MOBSF

ANDROID STATIC ANALYSIS REPORT

AllTrails (19.20.0)

File Name: com.alltrails.alltrails_60118.apk

Package Name:	com.alltrails.alltrails
Scan Date:	Aug. 29, 2025, 7:29 p.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	11/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
6	26	6	5	2

FILE INFORMATION

File Name: com.alltrails.alltrails_60118.apk
Size: 148.44MB
MD5: 75c13bd466215d8529f69cc3234e5058
SHA1: 7d873aafdb222fcb6a2e672041ca167d9a8097e1
SHA256: ef5cbe6db9a8febb51b7d2f6b7717e17c1736fee3431c66eb8692758deae15f0

APP INFORMATION

App Name: AllTrails
Package Name: com.alltrails.alltrails
Main Activity: com.alltrails.alltrails.StartActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 19.20.0
Android Version Code: 60118

APP COMPONENTS

Activities: 86
Services: 20
Receivers: 22

Providers: 8
Exported Activities: 6
Exported Services: 4
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=CA, L=San Francisco, O=AllTrails, OU=Android, CN=Developer
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2011-07-06 20:25:53+00:00
Valid To: 2038-11-21 20:25:53+00:00
Issuer: C=US, ST=CA, L=San Francisco, O=AllTrails, OU=Android, CN=Developer
Serial Number: 0x4e14c4d1
Hash Algorithm: md5
md5: 82f691b03c940fdcfc8fdce42bb45a68
sha1: 93caa2125544f7e981f3c8c9c13096e97bb97a5c
sha256: 48ce7d26b14313d87f0d18e66509d890f112b69424e141c009b14fb475edb8f8
sha512: 09dc2d3b052f6b30eacb66ad3fc7ba7d311667f88529627a021114c5cbee6db7f5492c26f1950e49700193335e4b8eeaca87413fda0fa397c57b0f1793725474
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: a3a9fa96bf6d0b72e39ec4912ba846777ae359d8e111710e0e21162bfbcf9580
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.FOREGROUND_SERVICE_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.ACCESS_MEDIA_LOCATION	dangerous	access any geographic locations	Allows an application to access any geographic locations persisted in the user's shared collection.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.DETECT_SCREEN_CAPTURE	normal	notifies when a screen capture of the app's windows is attempted.	Allows an application to get notified when a screen capture of its windows is attempted.
android.permission.health.WRITE_DISTANCE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_ELEVATION_GAINED	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_EXERCISE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_SPEED	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
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.alltrails.alltrails.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>75c13bd466215d8529f69cc3234e5058.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.BOARD check
network operator name check</td></tr>
<tr><td>Compiler</td><td>dexlib 1.x
r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes10.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes11.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
network operator name check
device ID check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes12.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.HARDWARE check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes13.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes14.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
SIM operator check
network operator name check
device ID check
ro.kernel.qemu check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
network operator name check
ro.kernel.qemu check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>network operator name check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes6.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes7.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes8.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes9.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT

ACTIVITY	INTENT
com.alltrails.alltrails.StartActivity	Schemes: @string/deep_linking_scheme://, alltrails://, https://, http://, Hosts: @string/appsflyer_onelink_deeplinking_host, @string/deep_linking_host, @string/deep_linking_host_legacy, alltrails.com, www.alltrails.com, ablink.email.alltrails.com, Path Prefixes: /pro/signup, /plus/signup, /explore, /lists, /members, /community, /guides, /my, /trail, /parks, /uni, Path Patterns: /../pro/signup.*, /..-../pro/signup.*, /../plus/signup.*, /..-../plus/signup.*, /../explore.*, /..-../explore.*, /../lists.*, /..-../lists.*, /../members.*, /..-../members.*, /../community.*, /..-../community.*, /../guides.*, /..-../guides.*, /../my.*, /..-../my.*, /../trail.*, /..-../trail.*, /../ruta.*, /..-../ruta.*, /../randonnee.*, /..-../randonnee.*, /../route.*, /..-../route.*, /../wandelpad.*, /..-../wandelpad.*, /../sentiero.*, /..-../sentiero.*, /../led.*, /..-../led.*, /../sti.*, /..-../sti.*, /../rute.*, /..-../rute.*, /../szlak.*, /..-../szlak.*, /../trilho.*, /..-../trilho.*, /../trilha.*, /..-../trilha.*, /../parks.*, /..-../parks.*, /../parques.*, /..-../parques.*, /../parcs.*, /..-../parcs.*, /../parken.*, /..-../parken.*, /../parchi.*, /..-../parchi.*, /../parker.*, /..-../parker.*, /../parki.*, /..-../parki.*,
com.alltrails.common.oauth.alltrails.ui.AlltrailsOAuthActivity	Schemes: com.alltrails.app://, Path Prefixes: /auth/success,
com.alltrails.common.oauth.garmin.GarminOAuthWebActivity	Schemes: https://, http://, Hosts: @string/deep_linking_host, @string/deep_linking_host_legacy, alltrails.com, www.alltrails.com, Path Prefixes: /users/auth/garmin_connect,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.alltrails.alltrails,

NETWORK SECURITY

HIGH: 2 | WARNING: 1 | INFO: 1 | SECURE: 1

NO	SCOPE	SEVERITY	DESCRIPTION
1	127.0.0.1	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.
2	alltrails.com	secure	Domain config is securely configured to disallow clear text traffic to these domains in scope.
3	alltrails.com	warning	Domain config is configured to trust system certificates.
4	alltrails.com	info	Domain config is configured to trust bundled certs @raw/alltrails_cert_expires_8_22_2025.

