



ANDROID STATIC ANALYSIS REPORT



 BIXI (2025.33.3.1757612536)

File Name:

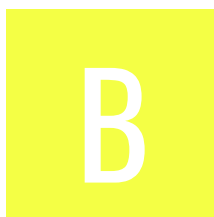
base.apk

Package Name: com.eightd.biximobile

Scan Date: Nov. 12, 2025, 6:55 p.m.






App Security Score: 53/100 (MEDIUM RISK)

Grade:



Trackers Detection: 3/432

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
1	20	3	2	1

FILE INFORMATION

File Name: base.apk

Size: 67.17MB

MD5: 6b6381f004b5ba12c9dbb9f05e388d07

SHA1: 12f4851aabb4d916acf607367f742717cf10f22

SHA256: 0be5f99e3a3eee389a6d10f75b529bfd0e1f8ce3441386f1a40ecea9151bf11

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

APP COMPONENTS

Activities: 40

Services: 13

Receivers: 6

Providers: 5
Exported Activities: 4
Exported Services: 2
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

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: 263b11d0be409636afc63a4790bf6116358d0b51cd71d6e4ea92d3376a158f59e26ef084a5321bd48da9868dcd4d60fc4b364cf90a4fd6c87b74dbe65f5e3b9a
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 937ee6d8c9eab07f366eb98d09734a921d5fb9e33e756d9596f53e4aee3ca7b1
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.health.WRITE_DISTANCE	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
android.permission.health.WRITE_EXERCISE	unknown	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.eightd.biximobile.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
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
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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
com.eightd.biximobile.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.ACCESS_AD_SERVICES_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.
android.permission.ACCESS_AD_SERVICES_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.

APKID ANALYSIS

FILE	DETAILS
------	---------

FILE	DETAILS	
lib/armeabi-v7a/libTMXProfiling-7.5-59-jni.so	FINDINGS	DETAILS
	Obfuscator	Arxan
lib/arm64-v8a/libTMXProfiling-7.5-59-jni.so	FINDINGS	DETAILS
	Obfuscator	Arxan
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.BOARD check Build.TAGS check
	Compiler	r8

FILE	DETAILS	
classes2.dex	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 possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8
classes3.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.MANUFACTURER check possible ro.secure check
	Compiler	r8

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
me.lyft.android.ui.main.SplashActivity	Schemes: bikesharemontreal://, @string/branch_uri://, https://, http://, Hosts: open, @string/branch_link_domain,

ACTIVITY	INTENT
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

NETWORK SECURITY

HIGH: 0 | WARNING: 0 | INFO: 0 | SECURE: 1

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+NyoXuWtQdX1al= Digest: SHA-256,Pin: f0KW/FtqTjs108NpYj42SrGvOB2PpxIVM8nWxjPqJGE= Digest: SHA-256,Pin: 47DEQpj8HBSa+/TImW+5JCeuQeRkm5NMpJWZG3hSuFU= Digest: SHA-256]

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 9 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	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.
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.
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 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.
6	Service (androidx.health.platform.client.impl.sdk.service.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.
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 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
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 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.
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.
11	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.

</> CODE ANALYSIS

HIGH: 0 | WARNING: 8 | INFO: 2 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/engine/g.java com/lyft/android/cardscanner/plugins/unidirectional/CardScannerPlugin.java com/lyft/android/cardscanner/plugins/unidirectional/overlay/CardScannerOverlayPlugin.java com/lyft/android/cardscanner/services/training/a.java com/lyft/android/experiments/b.java com/lyft/android/payment/ui/plugins/cardscan/CardScannerFullScreenPlugin.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/lyft/android/polaris/emailverification/plugins/mfa/ MfaEmailVerificationPlugin.java com/lyft/android/polaris/forgot/password/plugins/success/a.java com/lyft/android/polaris/login/plugins/screen/LoginScreenPlugin.java com/lyft/android/polaris/login/plugins/screen/f.java com/lyft/android/polaris/login/plugins/screen/l.java com/mapbox/common/PlatformHttpService.java com/mapbox/common/geofencing/GeofencingPropertiesKeys.java com/mapbox/common/location/LocationUpdatesReceiver.java com/mapbox/maps/ThreadChecker.java io/bitdrift/capture/providers/Field.java j6/c.java j6/l.java jl/b.java kl/c.java me/lyft/android/DeepLinkController.java me/lyft/android/api/model/ValidatePasswordStrengthRequest.java me/lyft/android/api/model/VerifyCredentialsRequest.java me/lyft/android/api/motivateLayer/ApiService.java me/lyft/android/config/PolarisConfig.java me/lyft/android/constants/EndpointsConsts.java me/lyft/android/constants/RemoteConfigConstants.java me/lyft/android/constants/ViolationConsts.java me/lyft/android/helpers/BffScreenFactory.java me/lyft/android/models/GroupRideProduct.java me/lyft/android/networking/PolarisHeadersInterceptor.java me/lyft/android/prefs/SignUpPreferences.java me/lyft/android/ui/login/LoginActivity.java me/lyft/android/ui/registration/PurchaseProductBundle.java me/lyft/android/ui/registration/payment/PaymentActivity.java me/lyft/android/ui/registration/signup/SignUpActivity.java me/lyft/android/ui/reward/RewardsActivity.java pb/api/endpoints/oauth2/access_token/CreateAccessTokenErrorDTO.java pb/api/endpoints/oauth2/access_token/CreateAccessTokenRequestDTO.java pb/api/endpoints/oauth2/access_token/RevokeAccessToken

NO	ISSUE	SEVERITY	STANDARDS	FILES
				<p>kenRequestDTO.java</p> <p>pb/api/endpoints/oauth2/access_token/RevokeAccessTo</p> <p>kenResponseDTO.java</p> <p>pb/api/endpoints/signed_url/SignURLRequestDTO.java</p> <p>pb/api/endpoints/signed_url/SignURLResponseDTO.java</p> <p>pb/api/endpoints/v1/banners/PostInAppBannerEventReq</p> <p>uestDTO.java</p> <p>pb/api/endpoints/v1/banners/PostInAppBannerEventRes</p> <p>ponseDTO.java</p> <p>pb/api/endpoints/v1/banners/ReadInAppBannersReques</p> <p>tDTO.java</p> <p>pb/api/endpoints/v1/banners/ReadInAppBannersRespon</p> <p>seDTO.java</p> <p>pb/api/endpoints/v1/client_urls/ShouldAllowOpenReque</p> <p>stDTO.java</p> <p>pb/api/endpoints/v1/client_urls/ShouldAllowOpenRespo</p> <p>nseDTO.java</p> <p>pb/api/endpoints/v1/inappmessaging/RenderInAppMess</p> <p>agesRequestDTO.java</p> <p>pb/api/endpoints/v1/inappmessaging/RenderInAppMess</p> <p>agesResponseDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/BffPolarisFinalizeHPPPayme</p> <p>ntFailedDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/BffPolarisHPPErrorDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/BffPolarisHPPPaymentFaile</p> <p>dDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/BffPolarisHPPPurchasePay</p> <p>mentFailedDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/BffPolarisLogin2FAErrorDT</p> <p>O.java</p> <p>pb/api/endpoints/v1/lbs_bff/GetAsyncFullscreenRequest</p> <p>DTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/GetAsyncFullscreenRespons</p> <p>eDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/GetFullscreenV3RequestDT</p> <p>O.java</p> <p>pb/api/endpoints/v1/lbs_bff/GetFullscreenV3ResponseD</p> <p>TO.java</p> <p>pb/api/endpoints/v1/lbs_bff/GetPolarisConfigRequestDT</p> <p>O.java</p> <p>pb/api/endpoints/v1/lbs_bff/GetPolarisConfigResponseD</p> <p>TO.java</p> <p>pb/api/endpoints/v1/lbs_bff/HRAMapItemPropertyDTO.j</p> <p>ava</p> <p>pb/api/endpoints/v1/lbs_bff/HppHeaderDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadActionRequestDTO.java</p>

NO	ISSUE	SEVERITY	STANDARDS	<p>pb/api/endpoints/v1/lbs_bff/ReadActionResponseDTO.java</p> <p>FILES</p> <p>pb/api/endpoints/v1/lbs_bff/ReadInRideMapInventoryRequestDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadInRideMapInventoryResponseDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadMapInventoryRequestDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadMapInventoryResponseDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadMapStyleRequestDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadMapStyleResponseDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadPanelRequestDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadPolarisFinalizeSignupRequestDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadPolarisFinalizeSignupResponseDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadPolarisHomePanelRequestDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadPolarisHomePanelResponseDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadPolarisHppCompleteTransactionRequestDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadPolarisHppCompleteTransactionResponseDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadPolarisHppPurchaseRequestDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadPolarisHppPurchaseResponseDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadPolarisHppRegisterRequestDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadPolarisHppRegisterResponseDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadPolarisHppUpdateBillingInfoRequestDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadPolarisHppUpdateBillingInfoResponseDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadPolarisInRideMapButtonsRequestDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadPolarisInRideMapButtonsResponseDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadPolarisInRidePanelRequestDTO.java</p> <p>pb/api/endpoints/v1/lbs_bff/ReadPolarisInRidePanelResponseDTO.java</p>

NO	ISSUE	SEVERITY	STANDARDS	FILES
				pb/api/endpoints/v1/lbs_bff/ReadPolarisLogin2FARequestDTO.java pb/api/endpoints/v1/lbs_bff/ReadPolarisLogin2FAResponseDTO.java pb/api/endpoints/v1/lbs_bff/ReadPolarisLogin2FAValidateRequestDTO.java pb/api/endpoints/v1/lbs_bff/ReadPolarisLogin2FAValidateResponseDTO.java pb/api/endpoints/v1/lbs_bff/ReadPolarisPasswordResetRequestDTO.java pb/api/endpoints/v1/lbs_bff/ReadPolarisPasswordResetResponseDTO.java pb/api/endpoints/v1/lbs_bff/ReadPolarisPreRideMapButtonsRequestDTO.java pb/api/endpoints/v1/lbs_bff/ReadPolarisPreRideMapButtonsResponseDTO.java pb/api/endpoints/v1/lbs_bff/ReadPolarisPreRidePanelRequestDTO.java pb/api/endpoints/v1/lbs_bff/ReadPolarisPreRidePanelResponseDTO.java pb/api/endpoints/v1/lbs_bff/ReadPolarisSearchRequestDTO.java pb/api/endpoints/v1/lbs_bff/ReadPolarisSearchResponseDTO.java pb/api/endpoints/v1/lbs_bff/ReadPolarisSignupEmailRequestCodeRequestDTO.java pb/api/endpoints/v1/lbs_bff/ReadPolarisSignupEmailRequestCodeResponseDTO.java pb/api/endpoints/v1/lbs_bff/ReadPolarisSignupEmailVerifyRequestDTO.java pb/api/endpoints/v1/lbs_bff/ReadPolarisSignupEmailVerifyResponseDTO.java pb/api/endpoints/v1/lbs_bff/ReadProfileAccessMethodsListRequestDTO.java pb/api/endpoints/v1/lbs_bff/ReadProfileAccessMethodsListResponseDTO.java pb/api/endpoints/v1/lbs_bff/ReadRideMutationRequestDTO.java pb/api/endpoints/v1/lbs_bff/ReadRideMutationResponseDTO.java pb/api/endpoints/v1/lbs_bff/ReadRideMutationTrackImpressionRequestDTO.java pb/api/endpoints/v1/lbs_bff/ReadRideMutationTrackImpressionResponseDTO.java pb/api/endpoints/v1/lbs_bff/SearchResultItemDTO.java pb/api/endpoints/v1/lbs_bff/ServerActionsDTO.java

