all **825** strings

lib/arm64-v8a/libmapbox-gl.so

▶ Show all **4954** strings

lib/arm64-v8a/libtensorflowlite_jni.so

▶ Show all **1938** strings

lib/arm64-v8a/libTMXProfiling-6.3-81-jni.so

▶ Show all **457** strings

lib/armeabi-v7a/libbugsnag-ndk.so

▶ Show all **1226** strings

lib/armeabi-v7a/libbugsnag-plugin-android-anr.so

▶ Show all **29** strings

lib/armeabi-v7a/libbugsnag-root-detection.so

▶ Show all **10** strings

lib/armeabi-v7a/libclientlocalization.so

▶ Show all **3380** strings

lib/armeabi-v7a/libenvoy_jni.so

▶ Show all **25436** strings

lib/armeabi-v7a/libloop.so

▶ Show all **765** strings

lib/armeabi-v7a/libmapbox-gl.so

▶ Show all **4938** strings

lib/armeabi-v7a/libtensorflowlite_jni.so

▶ Show all **2170** strings

lib/armeabi-v7a/libTMXProfiling-6.3-81-jni.so

▶ Show all **497** strings

lib/x86/libbugsnag-ndk.so

▶ Show all **1234** strings

lib/x86/libbugsnag-plugin-android-anr.so

▶ Show all **29** strings

lib/x86/libbugsnag-root-detection.so

▶ Show all **10** strings

lib/x86/libclientlocalization.so

▶ Show all **3353** strings

lib/x86/libenvoy_jni.so

▶ Show all **25408** strings

lib/x86/libloop.so

▶ Show all **793** strings

lib/x86/libmapbox-gl.so

▶ Show all **4892** strings

lib/x86/libtensorflowlite_jni.so

▶ Show all **2025** strings

lib/x86/libTMXProfiling-6.3-81-jni.so

▶ Show all **468** strings

lib/x86_64/libbugsnag-ndk.so

▶ Show all **1233** strings

lib/x86_64/libbugsnag-plugin-android-anr.so

▶ Show all **29** strings

lib/x86_64/libbugsnag-root-detection.so

▶ Show all **10** strings

lib/x86_64/libclientlocalization.so

▶ Show all **3363** strings

lib/x86_64/libenvoy_jni.so

▶ Show all **25430** strings

lib/x86_64/libloop.so

▶ Show all **812** strings

lib/x86_64/libmapbox-gl.so

▶ Show all **4893** strings

lib/x86_64/libtensorflowlite_jni.so

▶ Show all **2019** strings

lib/x86_64/libTMXProfiling-6.3-81-jni.so

▶ Show all **473** strings

ACTIVITIES

▼ Showing all **9** activities
me.lyft.android.ui.MainActivity
com.google.android.gms.common.api.GoogleApiActivity
com.masabi.justride.sdk.ui.features.universalticket.UniversalTicketActivity
com.masabi.justride.sdk.ui.features.ticket.TicketActivity
com.masabi.justride.sdk.ui.features.ticket_info.TicketInfoActivity
com.google.android.play.core.common.PlayCoreDialogWrapperActivity
com.google.android.gms.auth.api.signin.internal.SignInHubActivity
androidx.compose.ui.tooling.PreviewActivity
androidx.car.app.CarAppPermissionActivity

SERVICES

▼ Showing all **14** services
com.lyft.auth.RemoteAuthAndroidService
com.lyft.android.gcm.services.GcmService

com.google.android.datatransport.runtime.scheduling.jobscheduling.JobInfoSchedulerService
com.google.android.datatransport.runtime.backends.TransportBackendDiscovery
com.google.mlkit.common.internal.MlKitComponentDiscoveryService
androidx.room.MultiInstanceInvalidationService
androidx.work.impl.background.systemalarm.SystemAlarmService
androidx.work.impl.background.systemjob.SystemJobService
androidx.work.impl.foreground.SystemForegroundService
com.google.android.gms.auth.api.signin.RevocationBoundService
com.lyft.android.passengerx.ridebuzzerv2.service.RideBuzzerLyftService
com.google.firebase.components.ComponentDiscoveryService
com.google.firebase.messaging.FirebaseMessagingService
com.lyft.android.appservice.ForegroundService

RECEIVERS

▼ Showing all **12** receivers
androidx.profileinstaller.ProfileInstallReceiver
com.google.android.datatransport.runtime.scheduling.jobscheduling.AlarmManagerSchedulerBroadcastReceiver
androidx.work.impl.utils.ForceStopRunnable$BroadcastReceiver
androidx.work.impl.background.systemalarm.ConstraintProxy$BatteryChargingProxy
androidx.work.impl.background.systemalarm.ConstraintProxy$BatteryNotLowProxy
androidx.work.impl.background.systemalarm.ConstraintProxy$StorageNotLowProxy
androidx.work.impl.background.systemalarm.ConstraintProxy$NetworkStateProxy
androidx.work.impl.background.systemalarm.RescheduleReceiver
androidx.work.impl.background.systemalarm.ConstraintProxyUpdateReceiver
androidx.work.impl.diagnostics.DiagnosticsReceiver
com.google.firebase.iid.FirebaseInstanceIdReceiver
androidx.car.app.notification.CarAppNotificationBroadcastReceiver

PROVIDERS

▼ Showing all **5** providers

androidx.car.app.connection.provider
androidx.startup.InitializationProvider
androidx.core.content.FileProvider
com.google.mlkit.common.internal.MlKitInitProvider
com.google.firebase.provider.FirebaseInitProvider

LIBRARIES

▼ Showing all **1** libraries
org.apache.http.legacy

SBOM

FILES

▶ Show all **12015** files