NO	SCOPE	SEVERITY	DESCRIPTION
5	localhost	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm vulnerable to hash collision	high	Application is signed with MD5. MD5 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. 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 (com.alltrails.common.oauth.alltrails.ui.AlltrailsOAuthActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Activity (com.alltrails.common.oauth.garmin.GarminOAuthWebActivity) 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.
5	Service (com.alltrails.infra.wear.datalayer.AllTrailsWearableListenerService) 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.
6	Activity (com.canhub.cropper.CropImageActivity) 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.
7	Broadcast Receiver (com.appsflyer.SingleInstallBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity (com.alltrails.alltrails.healthconnect.PermissionsRationaleActivity) 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.
9	Activity (com.facebook.CustomTabActivity) 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	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
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.
12	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
13	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
14	Service (androidx.health.platform.client.impl.sdkservice.HealthDataSdkService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
15	Activity (androidx.compose.ui.tooling.PreviewActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
16	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: **2** | WARNING: **9** | INFO: **4** | SECURE: **3** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ch/qos/logback/classic/android/LogcatAppender.java ch/qos/logback/classic/pattern/TargetLengthBasedClassNameAbbreviator.java ch/qos/logback/classic/spi/ThrowableProxy.java ch/qos/logback/core/joran/util/ConfigurationWatchListUtil.java ch/qos/logback/core/net/DefaultSocketConnector.java ch/qos/logback/core/net/SocketConnectorBase.java ch/qos/logback/core/recovery/ResilientOutputStreamBase.java ch/qos/logback/core/spi/ContextAwareBase.java ch/qos/logback/core/spi/ContextAwareImpl.java com/algolia/search/logging/Logger.java com/algolia/search/model/response/ResponseLogs$Log$$serializer.java com/alltrails/alltrails/util/LocationLog.java com/amplitude/api/AmplitudeLog.java com/appsflyer/AFLogger.java com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFd1eSDK.java com/appsflyer/internal/AFd1fSDK.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/appsflyer/internal/AFd1kSDK.java com/appsflyer/internal/AFd1nSDK.java com/appsflyer/internal/AFd1oSDK.java com/appsflyer/internal/AFd1pSDK.java com/appsflyer/internal/AFd1sSDK.java com/appsflyer/internal/AFd1tSDK.java com/appsflyer/internal/AFd1uSDK.java com/appsflyer/internal/AFe1kSDK.java com/appsflyer/internal/AFe1rSDK.java com/appsflyer/internal/AFe1uSDK.java com/appsflyer/internal/AFf1bSDK.java com/apptentive/android/sdk/conversation/LegacyConversationMetadata.java com/braze/support/BrazeLogger.java com/bumptech/glide/a.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/canhub/cropper/CropImageActivity.java com/datadog/android/rum/DdRumContentProvider.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$e$1.java com/mapbox/common/logger/MapboxLogger$i$1.java com/mapbox/common/logger/MapboxLogger$w$