NO	ISSUE	SEVERITY	STANDARDS	pb/api/endpoints/v1/lbs_bff/UpdateProfileAccessMethodRequestDTO.java pb/api/endpoints/v1/lbs_bff/UpdateProfileAccessMethodResponseDTO.java pb/api/endpoints/v1/locations/IngestLocationsRequestDTO.java pb/api/endpoints/v1/locations/IngestLocationsResponseDTO.java pb/api/endpoints/v1/paydisputes/GetCardScanAssetsRequestDTO.java pb/api/endpoints/v1/paydisputes/GetCardScanAssetsResponseDTO.java pb/api/endpoints/v1/paydisputes/GetCardScanBeginRequestDTO.java pb/api/endpoints/v1/paydisputes/GetCardScanBeginResponseDTO.java pb/api/endpoints/v1/scoped_urls/GenerateScopedUrlRequestDTO.java pb/api/endpoints/v1/scoped_urls/GenerateScopedUrlResponseDTO.java pb/api/endpoints/v1/user_inbox/UserInboxMessageCTADTO.java pb/api/endpoints/v1/user_inbox/UserInboxMessageDTO.java pb/api/endpoints/v1/user_inbox/UserInboxNotificationCardCTADTO.java pb/api/models/last_mile_event_attributes/LastMileErrorAlertUXDTO.java pb/api/models/last_mile_event_attributes/LastMileManualEntrySubmitButtonUXDTO.java pb/api/models/last_mile_event_attributes/LastMileQrScanManualEntryTooltipUXDTO.java pb/api/models/last_mile_event_attributes/LastMileQrScanTorchButtonUXDTO.java pb/api/models/last_mile_event_attributes/LastMileScreenManualEntryUXDTO.java pb/api/models/last_mile_event_attributes/LastMileScreenQrScanUXDTO.java pb/api/models/last_mile_event_attributes/LastMileStationScanButtonUXDTO.java pb/api/models/oauth2/access_token/OAuth2TokenDTO.java pb/api/models/oauth2/access_token/PromptActionDTO.java pb/api/models/v1/banners/InAppBannerDTO.java pb/api/models/v1/banners/InAppMessageBaseDTO.java pb/api/models/v1/banners/InAppMessageDetailDTO.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				pb/api/models/v1/banners/InAppMessageIdDTO.java pb/api/models/v1/banners/LastMileContextDTO.java pb/api/models/v1/banners/PlacementContextDTO.java pb/api/models/v1/banners/RiderPlaceSearchScreenContextDTO.java pb/api/models/v1/banners/UpcomingFlightContextDTO.java pb/api/models/v1/canvas/AccessibilityDTO.java pb/api/models/v1/canvas/AccidentsReportDateTimePickerDTO.java pb/api/models/v1/canvas/AccidentsReportElementDTO.java pb/api/models/v1/canvas/ActionDTO.java pb/api/models/v1/canvas/AlertDTO.java pb/api/models/v1/canvas/AlignmentDTO.java pb/api/models/v1/canvas/AnimationDTO.java pb/api/models/v1/canvas/AnimationsDTO.java pb/api/models/v1/canvas/AttributeLayoutDTO\$SizeDTO\$FillDTO.java pb/api/models/v1/canvas/AttributeLayoutDTO\$SizeDTO\$FixedDTO.java pb/api/models/v1/canvas/AttributeLayoutDTO\$SizeDTO\$WrapDTO.java pb/api/models/v1/canvas/AttributeLayoutDTO.java pb/api/models/v1/canvas/BoxLayoutDTO\$SizeDTO\$FillDTO.java pb/api/models/v1/canvas/BoxLayoutDTO\$SizeDTO\$FixedDTO.java pb/api/models/v1/canvas/BoxLayoutDTO\$SizeDTO\$WrapDTO.java pb/api/models/v1/canvas/BoxLayoutDTO.java pb/api/models/v1/canvas/BulletedListDTO.java pb/api/models/v1/canvas/CallDTO.java pb/api/models/v1/canvas/CapabilitiesDTO.java pb/api/models/v1/canvas/CarDamageSelectorDTO.java pb/api/models/v1/canvas/CarouselDTO.java pb/api/models/v1/canvas/CheckboxDTO.java pb/api/models/v1/canvas/CircularButtonDTO.java pb/api/models/v1/canvas/CircularMeterDTO.java pb/api/models/v1/canvas/ClearErrorsDTO.java pb/api/models/v1/canvas/CombinedIconDTO.java pb/api/models/v1/canvas/CommandDTO\$CapabilitiesDTO.java pb/api/models/v1/canvas/CompletedDTO.java pb/api/models/v1/canvas/ConstraintDTO\$AndroidDTO\$AnchorDTO\$HorizontalDTO.java pb/api/models/v1/canvas/ConstraintDTO\$AndroidDTO\$

NO	ISSUE	SEVERITY	STANDARDS	<p>AnchorDTO\$VerticalDTO.java</p> <p>pb/api/models/v1/canvas/ConstraintDTO\$AndroidDTO\$SizeDTO\$ConstantDTO.java</p> <p>pb/api/models/v1/canvas/ConstraintDTO\$AndroidDTO\$SizeDTO\$DimensionRatioDTO.java</p> <p>pb/api/models/v1/canvas/ConstraintDTO\$AndroidDTO\$SizeDTO\$MatchConstraintsDTO.java</p> <p>pb/api/models/v1/canvas/ConstraintDTO\$AndroidDTO\$SizeDTO\$MatchParentDTO.java</p> <p>pb/api/models/v1/canvas/ConstraintDTO\$AndroidDTO\$SizeDTO\$PercentParentDTO.java</p> <p>pb/api/models/v1/canvas/ConstraintDTO\$AndroidDTO\$SizeDTO\$WeightDTO.java</p> <p>pb/api/models/v1/canvas/ConstraintDTO\$AndroidDTO\$SizeDTO\$WrapContentDTO.java</p> <p>pb/api/models/v1/canvas/ConstraintDTO\$IOSDTO\$AnchorDTO\$HorizontalDTO.java</p> <p>pb/api/models/v1/canvas/ConstraintDTO\$IOSDTO\$AnchorDTO\$VerticalDTO.java</p> <p>pb/api/models/v1/canvas/ConstraintDTO\$IOSDTO\$SizeDTO\$ConstantDTO.java</p> <p>pb/api/models/v1/canvas/ConstraintDTO\$IOSDTO\$SizeDTO\$RelativeDTO.java</p> <p>pb/api/models/v1/canvas/ConstraintDTO\$WebDTO\$AnchorDTO\$HorizontalDTO.java</p> <p>pb/api/models/v1/canvas/ConstraintDTO\$WebDTO\$AnchorDTO\$VerticalDTO.java</p> <p>pb/api/models/v1/canvas/ConstraintDTO\$WebDTO\$SizeDTO\$ConstantDTO.java</p> <p>pb/api/models/v1/canvas/ConstraintDTO\$WebDTO\$SizeDTO\$MatchParentDTO.java</p> <p>pb/api/models/v1/canvas/ConstraintDTO\$WebDTO\$SizeDTO\$SizeToContentDTO.java</p> <p>pb/api/models/v1/canvas/ConstraintLayoutConstraintDTO.java</p> <p>pb/api/models/v1/canvas/ConstraintLayoutDTO.java</p> <p>pb/api/models/v1/canvas/CornersDTO.java</p> <p>pb/api/models/v1/canvas/CustomElementDTO.java</p> <p>pb/api/models/v1/canvas/CustomLayoutDTO.java</p> <p>pb/api/models/v1/canvas/DeepLinkDTO.java</p> <p>pb/api/models/v1/canvas/DismissDTO.java</p> <p>pb/api/models/v1/canvas/DisplayCardDTO.java</p> <p>pb/api/models/v1/canvas/DividerDTO.java</p> <p>pb/api/models/v1/canvas/DriverDeactivationElementDTO.java</p> <p>pb/api/models/v1/canvas/DropdownDTO.java</p>
----	-------	----------	-----------	---

NO	ISSUE	SEVERITY	STANDARDS	FILES
				pb/api/models/v1/canvas/EmojiSurveyDTO.java pb/api/models/v1/canvas/FeatureTipDTO.java pb/api/models/v1/canvas/FilePickerDTO.java pb/api/models/v1/canvas/FileUploadDTO.java pb/api/models/v1/canvas/FlowBuilderCustomElementDT O.java pb/api/models/v1/canvas/GradientLayoutDTO.java pb/api/models/v1/canvas/GridLayoutDTO.java pb/api/models/v1/canvas/HStackLayoutDTO\$SizeDTO\$Fi llDTO.java pb/api/models/v1/canvas/HStackLayoutDTO\$SizeDTO\$Fi xedDTO.java pb/api/models/v1/canvas/HStackLayoutDTO\$SizeDTO\$ WeightedDTO.java pb/api/models/v1/canvas/HStackLayoutDTO\$SizeDTO\$ WrapDTO.java pb/api/models/v1/canvas/HStackLayoutDTO.java pb/api/models/v1/canvas/HelpElementDTO.java pb/api/models/v1/canvas/HideDTO.java pb/api/models/v1/canvas/IOSLayoutOverridesDTO.java pb/api/models/v1/canvas/IconButtonDTO.java pb/api/models/v1/canvas/ImageDTO\$ImageModeDTO\$A ndroidDTO.java pb/api/models/v1/canvas/ImageDTO.java pb/api/models/v1/canvas/ImageSourceDTO.java pb/api/models/v1/canvas/InAppMessagingPinkLogoDT O.java pb/api/models/v1/canvas/InfoPanelDTO.java pb/api/models/v1/canvas/InlineCardDTO.java pb/api/models/v1/canvas/InlineDTO.java pb/api/models/v1/canvas/InputDateDTO.java pb/api/models/v1/canvas/InputSSNDTO.java pb/api/models/v1/canvas/LabelCapabilitiesDTO.java pb/api/models/v1/canvas/LabelDTO.java pb/api/models/v1/canvas/LayoutChildDTO.java pb/api/models/v1/canvas/ListLayoutDTO.java pb/api/models/v1/canvas/ListSectionDTO\$ItemDTO\$Con tentDTO\$CheckboxDTO.java pb/api/models/v1/canvas/ListSectionDTO\$ItemDTO\$Con tentDTO\$IconDTO.java pb/api/models/v1/canvas/ListSectionDTO\$ItemDTO\$Con tentDTO\$ImageDTO.java pb/api/models/v1/canvas/ListSectionDTO\$ItemDTO\$Con tentDTO\$RadioButtonDTO.java pb/api/models/v1/canvas/ListSectionDTO\$ItemDTO\$Con tentDTO\$SwitchDTO.java pb/api/models/v1/canvas/ListSectionDTO\$ItemDTO\$Con

NO	ISSUE	SEVERITY	STANDARDS	<div> <div>tentDTO\$TagDTO.java</div> <div>FILES</div> <div> pb/api/models/v1/canvas/ListSectionDTO.java pb/api/models/v1/canvas/LocationPickerDTO\$SearchDT O\$ByAddressOrNameDTO.java pb/api/models/v1/canvas/LocationPickerDTO\$SearchDT O\$OnMapWithCurrentDeviceLocationDTO.java pb/api/models/v1/canvas/LocationPickerDTO.java pb/api/models/v1/canvas/MapDTO.java pb/api/models/v1/canvas/PaddingDTO.java pb/api/models/v1/canvas/PhoneNumberFieldDTO.java pb/api/models/v1/canvas/PillButtonDTO.java pb/api/models/v1/canvas/PlaceholderElementDTO.java pb/api/models/v1/canvas/PromptPanelDTO.java pb/api/models/v1/canvas/PromptScreenDTO.java pb/api/models/v1/canvas/RadioButtonDTO.java pb/api/models/v1/canvas/RadioGroupDTO.java pb/api/models/v1/canvas/RotateDTO.java pb/api/models/v1/canvas/RoutePickerDTO.java pb/api/models/v1/canvas/ScreenDTO.java pb/api/models/v1/canvas/ScrollLayoutDTO\$SizeDTO\$Fill DTO.java pb/api/models/v1/canvas/ScrollLayoutDTO\$SizeDTO\$Fix edDTO.java pb/api/models/v1/canvas/ScrollLayoutDTO\$SizeDTO\$Wr apDTO.java pb/api/models/v1/canvas/ScrollLayoutDTO.java pb/api/models/v1/canvas/SegmentedControlDTO\$Segm entItemDTO\$DetailTextDTO.java pb/api/models/v1/canvas/SegmentedControlDTO\$Segm entItemDTO\$IconDTO.java pb/api/models/v1/canvas/SegmentedControlDTO\$Segm entItemDTO\$PrimaryTextDTO.java pb/api/models/v1/canvas/SegmentedControlDTO\$Segm entItemDTO\$TextDTO.java pb/api/models/v1/canvas/SegmentedControlDTO.java pb/api/models/v1/canvas/SelectDTO.java pb/api/models/v1/canvas/ShapeDTO.java pb/api/models/v1/canvas/SheetDTO.java pb/api/models/v1/canvas/ShimmerDTO.java pb/api/models/v1/canvas/ShowDTO.java pb/api/models/v1/canvas/SliderButtonDTO.java pb/api/models/v1/canvas/SpacerDTO.java pb/api/models/v1/canvas/StackLayoutConstraintDTO.jav a pb/api/models/v1/canvas/StackLayoutDTO.java pb/api/models/v1/canvas/SubmitFormDTO.java ... </div> </div>

NO	ISSUE	SEVERITY	STANDARDS	FILES
				pb/api/models/v1/canvas/SwitchDTO.java pb/api/models/v1/canvas/TabsDTO.java pb/api/models/v1/canvas/TagDTO.java pb/api/models/v1/canvas/TextAreaDTO.java pb/api/models/v1/canvas/TextButtonDTO.java pb/api/models/v1/canvas/TextFieldDTO.java pb/api/models/v1/canvas/TextStylingDTO.java pb/api/models/v1/canvas/TimelineDTO.java pb/api/models/v1/canvas/ToastDTO.java pb/api/models/v1/canvas/ToggleButtonDTO.java pb/api/models/v1/canvas/ToggleGroupDTO.java pb/api/models/v1/canvas/ToggleVisibilityDTO.java pb/api/models/v1/canvas/TooltipDTO.java pb/api/models/v1/canvas/UpdateAccessibilityDTO.java pb/api/models/v1/canvas/VStackLayoutDTO\$SizeDTO\$FixedDTO.java pb/api/models/v1/canvas/VStackLayoutDTO\$SizeDTO\$FixedDTO.java pb/api/models/v1/canvas/VStackLayoutDTO\$SizeDTO\$WeightedDTO.java pb/api/models/v1/canvas/VStackLayoutDTO\$SizeDTO\$WrapDTO.java pb/api/models/v1/canvas/VStackLayoutDTO.java pb/api/models/v1/canvas/ValidateDTO.java pb/api/models/v1/canvas/ValidationDTO\$BooleanDTO.java pb/api/models/v1/canvas/ValidationDTO\$CountDTO.java pb/api/models/v1/canvas/ValidationDTO\$RegexDTO.java pb/api/models/v1/canvas/ValidationRuleDTO.java pb/api/models/v1/canvas/VideoDTO.java pb/api/models/v1/canvas/WebviewDTO.java pb/api/models/v1/canvas/actions/common/CommonActionDTO.java pb/api/models/v1/canvas/actions/consumer_rentals/RentalBookingActionDTO.java pb/api/models/v1/canvas/actions/driver_deactivation/DriverDeactivationActionDTO.java pb/api/models/v1/canvas/actions/driver_deactivation/DriverDeactivationAnimationDTO.java pb/api/models/v1/canvas/actions/driver_deactivation/DriverDeactivationAnimationsDTO.java pb/api/models/v1/canvas/actions/earnings/EarningsActionDTO.java pb/api/models/v1/canvas/actions/edit_ride_toolkit/CancelFrictionActionDTO.java pb/api/models/v1/canvas/actions/edit_ride_toolkit/CancelReasonActionDTO.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				pb/api/models/v1/canvas/actions/edit_ride_toolkit/EditRideToolkitActionDTO.java pb/api/models/v1/canvas/actions/edit_ride_toolkit/SwitchRideActionDTO.java pb/api/models/v1/canvas/actions/flow_builder/FlowBuilderActionDTO.java pb/api/models/v1/canvas/actions/flow_builder/ValidationDTO\$CountDTO.java pb/api/models/v1/canvas/actions/flow_builder/ValidationDTO\$NonEmptySelectedOptionIdDTO.java pb/api/models/v1/canvas/actions/flow_builder/ValidationDTO\$RegexDTO.java pb/api/models/v1/canvas/actions/flow_builder/ValidationRuleDTO.java pb/api/models/v1/canvas/actions/help/HelpActionDTO.java pb/api/models/v1/canvas/actions/home/HomeActionDTO.java pb/api/models/v1/canvas/actions/in_app_messaging/InAppMessagingActionDTO.java pb/api/models/v1/canvas/actions/lbs_bff/LbsBffPanelActionDTO.java pb/api/models/v1/canvas/actions/lyft_history/LyftHistoryActionDTO.java pb/api/models/v1/canvas/actions/lyft_history/LyftHistoryAnimationDTO.java pb/api/models/v1/canvas/actions/lyft_history/LyftHistoryAnimationsDTO.java pb/api/models/v1/canvas/actions/lyft_pass/LyftPassEnrollmentChallengeActionDTO.java pb/api/models/v1/canvas/actions/map_feedback_tool/MapFeedbackToolSmartSurveyActionDTO.java pb/api/models/v1/canvas/actions/offer_overview/OfferOverviewActionDTO.java pb/api/models/v1/canvas/actions/pink/PinkMembershipsActionDTO.java pb/api/models/v1/canvas/driver_onboarding_custom_elements/DriverOnboardingCustomElementDTO.java pb/api/models/v1/challenges/CanvasChallengeDTO.java pb/api/models/v1/challenges/FormBuilderChallengeDTO.java pb/api/models/v1/challenges/NativeChallengeDTO.java pb/api/models/v1/challenges/PersistedChallengeHeaderMetaDTO.java pb/api/models/v1/challenges/WebChallengeDTO.java pb/api/models/v1/coordinates/CoordinatedDTO.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				pb/api/models/v1/core_ui/AccessibilityStringDTO.java pb/api/models/v1/core_ui/AnimationDTO.java pb/api/models/v1/core_ui/IconDTO.java pb/api/models/v1/core_ui/PictureDTO.java pb/api/models/v1/core_ui/TextStyleDTO.java pb/api/models/v1/core_ui/text_styles/v1/CoreTextStyleDTO.java pb/api/models/v1/core_ui/text_styles/v1/NewTextStyleDTO.java pb/api/models/v1/displaycomponents/AnytimeOrderingStartMatchingActionDTO.java pb/api/models/v1/displaycomponents/CancelRideActionDTO.java pb/api/models/v1/displaycomponents/CanvasActionDTO.java pb/api/models/v1/displaycomponents/CanvasAnimationTypeDTO.java pb/api/models/v1/displaycomponents/CanvasAnimationSDTO.java pb/api/models/v1/displaycomponents/ConfirmPickupLocationActionDTO.java pb/api/models/v1/displaycomponents/ContactDriverActionDTO.java pb/api/models/v1/displaycomponents/DeepLinkActionDTO.java pb/api/models/v1/displaycomponents/DismissActionDTO.java pb/api/models/v1/displaycomponents/DisplayComponentsActionDTO.java pb/api/models/v1/displaycomponents/EditLocationActionDTO.java pb/api/models/v1/displaycomponents/EditPickupActionDTO.java pb/api/models/v1/displaycomponents/ExpandPanelActionDTO.java pb/api/models/v1/displaycomponents/RedispatchRideActionDTO.java pb/api/models/v1/displaycomponents/RemoveGateCodeActionDTO.java pb/api/models/v1/displaycomponents/RequestSupportCallbackActionDTO.java pb/api/models/v1/displaycomponents/RiderPickupFeedbackActionDTO.java pb/api/models/v1/displaycomponents/ServerActionDTO.java pb/api/models/v1/displaycomponents/ShareRideActionDTO.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	pb/api/models/v1/displaycomponents/ShowComponentActionDTO.java pb/api/models/v1/displaycomponents/ShowEditRideDialogActionDTO.java pb/api/models/v1/displaycomponents/ShowNavigationActionDTO.java pb/api/models/v1/displaycomponents/ShowSafetyToolsActionDTO.java pb/api/models/v1/displaycomponents/SwitchRideActionDTO.java pb/api/models/v1/displaycomponents/VerifyResponseActionDTO.java pb/api/models/v1/displaycomponents/ZoomInActionDTO.java pb/api/models/v1/distance/DistanceDTO.java pb/api/models/v1/driver_location/DriverLocationDTO.java pb/api/models/v1/errors/StandardErrorDTO.java pb/api/models/v1/errors/last_mile_errors/LastMileApplePayPreAuthErrorDTO.java pb/api/models/v1/errors/last_mile_errors/LastMileDateOfBirthMissingErrorDTO.java pb/api/models/v1/errors/last_mile_errors/LastMileSafetyQuizErrorDTO.java pb/api/models/v1/errors/last_mile_errors/LastMileTutorialErrorDTO.java pb/api/models/v1/errors/last_mile_errors/LinkDisplayTermsEntryDTO.java pb/api/models/v1/errors/last_mile_errors/RideableTypeTermsOfServiceDTO.java pb/api/models/v1/errors/last_mile_errors/UnlockUnprocessableEntityErrorDTO.java pb/api/models/v1/inappmessaging/CanvasSurfaceDTO.java pb/api/models/v1/inappmessaging/ContentFeedDTO.java pb/api/models/v1/inappmessaging/DeepLinkDTO.java pb/api/models/v1/inappmessaging/InAppMessageUnitDTO.java pb/api/models/v1/inappmessaging/InterventionContentDTO.java pb/api/models/v1/inappmessaging/PlacedUnitDTO.java pb/api/models/v1/inappmessaging/PlacementDTO.java pb/api/models/v1/inappmessaging/RealTimeCanvasSurfaceDTO.java pb/api/models/v1/inappmessaging/RiderInboxCardsDTO

NO	ISSUE	SEVERITY	STANDARDS	FILES
				.java pb/api/models/v1/inappmessaging/custom/AccessoryBulletDTO.java pb/api/models/v1/inappmessaging/custom/CarouselCardDTO.java pb/api/models/v1/inappmessaging/custom/CarouselCardsDTO.java pb/api/models/v1/inappmessaging/custom/DetailPanelDisplayDTO.java pb/api/models/v1/inappmessaging/custom/DriverNotificationsCenterDTO.java pb/api/models/v1/inappmessaging/custom/DriverOnboardingHeaderDTO.java pb/api/models/v1/inappmessaging/custom/EmailModuleDTO.java pb/api/models/v1/inappmessaging/custom/HomeIncentiveDTO.java pb/api/models/v1/inappmessaging/custom/IncentiveIconDTO.java pb/api/models/v1/inappmessaging/custom/MessageMetadataDTO.java pb/api/models/v1/inappmessaging/custom/OnboardingHeaderDTO.java pb/api/models/v1/inappmessaging/custom/PriceGuidanceBannerMessageMetadataDTO.java pb/api/models/v1/inappmessaging/custom/RiderGreetingMessageDTO.java pb/api/models/v1/inappmessaging/custom/RiderHomeBodyContentDTO.java pb/api/models/v1/inappmessaging/custom/RiderHomeBodyMessageDTO.java pb/api/models/v1/inappmessaging/custom/RiderHomeHeaderContentDTO.java pb/api/models/v1/inappmessaging/custom/RiderHomeHeaderMessageDTO.java pb/api/models/v1/inappmessaging/custom/RiderHomePrioritizedContentDTO.java pb/api/models/v1/inappmessaging/custom/RiderHomePrioritizedMessageDTO.java pb/api/models/v1/inappmessaging/custom/RiderHomeScreenCustomModuleDTO.java pb/api/models/v1/inappmessaging/custom/RiderHomeScreenCustomModuleItemDTO.java pb/api/models/v1/inappmessaging/custom/RiderHomeScreenIncentiveModuleDTO.java pb/api/models/v1/inappmessaging/custom/RiderOfferSelectorPanelHeaderDTO.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				<p> pb/api/models/v1/inappmessaging/custom/RiderRateAndPayBelowStarRatingsContentDTO.java pb/api/models/v1/inappmessaging/custom/SectionCardDTO.java pb/api/models/v1/inappmessaging/custom/SectionDTO.java pb/api/models/v1/inappmessaging/custom/SkinsContextualBannerMessageMetadataDTO.java pb/api/models/v1/inappmessaging/custom/SponsorDisplayDetailsDTO.java pb/api/models/v1/inappmessaging/custom/SponsoredPreRequestDisplayCardMessageMetadataDTO.java pb/api/models/v1/inappmessaging/custom/SponsoredRidesBannerMessageMetadataDTO.java pb/api/models/v1/inappmessaging/custom/StandardCardDTO.java pb/api/models/v1/inappmessaging/custom/TextDTO.java pb/api/models/v1/inappmessaging/placements/CrossPlatformPlacementDTO.java pb/api/models/v1/inappmessaging/placements/DeepLinkSurfaceDTO.java pb/api/models/v1/inappmessaging/placements/DriverAppPlacementDTO.java pb/api/models/v1/inappmessaging/placements/DriverCrossScreenDTO.java pb/api/models/v1/inappmessaging/placements/DriverOfflineIdlelingDTO.java pb/api/models/v1/inappmessaging/placements/DriverOnlineIdlelingDTO.java pb/api/models/v1/inappmessaging/placements/DriverPreferencesDTO.java pb/api/models/v1/inappmessaging/placements/EarningsHomeDTO.java pb/api/models/v1/inappmessaging/placements/EmailModulePlacementDTO.java pb/api/models/v1/inappmessaging/placements/EvHubScreenDTO.java pb/api/models/v1/inappmessaging/placements/ExpressPayCashoutScreenDTO.java pb/api/models/v1/inappmessaging/placements/HomeScreenDTO.java pb/api/models/v1/inappmessaging/placements/InRideContentFeedBelowFoldDTO.java pb/api/models/v1/inappmessaging/placements/InRideScreenAbovePanelDTO.java </p>