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/mapbox/common/logger/MapboxLogger$4$1.java com/mapbox/common/module/okhttp/NetworkUsageListener.java com/mapbox/common/module/provider/MapboxModuleProvider.java com/mapbox/maps/FontUtils.java defpackage/A77.java defpackage/AI.java defpackage/AX5.java defpackage/AbstractC21027zN5.java defpackage/AbstractC7325Zj3.java defpackage/B77.java defpackage/BinderC20898z77.java defpackage/C10267f65.java defpackage/C12237io.java defpackage/C12292iu6.java defpackage/C12438j97.java defpackage/C14107mR0.java defpackage/C14131mU0.java defpackage/C14958o52.java defpackage/C15131oQ2.java defpackage/C15137oR0.java defpackage/C15776pf3.java defpackage/C15931py6.java defpackage/C17172sO.java defpackage/C17649tI.java defpackage/C17699tO1.java defpackage/C18572v66.java defpackage/C18965vK0.java defpackage/C19145vg3.java defpackage/C19526wQ5.java defpackage/C19558wU5.java defpackage/C19881x77.java defpackage/C2029Bf1.java defpackage/C21031zO1.java defpackage/C3219Go0.java defpackage/C3563If0.java defpackage/C4950On.java defpackage/C5369Ql5.java defpackage/C5551Ri3.java defpackage/C6644Wd4.java defpackage/C8181bL2.java defpackage/C8185bL6.java defpackage/C8197bN2.java defpackage/C8692cL5.java defpackage/C8841cb7.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/C8841cb7.java defpackage/C9902eO1.java defpackage/CG0.java defpackage/CX1.java defpackage/D.java defpackage/D31.java defpackage/DG0.java defpackage/E47.java defpackage/FM2.java defpackage/GF0.java defpackage/GK5.java defpackage/GM2.java defpackage/GN5.java defpackage/GO1.java defpackage/J01.java defpackage/JP2.java defpackage/JU0.java defpackage/KI.java defpackage/KP2.java defpackage/L83.java defpackage/MapStyleNode.java defpackage/NY5.java defpackage/NdkCrashLog.java defpackage/QL.java defpackage/QN2.java defpackage/R10.java defpackage/SH.java defpackage/SL.java defpackage/TL5.java defpackage/U55.java defpackage/V45.java defpackage/VY6.java defpackage/W45.java defpackage/WJ0.java defpackage/Z46.java io/embrace/android/embracesdk/logging/EmbLoggerImpl.java io/ktor/client/plugins/logging/SimpleLogger.java io/ktor/http/parsing/DebugKt.java io/ktor/server/engine/internal/ApplicationUtilsJvmKt.java io/ktor/util/CoroutinesUtilsKt.java io/netty/util/Version.java io/netty/util/internal/logging/MessageFormatter.java org/slf4j/helpers/Util.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				sprig/graphics/h.java ch/qos/logback/classic/joran/action/ConfigurationAction.java ch/qos/logback/classic/sift/ContextBasedDiscriminator.java ch/qos/logback/core/CoreConstants.java ch/qos/logback/core/net/ssl/SSL.java ch/qos/logback/core/rolling/helper/DateTokenConverter.java ch/qos/logback/core/rolling/helper/IntegerTokenConverter.java coil/memory/MemoryCache.java com/algolia/search/configuration/internal/ConfigurationInsightsImpl.java com/algolia/search/model/indexing/BatchOperation.java com/algolia/search/model/response/ResponseAPIKey.java com/algolia/search/model/response/creation/CreationAPIKey.java com/algolia/search/model/response/revision/RevisionAPIKey.java com/algolia/search/serialize/internal/Countries.java com/algolia/search/serialize/internal/Key.java com/alltrails/alltrails/apiclient/IAllTrailsAuthenticationService.java com/alltrails/alltrails/apiclient/PostmanServiceRequestInterceptor.java com/alltrails/alltrails/community/service/privacy/PrivacyPreferenceType.java com/alltrails/alltrails/ui/map/util/state/MapCameraState.java com/alltrails/alltrails/ui/navigator/NavigatorAction.java com/alltrails/alltrails/ui/navigator/j.java com/alltrails/alltrails/ui/photo/PhotoDetailsBindingModel.java com/alltrails/alltrails/worker/configuration/AlgoliaConfiguration.java com/alltrails/cmty/collab/lists/ui/dialog/CollaboratorActionModalDialogConfig.java com/alltrails/infra/ui/pillcomponent/a.java com/alltrails/onboarding/ui/education/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/amplitude/api/AmplitudeClient.java com/apptentive/android/sdk/encryption/resolvers/KeyResolver18.java
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/braze/configuration/BrazeConfig.java com/mapbox/common/PlatformHttpService.java com/mapbox/common/experimental/geofencing/GeofencingPropertiesKeys.java com/mapbox/common/location/LocationUpdatesReceiver.java com/mapbox/maps/ThreadChecker.java defpackage/AK6.java defpackage/AbstractC2346Cl5.java defpackage/AbstractC4192Ky.java defpackage/AchievementViewState.java defpackage/AllTrailsTrailToTrailCardViewStateParams.java defpackage/C11872i61.java defpackage/C13708lf0.java defpackage/C16723rV2.java defpackage/C19650wg0.java defpackage/C21060zR6.java defpackage/C5776Sh.java defpackage/C7485a3.java defpackage/CelebratoryAttributes.java defpackage/D55.java defpackage/EvaluationFlag.java defpackage/EvaluationVariant.java defpackage/ExpandedItemKeyValueCell.java defpackage/Exposure.java defpackage/FeatureFlagOptionItem.java defpackage/GarminConnectConfiguration.java defpackage/HomepageMapControlsViewState.java defpackage/HorizontalTagItem.java defpackage/IQ2.java defpackage/IdentityConfiguration.java defpackage/InterfaceC14912o01.java defpackage/InterfaceC18030u3.java defpackage/InterfaceC18513v01.java defpackage/InterfaceC20320y01.java defpackage/L46.java defpackage/MapLayerDownloadBundle.java defpackage/NB0.java defpackage/O64.java defpackage/P01.java defpackage/PerformanceLoggerAttribute.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/Promotion.java defpackage/RU6.java defpackage/RemoteReviewsRequest.java defpackage/ReviewsRequest.java defpackage/RumViewInfo.java defpackage/TE1.java defpackage/TagCloudItem.java defpackage/TagCloudItemStateModel.java defpackage/User.java defpackage/UserSlim.java defpackage/Variant.java defpackage/WV3.java defpackage/Z2.java io/embrace/android/embracesdk/arch/destination/SpanAttributeData.java io/embrace/android/embracesdk/capture/crumbs/PushNotificationCaptureService.java io/embrace/android/embracesdk/internal/payload/Attribute.java io/embrace/android/embracesdk/internal/payload/EnvelopeMetadata.java io/embrace/android/embracesdk/payload/UserInfo.java io/embrace/android/embracesdk/prefs/EmbracePreferencesService.java io/ktor/client/request/forms/FormPart.java io/ktor/http/auth/HttpAuthHeader.java io/ktor/server/engine/ConfigKeys.java io/ktor/util/PlatformUtilsJvmKt.java io/netty/handler/codec/http/HttpHeaders.java io/netty/handler/ssl/PemPrivateKey.java io/netty/handler/ssl/SslMasterKeyHandler.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	bo/content/e1.java com/braze/support/IntentUtils.java defpackage/C10284f84.java defpackage/C13437l76.java defpackage/C15322oo.java defpackage/C15443p10.java defpackage/C16036qA0.java defpackage/C4265Lf1.java defpackage/C7995az4.java defpackage/EnumC2091Bn.java defpackage/EnumC7024Xy4.java defpackage/J24.java defpackage/NU5.java defpackage/R0.java defpackage/VB0.java defpackage/VG.java io/embrace/android/embracesdk/anr/ndk/EmbraceNativeThreadSamplerService.java io/netty/handler/ssl/util/ThreadLocalInsecureRandom.java io/netty/util/internal/PlatformDependent.java io/netty/util/internal/ThreadLocalRandom.java
4	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/appsflyer/internal/AFb1zSDK.java defpackage/C13126kW1.java defpackage/C2562Dl5.java defpackage/TA3.java io/ktor/util/CryptoKt__CryptoJvmKt.java io/netty/handler/codec/http/websocketx/WebSocketUtil.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	ch/qos/logback/core/net/ssl/SSLContextFactoryBean.java com/amplitude/api/PinnedAmplitudeClient.java defpackage/C10244f40.java defpackage/C16531r75.java defpackage/C4370Ls3.java defpackage/C7619al6.java defpackage/C7863an0.java defpackage/TA4.java io/ktor/server/netty/NettyChannelInitializer.java io/netty/handler/ssl/JdkSslClientContext.java io/netty/handler/ssl/JdkSslServerContext.java io/netty/handler/ssl/ReferenceCountedOpenSslClientContext.java io/netty/handler/ssl/ReferenceCountedOpenSslServerContext.java io/netty/handler/ssl/SslContext.java io/netty/handler/ssl/util/FingerprintTrustManagerFactory.java io/netty/handler/ssl/util/FingerprintTrustManagerFactoryBuilder.java
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	io/ktor/network/sockets/TcpSocketBuilder.java io/ktor/server/application/ApplicationConfigExtensionsKt.java io/ktor/server/engine/CommandLineKt$buildCommandLineEnvironment$environment$1.java io/ktor/server/engine/EmbeddedServerKt.java io/ktor/server/engine/EngineConnectorBuilder.java io/ktor/server/engine/internal/EngineUtilsJvmKt.java io/netty/channel/epoll/LinuxSocket.java io/netty/handler/codec/http2/HttpConversionUtil.java io/netty/handler/ssl/SslContext.java io/netty/handler/ssl/util/OpenJdkSelfSignedCertGenerator.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	bo/content/b0.java bo/content/d6.java bo/content/e.java bo/content/f1.java bo/content/g6.java bo/content/h4.java bo/content/l0.java bo/content/l1.java bo/content/m.java bo/content/m0.java bo/content/m6.java bo/content/n0.java bo/content/r3.java bo/content/v5.java bo/content/w4.java bo/content/y0.java com/braze/configuration/RuntimeAppConfigurationProvider.java com/braze/managers/BrazeGeofenceManager.java defpackage/C11207go.java defpackage/C6466Vm.java
8	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/alltrails/alltrails/ui/recordingshare/a.java defpackage/C19073vX4.java defpackage/WY4.java
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	defpackage/Kb7.java
10	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/canhub/cropper/CropImageActivity.java defpackage/HN5.java defpackage/KI.java defpackage/ZQ.java io/ktor/http/cio/CIOMultipartDataBase.java io/netty/handler/codec/http/multipart/AbstractDiskHttpData.java io/netty/handler/ssl/util/SelfSignedCertificate.java io/netty/util/internal/NativeLibraryLoader.java io/netty/util/internal/PlatformDependent.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	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	ch/qos/logback/classic/android/SQLiteAppender.java com/alltrails/alltrails/db/a.java com/amplitude/api/DatabaseHelper.java defpackage/C11245gs5.java defpackage/C16076qF0.java defpackage/C20728yn5.java defpackage/EC.java
12	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	com/alltrails/alltrails/apiclient/MapDownloadDiskWriteInterceptor.java com/alltrails/alltrails/util/deeplink/DeepLinkParser.java com/appsflyer/internal/AFb1zSDK.java com/braze/support/StringUtils.java defpackage/C7175Yr3.java defpackage/C7442Zy0.java defpackage/PP2.java io/embrace/android/embracesdk/capture/metadata/EmbraceMetadataService.java io/ktor/client/plugins/cache/storage/FileCacheStorage.java io/netty/handler/codec/http/websocketx/WebSocketUtil.java
13	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	ch/qos/logback/core/android/AndroidContextUtil.java com/alltrails/alltrails/util/a.java defpackage/C15074oJ1.java defpackage/FS5.java defpackage/KI.java defpackage/ZQ.java
14	Weak Encryption algorithm used	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	defpackage/C7442Zy0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
15	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	defpackage/C7442Zy0.java
16	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	co/datadome/sdk/internal/CaptchaActivity.java sprig/graphics/h.java
17	This App uses SQL Cipher. Ensure that secrets are not hardcoded in code.	info	OWASP MASVS: MSTG-CRYPTO-1	com/alltrails/alltrails/db/a.java
18	This app has capabilities to prevent tapjacking attacks.	secure	OWASP MASVS: MSTG-PLATFORM-9	sprig/graphics/a.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/libdatadog-native-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	arm64-v8a/libarcore_sdk_c.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	arm64-v8a/libcrashlytics-trampoline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Position Independent Executable (PIE) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	arm64-v8a/libmapbox-maps.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__vsnprintf_chk', '__strncpy_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64-v8a/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	arm64-v8a/libarcore_sdk_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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	arm64-v8a/libandroid-tests-support-code.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	arm64-v8a/libcrashlytics-handler.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	arm64-v8a/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__read_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	arm64-v8a/libmapbox-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__vsnprintf_chk', '__read_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	arm64-v8a/libembrace-native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsprintf_chk', '__memmove_chk', '__strchr_chk', '__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	arm64-v8a/libcrashlytics.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	arm64-v8a/libcrashlytics-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__read_chk', '__strchr_chk', '__vsnprintf_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	x86_64/libdatadog-native-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	x86_64/libarcore_sdk_c.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	x86_64/libcrashlytics-trampoline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Position Independent Executable (PIE) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	x86_64/libmapbox-maps.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__vsnprintf_chk', '__strncpy_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	x86_64/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	x86_64/libarcore_sdk_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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	x86_64/libandroid-tests-support-code.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	x86_64/libcrashlytics-handler.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	x86_64/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__read_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	x86_64/libmapbox-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__vsnprintf_chk', '__read_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	x86_64/libembrace-native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strchr_chk', '__strlen_chk', '__vsprintf_chk', '__memcpy_chk', '__read_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
25	x86_64/libcrashlytics.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
26	x86_64/libcrashlytics-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__read_chk', '__strchr_chk', '__vsnprintf_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
27	armeabi-v7a/libdatadog-native-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
28	armeabi-v7a/libarcore_sdk_c.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
29	armeabi-v7a/libcrashlytics-trampoline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Position Independent Executable (PIE) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
30	armeabi-v7a/libmapbox-maps.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__vsnprintf_chk', '__strncpy_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
31	armeabi-v7a/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
32	armeabi-v7a/libarcore_sdk_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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
33	armeabi-v7a/libandroid-tests-support-code.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
34	armeabi-v7a/libcrashlytics-handler.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
35	armeabi-v7a/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
36	armeabi-v7a/libmapbox-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__vsnprintf_chk', '__read_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
37	armeabi-v7a/libembrace-native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strchr_chk', '__strlen_chk', '__vsprintf_chk', '__read_chk', '__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
38	armeabi-v7a/libcrashlytics.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
39	armeabi-v7a/libcrashlytics-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__read_chk', '__strchr_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
40	x86/libdatadog-native-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
41	x86/libarcore_sdk_c.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
42	x86/libcrashlytics-trampoline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Position Independent Executable (PIE) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
43	x86/libmapbox-maps.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__vsnprintf_chk', '__strncpy_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
44	x86/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
45	x86/libarcore_sdk_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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
46	x86/libandroid-tests-support-code.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
47	x86/libcrashlytics-handler.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
48	x86/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
49	x86/libmapbox-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__vsnprintf_chk', '__read_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
50	x86/libembrace-native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strchr_chk', '__strlen_chk', '__vsprintf_chk', '__memcpy_chk', '__read_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
51	x86/libcrashlytics.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
52	x86/libcrashlytics-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__read_chk', '__strchr_chk', '__vsnprintf_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
53	arm64-v8a/libdatadog-native-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
54	arm64-v8a/libarcore_sdk_c.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
55	arm64-v8a/libcrashlytics-trampoline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Position Independent Executable (PIE) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
56	arm64-v8a/libmapbox-maps.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__vsnprintf_chk', '__strncpy_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
57	arm64-v8a/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
58	arm64-v8a/libarcore_sdk_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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
59	arm64-v8a/libandroid-tests-support-code.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
60	arm64-v8a/libcrashlytics-handler.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
61	arm64-v8a/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__read_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
62	arm64-v8a/libmapbox-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__vsnprintf_chk', '__read_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
63	arm64-v8a/libembrace-native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsprintf_chk', '__memmove_chk', '__strchr_chk', '__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
64	arm64-v8a/libcrashlytics.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
65	arm64-v8a/libcrashlytics-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__read_chk', '__strchr_chk', '__vsnprintf_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
66	x86_64/libdatadog-native-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
67	x86_64/libarcore_sdk_c.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
68	x86_64/libcrashlytics-trampoline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Position Independent Executable (PIE) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
69	x86_64/libmapbox-maps.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__vsnprintf_chk', '__strncpy_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
70	x86_64/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
71	x86_64/libarcore_sdk_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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
72	x86_64/libandroid-tests-support-code.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
73	x86_64/libcrashlytics-handler.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
74	x86_64/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__read_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
75	x86_64/libmapbox-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__vsnprintf_chk', '__read_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
76	x86_64/libembrace-native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strchr_chk', '__strlen_chk', '__vsprintf_chk', '__memcpy_chk', '__read_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
77	x86_64/libcrashlytics.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
78	x86_64/libcrashlytics-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__read_chk', '__strchr_chk', '__vsnprintf_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
79	armeabi-v7a/libdatadog-native-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
80	armeabi-v7a/libarcore_sdk_c.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
81	armeabi-v7a/libcrashlytics-trampoline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Position Independent Executable (PIE) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
82	armeabi-v7a/libmapbox-maps.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__vsnprintf_chk', '__strncpy_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
83	armeabi-v7a/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
84	armeabi-v7a/libarcore_sdk_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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
85	armeabi-v7a/libandroid-tests-support-code.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
86	armeabi-v7a/libcrashlytics-handler.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
87	armeabi-v7a/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
88	armeabi-v7a/libmapbox-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__vsnprintf_chk', '__read_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
89	armeabi-v7a/libembrace-native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strchr_chk', '__strlen_chk', '__vsprintf_chk', '__read_chk', '__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
90	armeabi-v7a/libcrashlytics.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
91	armeabi-v7a/libcrashlytics-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__read_chk', '__strchr_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
92	x86/libdatadog-native-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
93	x86/libarcore_sdk_c.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
94	x86/libcrashlytics-trampoline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Position Independent Executable (PIE) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
95	x86/libmapbox-maps.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__vsnprintf_chk', '__strncpy_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
96	x86/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
97	x86/libarcore_sdk_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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
98	x86/libandroid-tests-support-code.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
99	x86/libcrashlytics-handler.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
100	x86/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
101	x86/libmapbox-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__memmove_chk', '__strlen_chk', '__vsnprintf_chk', '__read_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
102	x86/libembrace-native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strchr_chk', '__strlen_chk', '__vsprintf_chk', '__memcpy_chk', '__read_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
103	x86/libcrashlytics.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
104	x86/libcrashlytics-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__read_chk', '__strchr_chk', '__vsnprintf_chk', '__memmove_chk']	True info Symbols are stripped.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1iSDK.java defpackage/C5057Pa2.java defpackage/YM5.java
00078	Get the network operator name	collection telephony	bo/content/m0.java com/amplitude/api/AmplitudeUserProvider.java com/amplitude/api/DeviceInfo.java com/appsflyer/internal/AFa1iSDK.java com/mapbox/maps/module/telemetry/PhoneState.java defpackage/C15612pL0.java defpackage/C19197vn.java defpackage/YZ5.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/alltrails/alltrails/StartActivity.java com/alltrails/alltrails/track/service/ATWatchdog.java com/alltrails/alltrails/ui/homepage/HomepageActivity.java com/alltrails/alltrails/ui/homepage/d.java com/alltrails/alltrails/ui/navigator/i.java com/alltrails/alltrails/ui/parks/ParkActivity.java com/alltrails/alltrails/ui/recordingdetail/RecordingDetailActivity.java com/alltrails/alltrails/ui/recordingdetail/edit/RecordingEditActivity.java com/alltrails/alltrails/util/deeplink/DeepLinkParser.java com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFb1uSDK.java com/appsflyer/internal/AFd1oSDK.java com/braze/Braze.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/support/UriUtils.java defpackage/AbstractC5320Qf4.java defpackage/C12438j97.java defpackage/C13681lb6.java defpackage/C13952m83.java defpackage/C14228mg.java defpackage/C14295mo2.java defpackage/C15513p87.java defpackage/C16526r70.java defpackage/C17226sU5.java defpackage/CQ2.java defpackage/DialogInterfaceOnClickListenerC4176Kw.java defpackage/EH6.java defpackage/ML.java defpackage/NG0.java defpackage/WY4.java io/embrace/android/embracesdk/EmbraceAutomaticVerification.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	ch/qos/logback/classic/android/SQLiteAppender.java ch/qos/logback/core/FileAppender.java ch/qos/logback/core/android/AndroidContextUtil.java ch/qos/logback/core/rolling/helper/Compressor.java ch/qos/logback/core/rolling/helper/FileFinder.java ch/qos/logback/core/rolling/helper/RenameUtil.java com/alltrails/alltrails/apiclient/MapDownloadDiskWriteInterceptor.java com/appsflyer/internal/AFe1uSDK.java com/apptentive/android/sdk/conversation/LegacyConversationMetadataItem.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java com/datadog/android/ndk/internal/NdkCrashReportsFeature.java com/mapbox/common/CoreInitializer.java com/pandulapeter/beagle/core/util/ScreenCaptureService.java defpackage/B44.java defpackage/BatchId.java defpackage/C13113kU4.java defpackage/C15074oJ1.java defpackage/C17911to4.java defpackage/C20441yE0.java defpackage/C20941zD.java defpackage/C6855Xd3.java defpackage/C7175Yr3.java defpackage/C7938as3.java defpackage/C9821eE0.java defpackage/C9902eO1.java defpackage/HD.java defpackage/InterfaceC11022gR0.java defpackage/NE.java defpackage/PD.java defpackage/TO2.java defpackage/Y31.java io/embrace/android/embracesdk/ndk/EmbraceNdkService.java io/embrace/android/embracesdk/ndk/EmbraceNdkServiceRepository.java io/embrace/android/embracesdk/samples/AutomaticVerificationChecker.java io/ktor/server/http/content/CompressedFileType.java io/ktor/server/http/content/LocalFileContent.java io/netty/handler/codec/http/multipart/DiskFileUpload.java io/netty/util/internal/NativeLibraryLoader.java