NO	ISSUE	SEVERITY	STANDARDS	pb/api/models/v1/inappmessaging/placements/InRideScreenAbovePanelDTO.java pb/api/models/v1/inappmessaging/placements/LastMileAppPlacementDTO.java pb/api/models/v1/inappmessaging/placements/LastMileHomeScreenAbovePanelDTO.java pb/api/models/v1/inappmessaging/placements/LastMileInRideScreenAbovePanelDTO.java pb/api/models/v1/inappmessaging/placements/LastMileRideEndedScreenAbovePanelDTO.java pb/api/models/v1/inappmessaging/placements/LastMileSelectedVehicleScreenAbovePanelDTO.java pb/api/models/v1/inappmessaging/placements/MotivatorMapPanelDTO.java pb/api/models/v1/inappmessaging/placements/NotificationsCenterDTO.java pb/api/models/v1/inappmessaging/placements/OfferSelectorDTO.java pb/api/models/v1/inappmessaging/placements/OfflineHomeScreenDTO.java pb/api/models/v1/inappmessaging/placements/OnboardingChecklistViewHeaderDTO.java pb/api/models/v1/inappmessaging/placements/OnboardingPaymentScreenDTO.java pb/api/models/v1/inappmessaging/placements/OnboardingSubFlowScreenDTO.java pb/api/models/v1/inappmessaging/placements/PostOnboardingDTO.java pb/api/models/v1/inappmessaging/placements/PreMatchScreenAbovePanelDTO.java pb/api/models/v1/inappmessaging/placements/PrePickUpScreenAbovePanelDTO.java pb/api/models/v1/inappmessaging/placements/RateAndPayScreenAbovePaymentMethodDTO.java pb/api/models/v1/inappmessaging/placements/RateAndPayScreenBelowStarRatingsDTO.java pb/api/models/v1/inappmessaging/placements/RideReceiptEmailPromotionalSectionDTO.java pb/api/models/v1/inappmessaging/placements/RideableDTO.java pb/api/models/v1/inappmessaging/placements/RiderAppPlacementDTO.java pb/api/models/v1/inappmessaging/placements/RiderCrossScreenDTO.java pb/api/models/v1/inappmessaging/placements/RiderInboxNotificationCardDTO.java pb/api/models/v1/inappmessaging/placements/StationD
----	-------	----------	-----------	---

NO	ISSUE	SEVERITY	STANDARDS	FILES
				pb/api/models/v1/mapping/messaging/placements/stationb TO.java pb/api/models/v1/last_mile/CameraScreenConfiguration DTO.java pb/api/models/v1/last_mile/LastMileInterstitialPanelDTO .java pb/api/models/v1/last_mile/LastMileRideRequestValidati onDTO.java pb/api/models/v1/last_mile/LastMileRideableStationDTO \$ReservationOptionDTO.java pb/api/models/v1/last_mile/PreAuthDataDTO.java pb/api/models/v1/last_mile_rewards/CircularProgressInd icatorDTO.java pb/api/models/v1/last_mile_rewards/CountdownDTO.jav a pb/api/models/v1/last_mile_rewards/LastMileRewardsBo ostDTO.java pb/api/models/v1/last_mile_rewards/LastMileRewardsPa nelStatusMessageDTO.java pb/api/models/v1/last_mile_rewards/LeftContentDTO.jav a pb/api/models/v1/lat_lng/LatLngDTO.java pb/api/models/v1/lbs_bff/FilterMapButtonComponentDT O.java pb/api/models/v1/lbs_bff/GenericMapButtonComponent DTO.java pb/api/models/v1/lbs_bff/GroupRideMapButtonCompon entDTO.java pb/api/models/v1/lbs_bff/MapButtonAppearanceDTO.jav a pb/api/models/v1/lbs_bff/MapButtonComponentDTO.jav a pb/api/models/v1/lbs_bff/PanelComponentDTO.java pb/api/models/v1/lbs_bff/PanelDTO.java pb/api/models/v1/lbs_bff/PanelSpecificationDTO.java pb/api/models/v1/lbs_bff/PreRideMapButtonsDTO.java pb/api/models/v1/lbs_bff/RecenterMapButtonComponen tDTO.java pb/api/models/v1/lbs_bff/ToggleMapButtonComponent DTO.java pb/api/models/v1/lbs_bff/actions/ActionSpecificationDT O.java pb/api/models/v1/lbs_bff/actions/AddMapItemsFilterActi onDTO.java pb/api/models/v1/lbs_bff/actions/AlertActionDTO.java pb/api/models/v1/lbs_bff/actions/ApplePayPreauthActio nDTO.java

NO	ISSUE	SEVERITY	STANDARDS	pb/api/models/v1/lbs_bff/actions/AsyncFullScreenActionDTO.java pb/api/models/v1/lbs_bff/actions/CanvasDismissActionDTO.java pb/api/models/v1/lbs_bff/actions/CanvasSubmitActionDTO.java pb/api/models/v1/lbs_bff/actions/ChangeCanvasViewAppearanceActionDTO.java pb/api/models/v1/lbs_bff/actions/ChangeGenericMapItemAppearanceActionDTO.java pb/api/models/v1/lbs_bff/actions/ChangeTabActionDTO.java pb/api/models/v1/lbs_bff/actions/DateOfBirthEntryActionDTO.java pb/api/models/v1/lbs_bff/actions/DeepLinkActionDTO.java pb/api/models/v1/lbs_bff/actions/DriversLicenseEntryActionDTO.java pb/api/models/v1/lbs_bff/actions/EbikeListTutorialActionDTO.java pb/api/models/v1/lbs_bff/actions/ExitPlannedTripActionDTO.java pb/api/models/v1/lbs_bff/actions/FeatureTipActionDTO.java pb/api/models/v1/lbs_bff/actions/FullScreenActionDTO.java pb/api/models/v1/lbs_bff/actions/FullScreenFlowActionDTO.java pb/api/models/v1/lbs_bff/actions/FullScreenFlowNavigationActionDTO.java pb/api/models/v1/lbs_bff/actions/FullScreenV3DTO.java pb/api/models/v1/lbs_bff/actions/GroupRiderScanToUnlockActionDTO.java pb/api/models/v1/lbs_bff/actions/HapPageActionDTO.java pb/api/models/v1/lbs_bff/actions/ImageShareActionDTO.java pb/api/models/v1/lbs_bff/actions/LastMileRideRequestErrorActionDTO.java pb/api/models/v1/lbs_bff/actions/LinkShareActionDTO.java pb/api/models/v1/lbs_bff/actions/ListActionDTO.java pb/api/models/v1/lbs_bff/actions/LottieFullScreenAnimationActionDTO.java pb/api/models/v1/lbs_bff/actions/MapCameraUpdateActionDTO.java pb/api/models/v1/lbs_bff/actions/MapScreenFullActionDTO.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				pb/api/models/v1/lbs_bff/actions/MapItemsFilterActionD TO.java pb/api/models/v1/lbs_bff/actions/MembershipSalesActio nDTO.java pb/api/models/v1/lbs_bff/actions/NavigateToTransitScre enActionDTO.java pb/api/models/v1/lbs_bff/actions/PanelActionDTO.java pb/api/models/v1/lbs_bff/actions/ParkingToggleActionD TO.java pb/api/models/v1/lbs_bff/actions/PolarisTermsOfService ActionDTO.java pb/api/models/v1/lbs_bff/actions/PromptPanelActionDT O.java pb/api/models/v1/lbs_bff/actions/PromptScreenActionD TO.java pb/api/models/v1/lbs_bff/actions/PronounsEntryActionD TO.java pb/api/models/v1/lbs_bff/actions/QRScannerConfigDTO. java pb/api/models/v1/lbs_bff/actions/RefreshInRideMapActi onDTO.java pb/api/models/v1/lbs_bff/actions/RefreshLastMileRewar dsActionDTO.java pb/api/models/v1/lbs_bff/actions/RemoveMapItemsFilter ActionDTO.java pb/api/models/v1/lbs_bff/actions/RetryReasonDTO.java pb/api/models/v1/lbs_bff/actions/RideCancelActionDTO.j ava pb/api/models/v1/lbs_bff/actions/RideDidCompleteActio nDTO.java pb/api/models/v1/lbs_bff/actions/RideDropoffActionDTO .java pb/api/models/v1/lbs_bff/actions/RideLockActionDTO.ja va pb/api/models/v1/lbs_bff/actions/RideMutationActionDT O.java pb/api/models/v1/lbs_bff/actions/RideMutationRetryActi onDTO.java pb/api/models/v1/lbs_bff/actions/RideScanToUnlockActi onDTO.java pb/api/models/v1/lbs_bff/actions/RideToStationActionDT O.java pb/api/models/v1/lbs_bff/actions/RideUnlockActionDTO. java pb/api/models/v1/lbs_bff/actions/RideableReportIssueAc tionDTO.java pb/api/models/v1/lbs_bff/actions/RideableReserveAction

NO	ISSUE	SEVERITY	STANDARDS	FILES
				DTO.java pb/api/models/v1/lbs_bff/actions/RideableScanActionDT O.java pb/api/models/v1/lbs_bff/actions/RideableTutorialAction DTO.java pb/api/models/v1/lbs_bff/actions/RideableUnlockAction DTO.java pb/api/models/v1/lbs_bff/actions/ScanActionDTO.java pb/api/models/v1/lbs_bff/actions/ScanToUnlockActionD TO.java pb/api/models/v1/lbs_bff/actions/SelectDestinationActio nDTO.java pb/api/models/v1/lbs_bff/actions/SelectFilterCategoryActi onDTO.java pb/api/models/v1/lbs_bff/actions/SelectReservationOpti onActionDTO.java pb/api/models/v1/lbs_bff/actions/SelectRideableActionD TO.java pb/api/models/v1/lbs_bff/actions/SelectStationActionDT O.java pb/api/models/v1/lbs_bff/actions/SetLastMileRewardsUs erPreferenceActionDTO.java pb/api/models/v1/lbs_bff/actions/SetupGroupRideAction DTO.java pb/api/models/v1/lbs_bff/actions/SheetActionDTO.java pb/api/models/v1/lbs_bff/actions/ShowAccessMethodScr eenActionDTO.java pb/api/models/v1/lbs_bff/actions/ShowPaymentMethod PickerActionDTO.java pb/api/models/v1/lbs_bff/actions/ShowPostRideFareBre akDownActionDTO.java pb/api/models/v1/lbs_bff/actions/ShowPricingDetailsCo mponentActionDTO.java pb/api/models/v1/lbs_bff/actions/ShowRateAndPayActio nDTO.java pb/api/models/v1/lbs_bff/actions/SleepActionDTO.java pb/api/models/v1/lbs_bff/actions/StationReportIssueActi onDTO.java pb/api/models/v1/lbs_bff/actions/StationReserveActionD TO.java pb/api/models/v1/lbs_bff/actions/StationScanActionDTO. java pb/api/models/v1/lbs_bff/actions/StationTutorialActionD TO.java pb/api/models/v1/lbs_bff/actions/StrobeRideableLightsA ctionDTO.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				pb/api/models/v1/lbs_bff/actions/TermsOfServiceAcknowledgeActionDTO.java pb/api/models/v1/lbs_bff/actions/ToastActionDTO.java pb/api/models/v1/lbs_bff/actions/TooltipActionDTO.java pb/api/models/v1/lbs_bff/actions/TrackEventActionDTO.java pb/api/models/v1/lbs_bff/actions/UpdateBikeAngelsStoreTotalActionDTO.java pb/api/models/v1/lbs_bff/actions/UpdateMembershipPaymentMethodActionDTO.java pb/api/models/v1/lbs_bff/actions/ValidateCheckboxActionDTO.java pb/api/models/v1/lbs_bff/actions/global_actions/ServerActionCapabilitiesDTO.java pb/api/models/v1/lbs_bff/actions/global_actions/ServerActionDTO.java pb/api/models/v1/lbs_bff/actions/polaris_actions/GetAppAssActionDTO.java pb/api/models/v1/lbs_bff/actions/polaris_actions/OpenFavoritesScreenActionDTO.java pb/api/models/v1/lbs_bff/actions/polaris_actions/PinCodeUnlockActionDTO.java pb/api/models/v1/lbs_bff/actions/polaris_actions/PlanARideActionDTO.java pb/api/models/v1/lbs_bff/actions/polaris_actions/ScanToUnlockActionDTO.java pb/api/models/v1/lbs_bff/actions/polaris_actions/ShowGroupRidePurchaseFlowActionDTO.java pb/api/models/v1/lbs_bff/actions/polaris_actions/UpdateFavoriteStationsActionDTO.java pb/api/models/v1/lbs_bff/components/ActionButtonDTO.java pb/api/models/v1/lbs_bff/components/ActionButtonRowDTO.java pb/api/models/v1/lbs_bff/components/CategorySelectorDTO.java pb/api/models/v1/lbs_bff/components/EbikeListCapabilitiesDTO.java pb/api/models/v1/lbs_bff/components/EbikeListDTO.java pb/api/models/v1/lbs_bff/components/InAppBannersCapabilitiesDTO.java pb/api/models/v1/lbs_bff/components/InAppBannersDTO.java pb/api/models/v1/lbs_bff/components/InRideRideableDetailsDTO.java pb/api/models/v1/lbs_bff/components/InlineCanvasDTO.

NO	ISSUE	SEVERITY	STANDARDS	FILES
				<p>java pb/api/models/v1/lbs_bff/components/LastMileRewards BoostComponentCapabilitiesDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/LastMileRewards BoostComponentDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/LastMileRewards PanelStatusMessageComponentCapabilitiesDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/LastMileRewards PanelStatusMessageComponentDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/LightweightStatio nInformationCapabilitiesDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/LightweightStatio nInformationDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/LottieAnimationV iewDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/PaymentMethod DTO.java</p> <p>pb/api/models/v1/lbs_bff/components/PostRideSavings DTO.java</p> <p>pb/api/models/v1/lbs_bff/components/PostRideStatsDT O.java</p> <p>pb/api/models/v1/lbs_bff/components/PostRideUpsellID TO.java</p> <p>pb/api/models/v1/lbs_bff/components/PricingDetailsCap abilitiesDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/PricingDetailsDT O.java</p> <p>pb/api/models/v1/lbs_bff/components/PricingSummary CapabilitiesDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/PricingSummary DTO.java</p> <p>pb/api/models/v1/lbs_bff/components/QRScanFormCo mponentDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/QRScanFormICon ButtonDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/QRScanFormPillB uttonDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/RatingsFormCom ponentDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/RegulatoryWarni ngCapabilitiesDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/RegulatoryWarni ngDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/RichTextSubstitut ionComponentDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/RideMenuCapabil</p>

NO	ISSUE	SEVERITY	STANDARDS	FILES
				<p>itiesDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/RideMenuDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/RideStatusHeaderCapabilitiesDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/RideStatusHeaderDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/RideableActionButtonDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/RideableActionButtonRowDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/RideableMessageCapabilitiesDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/RideableMessageDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/RideableNameAndDetailsDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/StationActionButtonCapabilitiesDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/StationActionButtonDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/StationActionButtonRowDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/StationAvailabilityCapabilitiesDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/StationAvailabilityDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/StationMessageCapabilitiesDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/StationMessageDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/StationNameCapabilitiesDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/StationNameDTO.java</p> <p>pb/api/models/v1/lbs_bff/components/StepperDTO.java</p> <p>pb/api/models/v1/locations/BluetoothNetworkDTO.java</p> <p>pb/api/models/v1/locations/EddystoneBeaconDTO.java</p> <p>pb/api/models/v1/locations/EddystoneUIDDTO.java</p> <p>pb/api/models/v1/locations/IBeaconNetworkDTO.java</p> <p>pb/api/models/v1/locations/IngestionLocationDTO.java</p> <p>pb/api/models/v1/locations/IngestionNavigationLocationDTO.java</p> <p>pb/api/models/v1/locations/IngestionNavigationRouteLineDTO.java</p> <p>pb/api/models/v1/locations/WifiNetworkDTO.java</p> <p>pb/api/models/v2/BasicLocationDTO.java</p>

NO	ISSUE	SEVERITY	STANDARDS	FILES
				pb/api/models/v1/locations/v2/LocationFeaturesDTO.java pb/api/models/v1/locations/v2/LocationMetadataDTO.java pb/api/models/v1/locations/v2/LocationV2DTO.java pb/api/models/v1/locations/v2/MapMatchFeaturesDTO.java pb/api/models/v1/locations/v2/MapProfileDTO.java pb/api/models/v1/locations/v2/MediaLocationMetadataDTO.java pb/api/models/v1/locations/v2/NavigationLocationMetadataDTO.java pb/api/models/v1/locations/v2/NodeDTO.java pb/api/models/v1/locations/v2/PortableLocationDTO.java pb/api/models/v1/locations/v2/PortableLocationWithFeaturesDTO.java pb/api/models/v1/locations/v2/ProbableLocationDTO.java pb/api/models/v1/locations/v2/RideableLocationMetadataDTO.java pb/api/models/v1/locations/v2/RoadsideLocationMetadataDTO.java pb/api/models/v1/locations/v2/SegmentDTO.java pb/api/models/v1/locations/v2/SegmentPositionDTO.java pb/api/models/v1/locations/v2/SpotDTO.java pb/api/models/v1/locations/v2/StaticLocationMetadataDTO.java pb/api/models/v1/locations/v2/TransitLocationMetadataDTO.java pb/api/models/v1/locations/v2/TransportationApiLocationMetadataDTO.java pb/api/models/v1/locations/v2/UserLocationMetadataDTO.java pb/api/models/v1/memberships/RenewalCycleDTO.java pb/api/models/v1/memberships/SubscriptionBillingDetailsDTO.java pb/api/models/v1/money/MoneyDTO.java pb/api/models/v1/navigation/CongestionSectionV2DTO.java pb/api/models/v1/navigation/InternalWaypointDTO.java pb/api/models/v1/navigation/RangeV2DTO.java pb/api/models/v1/navigation/RouteSegmentV2DTO.java pb/api/models/v1/places/AddressDetailsDTO.java pb/api/models/v1/places/PlaceDTO.java

NO	ISSUE	SEVERITY	STANDARDS	pb/api/models/v1/polaris/ConsentChoiceDTO.java pb/api/models/v1/polaris/PolarisConsentDTO.java pb/api/models/v1/view/panel/HeaderBodyItemsDTO.java a pb/api/models/v1/view/presentation/components/CanvasComponentDTO.java pb/api/models/v1/view/presentation/components/ComponentDTO.java pb/api/models/v1/view/presentation/components/CustomComponentDTO.java pb/api/models/v1/view/primitives/RichTextDTO.java pb/api/models/v1/view/primitives/StyledRichTextDTO.java a pb/api/models/v1/view/primitives/TintedIconDTO.java rx/internal/schedulers/NewThreadWorker.java sb/a.java ul/a.java um/b.java wm/n.java wm/r0.java
				a7/d.java a7/k.java ac/a.java c6/d.java cb/f.java cb/z.java com/bumptechnology/glide/b.java com/bumptechnology/glide/j.java com/bumptechnology/glide/k.java com/bumptechnology/glide/load/data/b.java com/bumptechnology/glide/load/data/j.java com/bumptechnology/glide/load/data/l.java com/bumptechnology/glide/load/engine/DecodeJob.java com/bumptechnology/glide/load/engine/GlideException.java com/bumptechnology/glide/load/engine/e.java com/bumptechnology/glide/load/engine/j.java com/bumptechnology/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptechnology/glide/load/resource/bitmap/VideoDecoder.java com/bumptechnology/glide/load/resource/bitmap/a.java com/bumptechnology/glide/request/SingleRequest.java com/lexisnexisrisk/threatmetrix/tmxprofiling/eebbbee.java va com/lyft/android/camera/unidirectional/plugin/service/a

NO	ISSUE	SEVERITY	STANDARDS	FILES
				.java com/lyft/android/cardscanner/plugins/ui/d.java com/lyft/android/polaris/http/customtabs/services/f.java com/lyft/auth/LogoutService.java com/lyft/auth/g.java com/lyft/common/composition/a.java com/mapbox/common/AccessTokenInitializer.java com/mapbox/common/BaseMapboxInitializer.java com/mapbox/common/CoreInitializer.java com/mapbox/common/LifecycleMonitorAndroid.java com/mapbox/common/LifecycleService.java com/mapbox/common/LifecycleUtils.java com/mapbox/common/MapboxCommonLogger.java com/mapbox/common/MapboxMapsAndroidLogger.java com/mapbox/common/Reachability.java com/mapbox/common/RunloopErrorHandler.java com/mapbox/common/SettingsServiceHelper.java com/mapbox/common/TelemetrySystemUtils.java com/mapbox/common/ValueUtilsKt.java com/mapbox/common/location/LocationUpdatesReceiver.java com/mapbox/common/logger/MapboxLogger.java com/mapbox/common/module/okhttp/NetworkUsageListener.java com/mapbox/common/module/provider/MapboxModuleProvider.java com/mapbox/maps/FontUtils.java com/mapbox/maps/extension/style/layers/Layer.java com/mapbox/maps/extension/style/sources/Source.java com/mapbox/maps/plugin/locationcomponent/t.java com/usebutton/merchant/ButtonApiImpl.java com/usebutton/merchant/ButtonInternalImpl.java com/usebutton/merchant/ButtonRepositoryImpl.java com/usebutton/merchant/ButtonUtil.java com/usebutton/merchant/ConnectionManagerImpl.java com/usebutton/merchant/Event.java d3/f.java e2/b.java e6/a.java e7/a.java es/a.java f/g.java f3/b.java f6/d.java f6/e.java g2/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	g5/a.java g5/b.java g9/f.java g9/g2.java g9/q1.java gb/e.java h5/c0.java h5/e.java i/h.java i1/j0.java i2/a.java i6/a.java i9/g2.java i9/q3.java i9/w0.java io/bitdrift/capture/providers/MetadataProvider.java io/branch/referral/Branch.java io/branch/referral/BranchJsonConfig.java io/branch/referral/k.java io/branch/referral/q.java io/sentry/android/core/r.java io/sentry/android/core/s.java io/sentry/android/replay/ReplayIntegration.java io/sentry/android/replay/WindowManagerSpy.java io/sentry/l4.java j4/c.java j4/g.java j6/d.java k3/b.java k5/b.java k6/h.java k6/i.java l4/j.java l6/d.java l6/e.java l6/h.java l7/b.java m2/d.java m2/e.java m2/j.java m2/o.java m2/y.java m6/a.java m8/b.java m8/c.java m8/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				m8/h.java m8/i.java m8/s.java m8/t.java m8/u.java m8/v.java m8/w.java m8/x.java m8/y.java me/lyft/android/PolarisApplication.java me/lyft/android/helpers/UnlockBikeMethodHelperImpl.java me/lyft/android/ui/favorites/FavoritesFragment.java me/lyft/android/ui/menu/RideDetailFragment.java me/lyft/android/ui/qrscanner/QrScannerActivity.java n/f.java n2/a.java n6/c.java n6/f.java n6/v.java n6/w.java n7/h.java n9/a.java o7/i.java p/c0.java p/f1.java p/j.java p/l0.java p/n0.java p/r0.java p/t0.java p/x.java p2/f.java p2/k.java p3/a.java p6/f.java p9/a.java pb/q.java q2/f.java q2/h.java q2/i.java q2/j.java q2/k.java q2/m.java q2/n.java q2/p.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				q6/b.java q6/c.java q6/m.java q6/o.java q6/s.java q6/x.java q9/a.java qb/a0.java qb/c0.java qb/d0.java qb/l0.java qb/w.java qb/y.java qb/z.java qc/a.java r8/a.java r9/c.java rx/plugins/RxJavaHooks.java s1/a.java sa/a.java siftscience/android/AppStateCollector.java siftscience/android/DevicePropertiesCollector.java siftscience/android/Sift.java siftscience/android/SiftImpl.java siftscience/android/TaskManager.java siftscience/android/Uploader.java t8/a.java tb/l.java u6/a.java u6/i.java u8/a.java u9/g.java ua/f.java v2/f.java v2/j.java v4/a.java v8/k.java v8/l.java w2/d.java w4/a.java w6/p.java wc/d.java xc/k.java xq/f.java yc/a.java z8/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	i9/f8.java i9/j.java i9/o.java i9/u0.java t7/h.java t7/j.java t7/k.java t7/l.java t7/m.java t7/n.java tb/o.java
4	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	io/sentry/android/core/v0.java me/lyft/android/utis/PickImageUtils.java
5	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	me/lyft/android/utis/PickImageUtils.java
6	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/lyft/android/panel/ui/g.java
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	com/lexisnexisrisk/threatmetrix/tmxprofiling/fyyffyy.java com/mapbox/common/module/okhttp/WssBackend.java ec/f.java i9/y7.java lt/a.java lt/b.java me/lyft/android/dagger/SkabbardAppComponent.java mt/a.java wb/a.java wc/n.java wc/o.java
8	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	cb/f.java io/sentry/android/core/internal/util/n.java io/sentry/android/core/v0.java siftscience/android/DevicePropertiesCollector.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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
10	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	com/lexisnexisrisk/threatmetrix/tmxprofiling/eebeebb.java com/lexisnexisrisk/threatmetrix/tmxprofiling/fyyyyyf.java io/sentry/SentryOptions.java qc/a.java v8/a.java zb/k.java
11	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 i9/y7.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
----	---------------	----	-----	--------------	-------	-------	---------	---------	------------------