RULE ID	BEHAVIOUR	LABEL	FILES
			bo/content/o0.java ch/qos/logback/core/joran/GenericConfigurator.java ch/qos/logback/core/joran/action/PropertyAction.java ch/qos/logback/core/rolling/helper/Compressor.java
00013	Read file and put it into a stream	file	ch/qos/logback/core/util/FileUtil.java com/appsflyer/internal/AFa1jSDK.java com/appsflyer/internal/AFe1uSDK.java com/apptentive/android/sdk/serialization/ObjectSerialization.java com/apptentive/android/sdk/storage/FileSerializer.java com/apptentive/android/sdk/util/Util.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java com/bumptech/glide/load/a.java com/mapbox/common/PlatformStreamFactoryKt.java defpackage/A24.java defpackage/C13828lu0.java defpackage/C14107mR0.java defpackage/C16612rH3.java defpackage/C17911to4.java defpackage/C1855An1.java defpackage/C20941zD.java defpackage/C2366Cn1.java defpackage/C7175Yr3.java defpackage/C7938as3.java defpackage/C8932cn1.java defpackage/C9902eO1.java defpackage/D74.java defpackage/IM2.java defpackage/KI6.java defpackage/P05.java defpackage/R02.java defpackage/Y31.java defpackage/ZQ.java io/embrace/android/embracesdk/capture/metadata/EmbraceMetadataService.java io/embrace/android/embracesdk/comms/delivery/EmbraceCacheService$loadPayload$1.java io/embrace/android/embracesdk/comms/delivery/EmbraceCacheService.java io/embrace/android/embracesdk/ndk/EmbraceNdkService.java io/ktor/client/plugins/cache/storage/FileCacheStorage.java io/ktor/http/cio/CIOMultipartDataBase$withTempFile$lazyInput$1.java io/ktor/server/engine/EnvironmentUtilsJvmKt.java io/ktor/server/netty/NettyChannelInitializer.java io/netty/handler/ssl/PemReader.java io/netty/handler/ssl/util/SelfSignedCertificate.java io/netty/resolver/HostsFileEntriesProvider.java