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libandroidx.graphics.path.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	arm64-v8a/libc++_shared.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>False high</p> <p>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 canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	arm64-v8a/libcapture.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>False high</p> <p>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 canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	arm64-v8a/libmapbox-common.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__vsnprintf_chk', '__memset_chk', '__read_chk', '__strchr_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64-v8a/libmapbox-maps.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__vsprintf_chk', '__strncpy_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	arm64-v8a/libentry-android.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__vsprintf_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	arm64-v8a/libentry.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__vsprintf_chk', '__read_chk', '__memmove_chk', '__strncpy_chk', '__strlen_chk', '__memcpy_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	arm64-v8a/libtensorflowlite_jni.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__vsprintf_chk', '__read_chk', '__strlen_chk', '__memmove_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	arm64-v8a/libTMXProfiling-7.5-59-jni.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions:</p> <p>['__strlen_chk', '__strncpy_chk', '__vsnprintf_chk', '__memcpy_chk', '__memmove_chk', '__memset_chk', '__strchr_chk', '__fgets_chk', '__read_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	armeabi-v7a/libandroidx.graphics.path.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	armeabi-v7a/libc++_shared.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>False high</p> <p>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 canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	armeabi-v7a/libcapture.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>False high</p> <p>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 canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	armeabi-v7a/libmapbox-common.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__vsprintf_chk', '__memset_chk', '__read_chk', '__strchr_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	armeabi-v7a/libmapbox-maps.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__vsprintf_chk', '__strncpy_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	armeabi-v7a/libentry-android.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__vsprintf_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	armeabi-v7a/libentry.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__vsprintf_chk', '__read_chk', '__memmove_chk', '__strncpy_chk', '__strlen_chk', '__memcpy_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	armeabi-v7a/libtensorflowlite_jni.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__vsprintf_chk', '__strlen_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	armeabi-v7a/libTMXProfiling-7.5-59-jni.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__strlen_chk', '__vsprintf_chk', '__memcpy_chk', '__memmove_chk', '__memset_chk', '__strchr_chk', '__fgets_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	x86/libandroidx.graphics.path.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	x86/libc++_shared.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>False high</p> <p>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 canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	x86/libcapture.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>False high</p> <p>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 canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	x86/libmapbox-common.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__vsnprintf_chk', '__memset_chk', '__read_chk', '__strchr_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	x86/libmapbox-maps.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__vsnprintf_chk', '__strncpy_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	x86/libsendry-android.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__vsprintf_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
25	x86/libsendry.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__vsprintf_chk', '__read_chk', '__memmove_chk', '__strncpy_chk', '__strlen_chk', '__memcpy_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
26	x86/libtensorflowlite_jni.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__vsprintf_chk', '__strlen_chk', '__memmove_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
27	x86/libTMXProfiling-7.5-59-jni.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions:</p> <p>['__strlen_chk', '__vsprintf_chk', '__memcpy_chk', '__memmove_chk', '__memset_chk', '__strchr_chk', '__fgets_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
28	x86_64/libandroidx.graphics.path.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
29	x86_64/libc++_shared.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>False high</p> <p>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 canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
30	x86_64/libcapture.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>False high</p> <p>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 canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
31	x86_64/libmapbox-common.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__vsnprintf_chk', '__memset_chk', '__read_chk', '__strchr_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
32	x86_64/libmapbox-maps.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__vsprintf_chk', '__strncpy_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
33	x86_64/libsendry-android.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__vsprintf_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
34	x86_64/libsendry.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__vsprintf_chk', '__read_chk', '__memmove_chk', '__strncpy_chk', '__strlen_chk', '__memcpy_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
35	x86_64/libtensorflowlite_jni.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>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.</p>	<p>True info</p> <p>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.</p>	<p>Full RELRO info</p> <p>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.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__vsprintf_chk', '__read_chk', '__strlen_chk', '__memmove_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
36	x86_64/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.	True info The binary has the following fortified functions: ['__strlen_chk', '__strncpy_chk', '__vsprintf_chk', '__memcpy_chk', '__memmove_chk', '__memset_chk', '__strchr_chk', '__fgets_chk', '__read_chk']	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	a6/d.java com/lyft/android/camera/unidirectional/plugin/service/Camera2Service.java com/mapbox/common/CoreInitializer.java io/sentry/SentryOptions.java io/sentry/android/core/AnrV2Integration.java io/sentry/android/core/k1.java io/sentry/android/core/v.java io/sentry/android/core/v0.java io/sentry/android/replay/ReplayCache.java io/sentry/android/replay/capture/BufferCaptureStrategy.java io/sentry/android/replay/capture/l.java io/sentry/cache/c.java io/sentry/cache/e.java io/sentry/l3.java io/sentry/s2.java io/sentry/u2.java io/sentry/w.java lk/d.java me/lyft/android/controllers/FileControllerImpl.java me/lyft/android/utills/OomExceptionHandler.java me/lyft/android/utills/PickImageUtils.java q5/h.java q5/q.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	a6/d.java com/airbnb/lottie/compose/h.java com/bumptech/glide/load/resource/bitmap/b.java com/lexisnexisrisk/threatmetrix/tmxprofiling/eebebeb.java com/lexisnexisrisk/threatmetrix/tmxprofiling/uuiuuu.java com/mapbox/common/PlatformStreamFactoryKt.java e6/a.java e6/b.java io/sentry/android/core/SentryPerformanceProvider.java io/sentry/android/replay/ReplayCache.java io/sentry/cache/b.java io/sentry/cache/c.java io/sentry/cache/e.java io/sentry/s2.java io/sentry/u2.java io/sentry/util/b.java io/sentry/w.java lk/c.java m2/e.java me/lyft/android/controllers/FileControllerImpl.java n6/h.java okio/Okio.java org/joda/time/tz/e.java p3/a.java q2/i.java q2/j.java q2/p.java q5/h.java xc/e.java z4/c.java
00012	Read data and put it into a buffer stream	file	io/sentry/cache/b.java io/sentry/cache/e.java io/sentry/s2.java io/sentry/util/b.java io/sentry/w.java p3/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/lyft/android/browser/widget/ui/WebBrowserView.java com/lyft/android/polaris/hpp/customtabs/services/PolarisCustomTabs.java com/lyft/android/polaris/hpp/customtabs/services/f.java com/lyft/android/rider/lastmile/bff/plugins/actions/handler/sync/e.java com/lyft/android/rider/lastmile/bff/plugins/panelitems/b.java com/usebutton/merchant/ButtonInternalImpl.java es/f.java i9/v4.java i9/y7.java io/branch/referral/Branch.java me/lyft/android/constants/AppConsts.java me/lyft/android/extensions/ExtensionsKt.java me/lyft/android/ui/invites/SocialIntentProvider.java me/lyft/android/ui/main/MainPresenter.java me/lyft/android/ui/takeover/TakeOverPresenter.java me/lyft/android/utls/AndroidUtils.java me/lyft/android/utls/DialogUtils.java me/lyft/android/views/WebViewActivity.java or/h.java
00024	Write file after Base64 decoding	reflection file	q5/q.java
00195	Set the output path of the recorded file	record file	com/lyft/android/camera/unidirectional/plugin/service/Camera2Service.java
00194	Set the audio source (MIC) and recorded file format	record	com/lyft/android/camera/unidirectional/plugin/service/Camera2Service.java
00197	Set the audio encoder and initialize the recorder	record	com/lyft/android/camera/unidirectional/plugin/service/Camera2Service.java
00007	Use absolute path of directory for the output media file path	file	com/lyft/android/camera/unidirectional/plugin/service/Camera2Service.java
00196	Set the recorded file format and output path	record file	com/lyft/android/camera/unidirectional/plugin/service/Camera2Service.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	a6/b.java com/bumptech/glide/load/data/j.java io/branch/referral/BranchViewHandler.java io/sentry/transport/d.java siftscience/android/Uploader.java
00029	Initialize class object dynamically	reflection	com/mapbox/common/module/provider/MapboxModuleProvider.java
00157	Instantiate new object using reflection, possibly used for dexClassLoader	reflection dexClassLoader	com/mapbox/common/module/provider/MapboxModuleProvider.java
00046	Method reflection	reflection	com/lyft/protocgenlyftandroid/androidnetworkinterfaces/adapters/ReflectiveTypeAdapter.java com/mapbox/common/module/provider/MapboxModuleProvider.java
00026	Method reflection	reflection	com/mapbox/common/module/provider/MapboxModuleProvider.java
00056	Modify voice volume	control	gp/c.java
00042	Query WiFi BSSID and scan results	collection wifi	com/lexisnexisrisk/threatmetrix/tmxprofiling/ebbebbe.java
00130	Get the current WIFI information	wifi collection	com/lexisnexisrisk/threatmetrix/tmxprofiling/ebbebbe.java
00123	Save the response to JSON after connecting to the remote server	network command	io/branch/referral/BranchViewHandler.java
00094	Connect to a URL and read data from it	command network	io/branch/referral/BranchViewHandler.java siftscience/android/Uploader.java
00108	Read the input stream from given URL	network command	i9/a5.java i9/d1.java io/branch/referral/BranchViewHandler.java siftscience/android/Uploader.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	i9/v4.java io/branch/referral/Branch.java me/lyft/android/ui/planride/mvp/PlanRidePresenter.java
00079	Hide the current app's icon	evasion	i/h.java
00147	Get the time of current location	collection location	i/h.java
00075	Get location of the device	collection location	i/h.java
00115	Get last known location of the device	collection location	com/lexisnexisrisk/threatmetrix/tmxprofiling/ebbbbb.java i/h.java
00159	Use accessibility service to perform action getting node info by text	accessibility service	me/lyft/android/controls/CustomPicker.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/lyft/android/rider/lastmile/bff/plugins/actions/handler/sync/e.java io/branch/referral/Branch.java me/lyft/android/extensions/ExtensionsKt.java me/lyft/android/utis/AndroidUtils.java or/h.java
00031	Check the list of currently running applications	reflection collection	com/mapbox/common/LifecycleUtils.java
00036	Get resource file from res/raw directory	reflection	com/mapbox/maps/plugin/f.java io/branch/referral/Branch.java me/lyft/android/utis/AndroidUtils.java p/r0.java
00065	Get the country code of the SIM card provider	collection	com/lexisnexisrisk/threatmetrix/tmxprofiling/ebeeeeee.java siftscience/android/DevicePropertiesCollector.java
00004	Get filename and put it to JSON object	file collection	com/lexisnexisrisk/threatmetrix/tmxprofiling/ebeeeeee.java me/lyft/android/PolarisApplication.java