RULE ID	BEHAVIOUR	LABEL	FILES
			io/netty/util/internal/PlatformDependent.java ch/qos/logback/core/rolling/helper/Compressor.java ch/qos/logback/core/util/FileUtil.java defpackage/C13828lu0.java
00012	Read data and put it into a buffer stream	file	defpackage/D74.java defpackage/ZQ.java io/embrace/android/embracesdk/comms/delivery/EmbraceCacheService$loadPayload$1.java io/ktor/client/plugins/cache/storage/FileCacheStorage.java
00091	Retrieve data from broadcast	collection	com/alltrails/alltrails/community/feed/singlepost/SingleCommunityFeedPostActivity.java com/alltrails/alltrails/ui/guides/GuideActivity.java com/alltrails/alltrails/ui/homepage/HomepageActivity.java com/alltrails/alltrails/ui/parks/ParkActivity.java com/alltrails/alltrails/ui/parks/ParkDetailsActivity.java com/alltrails/alltrails/ui/user/stats/v2/UserStatsV2Activity.java com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFb1uSDK.java com/braze/push/BrazeNotificationUtils.java defpackage/C13682lb7.java defpackage/C13947m77.java defpackage/ML.java io/embrace/android/embracesdk/capture/crumbs/PushNotificationCaptureService.java
00096	Connect to a URL and set request method	command network	com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFc1mSDK.java com/appsflyer/internal/AFc1rSDK.java defpackage/C19465wJ0.java defpackage/C8869cf2.java defpackage/D42.java defpackage/ES.java defpackage/ZJ0.java
00089	Connect to a URL and receive input stream from the server	command network	com/appsflyer/internal/AFc1mSDK.java com/appsflyer/internal/AFc1rSDK.java defpackage/C14958o52.java defpackage/C19465wJ0.java defpackage/C8869cf2.java defpackage/D42.java defpackage/ES.java io/embrace/android/embracesdk/samples/VerificationActions.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFc1mSDK.java com/appsflyer/internal/AFc1rSDK.java com/appsflyer/internal/AFd1lSDK.java defpackage/C14958o52.java defpackage/C19465wJ0.java defpackage/C8869cf2.java defpackage/D42.java defpackage/ES.java io/embrace/android/embracesdk/samples/VerificationActions.java
00036	Get resource file from res/raw directory	reflection	com/alltrails/alltrails/ui/parks/ParkActivity.java com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFf1gSDK.java com/appsflyer/internal/AFf1iSDK.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/support/UriUtils.java defpackage/BQ2.java defpackage/C9902eO1.java defpackage/ML.java defpackage/S55.java defpackage/WY4.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/alltrails/alltrails/ui/homepage/d.java com/alltrails/alltrails/ui/parks/ParkActivity.java defpackage/AbstractC5320Qf4.java defpackage/C13681lb6.java defpackage/CQ2.java defpackage/DialogInterfaceOnClickListenerC4176Kw.java defpackage/EH6.java defpackage/ML.java io/embrace/android/embracesdk/EmbraceAutomaticVerification.java