RULE ID	BEHAVIOUR	LABEL	FILES
00137	Get last known location of the device	location collection	com/lexisnexisrisk/threatmetrix/tmxprofiling/ebbbbb.java
00034	Query the current data network type	collection network	com/mapbox/common/TelemetrySystemUtils.java
00125	Check if the given file path exist	file	me/lyft/android/extensions/ExtensionsKt.java n2/a.java
00131	Get location of the current GSM and put it into JSON	collection location	com/lexisnexisrisk/threatmetrix/tmxprofiling/ebefeee.java
00085	Get the ISO country code and put it into JSON	collection telephony	com/lexisnexisrisk/threatmetrix/tmxprofiling/ebefeee.java
00099	Get location of the current GSM and put it into JSON	collection location	com/lexisnexisrisk/threatmetrix/tmxprofiling/ebefeee.java
00016	Get location info of the device and put it to JSON object	location collection	com/lexisnexisrisk/threatmetrix/tmxprofiling/ebefeee.java
00132	Query The ISO country code	telephony collection	com/lexisnexisrisk/threatmetrix/tmxprofiling/ebefeee.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	i6/a.java
00112	Get the date of the calendar event	collection calendar	io/sentry/j.java
00121	Create a directory	file command	n2/a.java
00003	Put the compressed bitmap data into JSON object	camera	io/branch/referral/network/a.java
00009	Put data in cursor to JSON object	file	i9/k2.java
00191	Get messages in the SMS inbox	sms	p/r0.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://montreal-production.firebaseio.com
Firebase Remote Config enabled	warning	<p>The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/532883359162/namespaces/firebase:fetch?key=AlzaSyAqGMDEe0AFdLsnglhlfzqM-UHqAk_IXcA is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: { 'entries': { 'ActiveOrganicTakeovers': ' ', 'AppMinBuildAndroid': '1730248164', 'AppMinBuildIOS': '236523134', 'AppMinVersionIOS': '2024.46', 'BFFInRidePanel': 'true', 'BikeAngelURL': 'https://bixi.com/en/ami-bixi/', 'ChargingHubsEnabled': 'true', 'DefaultCoordinate': { 'Latitude': 45.504572, 'Longitude': -73.565483 }, 'EbikeChargingLevel': 'true', 'FeatureMinimumBuild': 'true', 'GroupRideProductId': '112', 'HelpURL': 'https://support.bixi.com/hc/en-ca', 'HttpWebsite': 'https://bixi.com/en/how-to-use-the-bixi-service/', 'LiabilityWaiverURL': 'https://s3.amazonaws.com/bixi-assets/liability-waiver.html', 'MapBounds': { 'north': 45.8515924, 'east': -71.4887945, 'south': 45.0054225, 'west': -74.468836 }, 'MapDataFetchIntervalSeconds': '10', 'MenuSponsorshipBanner': { 'imageURL': { 'en': 'https://firebasestorage.googleapis.com/v0/b/montreal-production.appspot.com/o/public-assets%2FRachelleBery_202509_ProfileBanner_EN.jpg?alt=media', 'fr': 'https://firebasestorage.googleapis.com/v0/b/montreal-production.appspot.com/o/public-assets%2FRachelleBery_202509_ProfileBanner_FR.jpg?alt=media', 'en': 'https://firebasestorage.googleapis.com/v0/b/montreal-production.appspot.com/o/public-assets%2FRachelleBery_202509_ProfileBanner_FR.jpg?alt=media' } }, 'linkOutURL': { 'en': 'https://www.rachellebery.ca/en/about-us/our-partners/bixi-montreal/ ', 'fr': 'https://www.rachellebery.ca/fr/a-propos/nos-collaborations/bixi-montreal/' }, 'es': 'https://www.rachellebery.ca/fr/a-propos/nos-collaborations/bixi-montreal/' }, 'contentDescription': { 'en': 'RachelleBerry x BIXI 2025', 'fr': 'RachelleBerry x BIXI 2025', 'es': 'RachelleBerry x BIXI 2025' }, 'OpenRentalSetup': { 'timeout': 70, 'interval': 5 }, 'PrivacyPolicyUrl': 'https://bixi.com/en/mobile-app-terms', 'QRToUnlockZones': { 'id': 'mtl', 'north': 90, 'south': -90, 'west': -180, 'east': 180, 'introductionTitle': { 'en': 'A better way to unlock', 'es': 'Nueva forma de desbloquear', 'fr': 'Nouvelle manière de déverrouiller' }, 'introductionBody': { 'en': 'Scan the QR code located between the handlebars to start riding!', 'es': 'Puedes desbloquear bicis con códigos QR que está entre los manillares', 'fr': 'Vous pouvez maintenant déverrouiller les vélos en utilisant un code QR.' } }, 'QRToUnlockEnabled': 'true', 'RentalAgreementURL': 'https://s3.amazonaws.com/bixi-assets/rental-agreement.html', 'ReportFormURL': ' ', 'RideCodeActiveKeyTest': 'false', 'RideCodeRequestStationDistance': '100', 'ShowRegistrationButtonInMenu': 'true', 'bffRideMutationUnlockEnabled': 'true', 'bikeAngelsEnabled': 'false', 'isRecaptchaEnabled': 'true', 'jsEnabledTermsAndConditions': 'true', 'lusPolarisMonorepoAnalyticsBlockedAnalytics': ['stream_subscribe', 'stream_unsubscribe'], 'pyCardScanLabels': 'background,0,1,2,3,4,5,6,7,8,9,/,card,moire', 'pyCardScanModelVersion': '2171ce5e7ff57ef8cb1cf73258a84f9d', 'recaptchaEndpoints': [{ 'url': '/v1/lbsbff/polaris/api/login/2fa', 'action': 'login' }, { 'url': '/v1/lbsbff/polaris/api/signup/email/request-code', 'action': 'signupRequestCode' }, { 'url': '/v1/lbsbff/polaris/api/signup/email/verify', 'action': 'signupValidateCode' }, { 'url': '/mobile/v1/*/signup', 'action': 'signup' }, { 'url': '/v1/*/account/billing', 'action': 'updateBillingInfo' }], 'roundUpRideHistory': 'true', 'sentryEnabled': 'true', 'state': 'UPDATE', 'templateVersion': '303' }</p>

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
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:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION
--------	----------------

🔍 DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.googleadservices.com	ok	IP: 142.250.69.98 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
s3.amazonaws.com	ok	IP: 54.231.196.176 Country: Germany Region: Hessen City: Frankfurt am Main Latitude: 50.115520 Longitude: 8.684170 View: Google Map
docs.sentry.io	ok	IP: 76.76.21.93 Country: United States of America Region: California City: Walnut Latitude: 34.015400 Longitude: -117.858223 View: Google Map
docs.mapbox.com	ok	IP: 54.192.51.72 Country: United States of America Region: New York City: New York City Latitude: 40.714272 Longitude: -74.005966 View: Google Map
google.com	ok	IP: 142.250.69.46 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
ns.adobe.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
apps.mapbox.com	ok	IP: 54.192.51.58 Country: United States of America Region: New York City: New York City Latitude: 40.714272 Longitude: -74.005966 View: Google Map
api.mapbox.com	ok	IP: 3.161.213.58 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
10.0.2.2	ok	IP: 10.0.2.2 Country: - Region: - City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map
accounts.google.com	ok	IP: 142.251.163.84 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
lft.to	ok	IP: 67.199.248.13 Country: United States of America Region: New York City: New York City Latitude: 40.739288 Longitude: -73.984955 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.google.com	ok	IP: 142.250.69.68 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
cdn.lyft.net	ok	IP: 54.192.51.76 Country: United States of America Region: New York City: New York City Latitude: 40.714272 Longitude: -74.005966 View: Google Map
play.google.com	ok	IP: 142.250.69.46 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.lyft.com	ok	IP: 54.192.51.31 Country: United States of America Region: New York City: New York City Latitude: 40.714272 Longitude: -74.005966 View: Google Map
montreal-production.firebaseio.com	ok	IP: 35.190.39.113 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map

DOMAIN	STATUS	GEOLOCATION
cloudfront-staging.tilestream.net	ok	IP: 54.192.51.42 Country: United States of America Region: New York City: New York City Latitude: 40.714272 Longitude: -74.005966 View: Google Map
config.mapbox.com	ok	IP: 3.214.250.191 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
api2.branch.io	ok	IP: 3.161.213.39 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
docs.rs	ok	IP: 3.162.3.120 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
firebase.google.com	ok	IP: 142.250.69.110 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.mapbox.com	ok	IP: 151.101.136.143 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
github.com	ok	IP: 140.82.114.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
api.lyft.com	ok	IP: 3.162.3.57 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
mobileapi.usebutton.com	ok	IP: 3.134.227.174 Country: United States of America Region: Ohio City: Columbus Latitude: 39.961182 Longitude: -82.998787 View: Google Map
o4507234886615040.ingest.us.sentry.io	ok	IP: 34.120.195.249 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map

DOMAIN	STATUS	GEOLOCATION
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
schemas.android.com	ok	No Geolocation information available.
s.mobileapi.usebutton.com	ok	IP: 3.134.227.174 Country: United States of America Region: Ohio City: Columbus Latitude: 39.961182 Longitude: -82.998787 View: Google Map
app.usebutton.com	ok	IP: 54.71.111.2 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map
account.lyft.com	ok	IP: 54.192.51.114 Country: United States of America Region: New York City: New York City Latitude: 40.714272 Longitude: -74.005966 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.tensorflow.org	ok	IP: 142.250.69.110 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.winimage.com	ok	IP: 95.134.100.159 Country: Ukraine Region: Kirovohradska oblast City: Pomichna Latitude: 48.242222 Longitude: 31.415831 View: Google Map
api-events-config-staging.tilestream.net	ok	IP: 54.92.226.151 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
cdn.branch.io	ok	IP: 3.161.213.114 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
blog.lyft.com	ok	IP: 52.54.211.120 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map

DOMAIN	STATUS	GEOLOCATION
events.mapbox.com	ok	IP: 3.221.195.116 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
help.lyft.com	ok	IP: 54.192.51.101 Country: United States of America Region: New York City: New York City Latitude: 40.714272 Longitude: -74.005966 View: Google Map
app-measurement.com	ok	IP: 142.250.69.46 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
layer.bicyclesharing.net	ok	IP: 100.28.53.15 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
api-events-staging.tilestream.net	ok	IP: 100.27.117.62 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map

DOMAIN	STATUS	GEOLOCATION
goo.gl	ok	IP: 142.250.69.110 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
lyft.com	ok	IP: 54.192.51.101 Country: United States of America Region: New York City: New York City Latitude: 40.714272 Longitude: -74.005966 View: Google Map

EMAILS

EMAIL	FILE
-dark@2x.png -dark@3x.png	vh/m.java
366547c14f0d186fd650@o4507234886615040.ingest	me/lyft/android/PolarisApplication.java
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

TRACKERS

TRACKER	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

HARDCODED SECRETS

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Contraseña"
"mapbox_access_token" : "pk.eyJ1IjoibW90aXZhdGVjbyIsImEiOiIyMmZiZjgxZDk3ZjFmYmVkM2RlMjIjOTIhInMl4MWQzYSJ9.w4Pt2wTiMPllStx2czBzw"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"branch_key_live" : "key_live_bftVVjsnCMi5JW65w9dxlcbbyuhmeYWa"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Senha"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"google_crash_reporting_api_key" : "AlzaSyAqGMDEe0AFdLsnglhlfzqM-UHqAk_IXcA"
"google_api_key" : "AlzaSyAqGMDEe0AFdLsnglhlfzqM-UHqAk_IXcA"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Sarbide-gakoa"
"client_secret" : "R-UBCG-EWwF93eSD_T7zaxt81ajTWRas"
"firebase_database_url" : "https://montreal-production.firebaseio.com"

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL " : "Pasahitza"
"branch_key_test" : "key_test_bfsOVdsmAHk2U306w0yhhbcoCyeob13C"
CGiNgzoyE02Vb26y6BkqGEJ5zCHmZ/Ea+Zhr
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
HmeElzU6FU2YZHWu4BswBI1kyT3iaOEG/JNHGBoLmw==
H16u7wATM3S4Tl6egTYleX5f+xfdXtsmmA==
CGiNgzo2GE+cbGOp/hY4HVx12y0=
AWalgTorHkuYYW6y9h4oEVF12izmZQ==
GH2AjC4gA1eZZXir7RgrBkN52y3gefMX94ZQDBcKiA==
BmiKijo8F1WRYmuu6gg1F1hxxDftaPUM/IRQDQU=
HkeprgsbOny5AEiU1TlfNmpVqAjMRcch17g1
8920e690dd011895672947112477d10d5c8afb09-
115792089210356248762697446949407573530086143415290314195533631308867097853951
af60eb711bd85bc1e4d3e0a462e074eea428a8
GGyThiQzH0OYf2Oj9xYwEEpvxy7sZfUG/A==
GWyVkDYrF1qWZnis7BljFEdjyTLgcPoN/A==
258EAFa5-E914-47DA-95CA-C5AB0DC85B11
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZlJvaWQuYXBCwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n

POSSIBLE SECRETS
808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
BmCSnCwxEUaNcmWq8xYxBlx13Cv7eese+ZpAGw==
BHmCgCE6CVCTdmuh6BMjClpxyzX2e/sL+YjcERg=
D3uOnzosAliea3W47xM5C0h8xyk=
BmyMgDcmCU2Sb3W+7BYwFVF2xyz2fvoB7J9UEh8ejfYjRI4=
D3yRkCwxAFiRaW6y8gM9GkVvxzvZPEc
6b39de30ea0619404ba2dd850e195c5a9ce0c7a5
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
BmiNiSotG1yZf2Og7BI4EE9kzSHoZfMd9ZNbCg==
AwNEBWVGK2I5B4O3eUfYMIYrOILjvXa1PHClion7qdZRbxqjQAYvcaExSNJbplCz
G3uOiDc+G0afdWyr5AUjFlh12iz8eesF8YVGFxgDk+06Tplz2cE=
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececb6406837bf51f5
BkCyyAwRMTm0TkOZyDYQMhRR/BfGWZQu16Q1Ljk3pdYDZK5S
TVRWQVBjX21vYmlsZTo4Q0p0b2pGS3Qke0RYIVdX
GH2AjC4gAlaSf3mg4BswBkh/2iHoZfMd9ZNbCg==
Ake3rgkWMjm/WV6lwjgYPC5A+hHdWn1PY=
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

POSSIBLE SECRETS
expWomenPlusConnectDriverVisibilityM1AutoExpand
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
ce01246084b5366547c14f0d186fd650
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
HmeElzU6FU2YZHWn4AE9Bktoyzv5Y/0H9g==
G3uOiDc+G0afdWyr5AUjFlh12iz8eQ==
DWCPizoyE02Vb26y6BkqGEJ5zCHmZ/Ea+ZhR
a0784d7a4716f3feb4f64e7f4b39bf04
5aab261f4f0ca9cf59bf90fe
DWCPizo8GliOc3Wk7wE9FUd01zH5cuYJ9pl=
BHmCgCE6CVCTdmuh6BMjEENGxDvkcvoc+YjcERgbmPs6Tg==
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
GH2AjC4gAlaSf3mg4BswBkh/2iHkdv0G55BAEBUQhe0k
bae8e37fc83441b16034566b
CGiPgSorCUyTbWu/8h89FUJv2jv9YuYG54BUEgMB
GH2AjC4gAlaSf3mg4BswBkh/2iHgef0c8ZdZFwwFmOsIRQ==
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
DWCPizoyE02Vb26y7BloEUF01zDmY+sO94NbGg==

POSSIBLE SECRETS
24bbf6e6dd901556b6cb9013e03cda89
DWCPizo8GliOc3Wu7RYvClF+xyr2cfsd9pl=
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
HmeJjis7GlyZf3q/7hAuGENvzSz7eOY=
Ake3rgkWMjm+UIOd1Tg3PHccqBbIRJQk3bhyKj5k
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
36864200e0eaf5284d884a0e77d31646
ed778c73ea51338d6576fb5992b189f2b94d9f3d5e199f46c1af520d6b0b3e6c
SRQznwSqEierDbkXg2yZTsse5Tb+l4Z4JiS6GvFcIFe=
115792089210356248762697446949407573529996955224135760342422259061068512044369
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151

PLAYSTORE INFORMATION

Title: BIXI

Score: 3.8152175 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Lifestyle **Play Store URL:** [com.eightd.biximobile](https://play.google.com/store/apps/details?id=com.eightd.biximobile)

Developer Details: Lyft, Inc., 6629245766506578153, None, <https://montreal.bixi.com>, 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.

☰ SCAN LOGS

Timestamp	Event	Error
2025-11-12 18:55:22	Generating Hashes	OK
2025-11-12 18:55:22	Extracting APK	OK
2025-11-12 18:55:22	Unzipping	OK
2025-11-12 18:55:27	Parsing APK with androguard	OK
2025-11-12 18:55:28	Extracting APK features using aapt/aapt2	OK
2025-11-12 18:55:29	Getting Hardcoded Certificates/Keystores	OK
2025-11-12 18:55:40	Parsing AndroidManifest.xml	OK
2025-11-12 18:55:40	Extracting Manifest Data	OK
2025-11-12 18:55:40	Manifest Analysis Started	OK

2025-11-12 18:55:40	Reading Network Security config from network_security_config.xml	OK
2025-11-12 18:55:40	Parsing Network Security config	OK
2025-11-12 18:55:41	Performing Static Analysis on: BIXI (com.eightd.biximobile)	OK
2025-11-12 18:55:41	Fetching Details from Play Store: com.eightd.biximobile	OK
2025-11-12 18:55:42	Checking for Malware Permissions	OK
2025-11-12 18:55:42	Fetching icon path	OK
2025-11-12 18:55:42	Library Binary Analysis Started	OK
2025-11-12 18:55:42	Analyzing apktool_out/lib/arm64-v8a/libandroidx.graphics.path.so	OK
2025-11-12 18:55:42	Analyzing apktool_out/lib/arm64-v8a/libc++_shared.so	OK
2025-11-12 18:55:42	Analyzing apktool_out/lib/arm64-v8a/libcapture.so	OK
2025-11-12 18:55:42	Analyzing apktool_out/lib/arm64-v8a/libmapbox-common.so	OK
2025-11-12 18:55:42	Analyzing apktool_out/lib/arm64-v8a/libmapbox-maps.so	OK

2025-11-12 18:55:42	Analyzing apktool_out/lib/arm64-v8a/libentry-android.so	OK
2025-11-12 18:55:42	Analyzing apktool_out/lib/arm64-v8a/libentry.so	OK
2025-11-12 18:55:42	Analyzing apktool_out/lib/arm64-v8a/libtensorflowlite_jni.so	OK
2025-11-12 18:55:42	Analyzing apktool_out/lib/arm64-v8a/libTMXProfiling-7.5-59-jni.so	OK
2025-11-12 18:55:43	Analyzing apktool_out/lib/armeabi-v7a/libandroidx.graphics.path.so	OK
2025-11-12 18:55:43	Analyzing apktool_out/lib/armeabi-v7a/libc++_shared.so	OK
2025-11-12 18:55:43	Analyzing apktool_out/lib/armeabi-v7a/libcapture.so	OK
2025-11-12 18:55:43	Analyzing apktool_out/lib/armeabi-v7a/libmapbox-common.so	OK
2025-11-12 18:55:43	Analyzing apktool_out/lib/armeabi-v7a/libmapbox-maps.so	OK
2025-11-12 18:55:43	Analyzing apktool_out/lib/armeabi-v7a/libentry-android.so	OK
2025-11-12 18:55:43	Analyzing apktool_out/lib/armeabi-v7a/libentry.so	OK
2025-11-12 18:55:43	Analyzing apktool_out/lib/armeabi-v7a/libtensorflowlite_jni.so	OK

2025-11-12 18:55:43	Analyzing apktool_out/lib/armeabi-v7a/libTMXProfiling-7.5-59-jni.so	OK
2025-11-12 18:55:43	Analyzing apktool_out/lib/x86/libandroidx.graphics.path.so	OK
2025-11-12 18:55:43	Analyzing apktool_out/lib/x86/libc++_shared.so	OK
2025-11-12 18:55:43	Analyzing apktool_out/lib/x86/libcapture.so	OK
2025-11-12 18:55:43	Analyzing apktool_out/lib/x86/libmapbox-common.so	OK
2025-11-12 18:55:43	Analyzing apktool_out/lib/x86/libmapbox-maps.so	OK
2025-11-12 18:55:43	Analyzing apktool_out/lib/x86/libentry-android.so	OK
2025-11-12 18:55:44	Analyzing apktool_out/lib/x86/libentry.so	OK
2025-11-12 18:55:44	Analyzing apktool_out/lib/x86/libtensorflowlite_jni.so	OK
2025-11-12 18:55:44	Analyzing apktool_out/lib/x86/libTMXProfiling-7.5-59-jni.so	OK
2025-11-12 18:55:44	Analyzing apktool_out/lib/x86_64/libandroidx.graphics.path.so	OK
2025-11-12 18:55:44	Analyzing apktool_out/lib/x86_64/libc++_shared.so	OK

2025-11-12 18:55:44	Analyzing apktool_out/lib/x86_64/libcapture.so	OK
2025-11-12 18:55:44	Analyzing apktool_out/lib/x86_64/libmapbox-common.so	OK
2025-11-12 18:55:44	Analyzing apktool_out/lib/x86_64/libmapbox-maps.so	OK
2025-11-12 18:55:44	Analyzing apktool_out/lib/x86_64/libentry-android.so	OK
2025-11-12 18:55:44	Analyzing apktool_out/lib/x86_64/libentry.so	OK
2025-11-12 18:55:44	Analyzing apktool_out/lib/x86_64/libtensorflowlite_jni.so	OK
2025-11-12 18:55:44	Analyzing apktool_out/lib/x86_64/libTMXProfiling-7.5-59-jni.so	OK
2025-11-12 18:55:46	Reading Code Signing Certificate	OK
2025-11-12 18:55:47	Running APKID 3.0.0	OK
2025-11-12 18:55:57	Detecting Trackers	OK
2025-11-12 18:56:03	Decompiling APK to Java with JADX	OK
2025-11-12 18:58:25	Converting DEX to Smali	OK

2025-11-12 18:58:25	Code Analysis Started on - java_source	OK
2025-11-12 18:58:50	Android SBOM Analysis Completed	OK
2025-11-12 18:59:00	Android SAST Completed	OK
2025-11-12 18:59:00	Android API Analysis Started	OK
2025-11-12 18:59:08	Android API Analysis Completed	OK
2025-11-12 18:59:09	Android Permission Mapping Started	OK
2025-11-12 18:59:16	Android Permission Mapping Completed	OK
2025-11-12 18:59:18	Android Behaviour Analysis Started	OK
2025-11-12 18:59:29	Android Behaviour Analysis Completed	OK
2025-11-12 18:59:29	Extracting Emails and URLs from Source Code	OK
2025-11-12 18:59:41	Email and URL Extraction Completed	OK
2025-11-12 18:59:41	Extracting String data from APK	OK

2025-11-12 18:59:41	Extracting String data from SO	OK
2025-11-12 18:59:42	Extracting String data from Code	OK
2025-11-12 18:59:42	Extracting String values and entropies from Code	OK
2025-11-12 19:01:59	Performing Malware check on extracted domains	OK
2025-11-12 19:02:03	Saving to Database	OK

Report Generated by - MobSF v4.4.3

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.

© 2025 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).