RULE ID	BEHAVIOUR	LABEL	FILES
00162	Create InetSocketAddress object and connecting to it	socket	io/ktor/network/sockets/SocketImpl.java io/netty/bootstrap/Bootstrap.java io/netty/channel/AbstractChannel.java io/netty/channel/epoll/AbstractEpollChannel.java io/netty/channel/kqueue/AbstractKQueueChannel.java io/netty/channel/socket/nio/NioDatagramChannel.java io/netty/channel/socket/nio/NioSocketChannel.java io/netty/channel/socket/oio/OioDatagramChannel.java io/netty/channel/socket/oio/OioSocketChannel.java io/netty/handler/codec/DatagramPacketEncoder.java io/netty/util/internal/SocketUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00163	Create new Socket and connecting to it	socket	io/ktor/network/sockets/SocketImpl.java io/ktor/network/sockets/UDPSocketBuilderJvmKt.java io/netty/bootstrap/Bootstrap.java io/netty/channel/AbstractChannel.java io/netty/channel/AbstractChannelHandlerContext.java io/netty/channel/ChannelDuplexHandler.java io/netty/channel/ChannelOutboundHandlerAdapter.java io/netty/channel/CombinedChannelDuplexHandler.java io/netty/channel/DefaultChannelPipeline.java io/netty/channel/embedded/EmbeddedChannel.java io/netty/channel/epoll/AbstractEpollChannel.java io/netty/channel/kqueue/AbstractKQueueChannel.java io/netty/channel/socket/nio/NioDatagramChannel.java io/netty/channel/socket/nio/NioSocketChannel.java io/netty/channel/socket/oio/OioDatagramChannel.java io/netty/channel/socket/oio/OioSocketChannel.java io/netty/handler/address/DynamicAddressConnectHandler.java io/netty/handler/address/ResolveAddressHandler.java io/netty/handler/codec/DatagramPacketEncoder.java io/netty/handler/codec/http/HttpClientUpgradeHandler.java io/netty/handler/codec/http/websocketx/WebSocketClientProtocolHandler.java io/netty/handler/codec/http/websocketx/WebSocketProtocolHandler.java io/netty/handler/codec/http/websocketx/WebSocketServerProtocolHandler.java io/netty/handler/codec/http2/AbstractHttp2StreamChannel.java io/netty/handler/codec/http2/Http2ConnectionHandler.java io/netty/handler/codec/spdy/SpdyFrameCodec.java io/netty/handler/logging/LoggingHandler.java io/netty/handler/ssl/SslClientHelloHandler.java io/netty/handler/ssl/SslHandler.java io/netty/util/internal/SocketUtils.java
00030	Connect to the remote server through the given URL	network	com/appsflyer/internal/AFa1uSDK.java defpackage/C14958o52.java defpackage/C8869cf2.java defpackage/ZJ0.java
00137	Get last known location of the device	location collection	com/amplitude/api/DeviceInfo.java defpackage/C19197vn.java defpackage/RJ2.java

RULE ID	BEHAVIOUR	LABEL	FILES
00039	Start a web server	control network	ch/qos/logback/classic/net/SimpleSocketServer.java
00175	Get notification manager and cancel notifications	notification	com/alltrails/alltrails/manager/AuthenticationManager.java
00123	Save the response to JSON after connecting to the remote server	network command	bo/content/s1.java
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFf1hSDK.java defpackage/C7148Yo0.java
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFf1hSDK.java defpackage/C7148Yo0.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFf1hSDK.java defpackage/C7148Yo0.java
00187	Query a URI and check the result	collection sms calllog calendar	defpackage/C16650rM1.java defpackage/C7148Yo0.java
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFf1hSDK.java defpackage/C7148Yo0.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFa1eSDK.java com/appsflyer/internal/AFf1gSDK.java com/appsflyer/internal/AFf1hSDK.java defpackage/C7148Yo0.java defpackage/V46.java
00209	Get pixels from the latest rendered image	collection	defpackage/C4580Ms5.java
00210	Copy pixels from the latest rendered image into a Bitmap	collection	defpackage/C4580Ms5.java

RULE ID	BEHAVIOUR	LABEL	FILES
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFa1eSDK.java com/appsflyer/internal/AFf1gSDK.java com/appsflyer/internal/AFf1hSDK.java
00014	Read file into a stream and put it into a JSON object	file	com/appsflyer/internal/AFe1uSDK.java
00005	Get absolute path of file and put it to JSON object	file	com/appsflyer/internal/AFe1uSDK.java defpackage/C9821eE0.java
00033	Query the IMEI number	collection	bo/content/m0.java com/amplitude/api/AmplitudeUserProvider.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFa1eSDK.java
00115	Get last known location of the device	collection location	com/amplitude/api/DeviceInfo.java defpackage/C19197vn.java
00132	Query The ISO country code	telephony collection	com/amplitude/api/DeviceInfo.java defpackage/C19197vn.java
00034	Query the current data network type	collection network	com/mapbox/common/TelemetrySystemUtils.java
00083	Query the IMEI number	collection telephony	bo/content/m0.java
00028	Read file from assets directory	file	defpackage/C5331Qh.java
00112	Get the date of the calendar event	collection calendar	defpackage/C15229oc2.java defpackage/LT5.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

RULE ID	BEHAVIOUR	LABEL	FILES
00046	Method reflection	reflection	com/mapbox/common/module/provider/MapboxModuleProvider.java defpackage/C12614jV6.java
00026	Method reflection	reflection	com/mapbox/common/module/provider/MapboxModuleProvider.java defpackage/C17312sf2.java defpackage/C17837tf2.java
00016	Get location info of the device and put it to JSON object	location collection	com/amplitude/api/AmplitudeClient.java
00009	Put data in cursor to JSON object	file	com/amplitude/api/DatabaseHelper.java defpackage/C9821eE0.java
00003	Put the compressed bitmap data into JSON object	camera	io/branch/referral/network/a.java
00047	Query the local IP address	network collection	io/ktor/network/sockets/SocketImpl.java
00024	Write file after Base64 decoding	reflection file	defpackage/TO2.java
00204	Get the default ringtone	collection	com/alltrails/alltrails/ui/navigator/i.java
00195	Set the output path of the recorded file	record file	com/pandulapeter/beagle/core/util/ScreenCaptureService.java
00199	Stop recording and release recording resources	record	com/pandulapeter/beagle/core/util/ScreenCaptureService.java
00198	Initialize the recorder and start recording	record	com/pandulapeter/beagle/core/util/ScreenCaptureService.java
00007	Use absolute path of directory for the output media file path	file	com/pandulapeter/beagle/core/util/ScreenCaptureService.java
00196	Set the recorded file format and output path	record file	com/pandulapeter/beagle/core/util/ScreenCaptureService.java

RULE ID	BEHAVIOUR	LABEL	FILES
00031	Check the list of currently running applications	reflection collection	com/mapbox/common/LifecycleUtils.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://alltrails-com-api-project-127587500781.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/127587500781/namespaces/firebase:fetch?key=AIzaSyBiDQWtJlGkCXxlk8Kw2mrhr-YQ_1_lO3g. This is indicated by the response: The response code is 403

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.READ_CONTACTS, android.permission.VIBRATE
Other Common Permissions	4/44	android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
api.lab.eu.amplitude.com	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
privacy.alltrails.com	ok	**IP:** 18.155.173.91 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
flag.lab.eu.amplitude.com	ok	**IP:** 151.101.66.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api-events-config-staging.tilestream.net	ok	**IP:** 3.92.154.154 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
alltrails-com-api-project-127587500781.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
sconversions.s	ok	No Geolocation information available.
www.openssl.org	ok	**IP:** 34.49.79.89 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
smonitorsdk.s	ok	No Geolocation information available.
tools.ietf.org	ok	**IP:** 104.16.45.99 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.braze.com	ok	**IP:** 104.17.227.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
assets.mostpaths.com	ok	**IP:** 52.217.10.228 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
connectapi.garmin.com	ok	**IP:** 104.17.150.222 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
docs.mapbox.com	ok	**IP:** 18.238.96.47 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.mapbox.com	ok	**IP:** 199.232.196.143 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
support.alltrails.com	ok	**IP:** 216.198.54.6 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
youtrack.jetbrains.com	ok	**IP:** 63.33.88.220 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
braze-images.com	ok	**IP:** 104.19.152.69 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
opensource.org	ok	**IP:** 172.66.171.169 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
alpha.mostpaths.com	ok	**IP:** 18.238.96.60 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
crashpad.chromium.org	ok	**IP:** 172.253.124.121 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api2.amplitude.com	ok	**IP:** 54.200.134.180 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
terms.alltrails.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
raw.githubusercontent.com	ok	**IP:** 185.199.109.133 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
fonts.gstatic.com	ok	**IP:** 172.217.215.94 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
cdn-app-marketing.alltrails.com	ok	**IP:** 18.238.109.16 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sinapps.s	ok	No Geolocation information available.
api.amplitude.com	ok	**IP:** 52.13.248.80 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.eu.amplitude.com	ok	**IP:** 18.185.210.151 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
xml.org	ok	**IP:** 104.239.142.8 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
upload.wikimedia.org	ok	**IP:** 198.35.26.112 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.791256 **Longitude:** -122.400810 **View:** Google Map
weather-radar.alltrails.com	ok	**IP:** 18.238.109.54 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sgcdsdk.s	ok	No Geolocation information available.
sars.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
sondheim.braze.com	ok	**IP:** 172.64.144.252 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.eclipse.org	ok	**IP:** 198.41.30.198 **Country:** Canada **Region:** Ontario **City:** Ottawa **Latitude:** 45.345139 **Longitude:** -75.765076 **View:** Google Map
cdn-assets.alltrails.com	ok	**IP:** 18.238.96.9 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sregister.s	ok	No Geolocation information available.
fonts.googleapis.com	ok	**IP:** 142.250.9.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
1000logos.net	ok	**IP:** 104.26.8.175 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
slaunches.s	ok	No Geolocation information available.
events.mapbox.com	ok	**IP:** 44.241.67.103 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
ktor.io	ok	**IP:** 13.224.53.103 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
api.sprig.com	ok	**IP:** 50.19.89.137 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.mapbox.com	ok	**IP:** 18.238.109.38 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.112.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
simpression.s	ok	No Geolocation information available.
flag.lab.amplitude.com	ok	**IP:** 151.101.130.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 64.233.176.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	ok	**IP:** 142.251.15.105 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sattr.s	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
dash-api.embrace.io	ok	**IP:** 35.80.98.234 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
via.placeholder.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
api-sdk.datadome.co	ok	**IP:** 35.201.98.152 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
connect.garmin.com	ok	**IP:** 104.17.167.14 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api3-eu.branch.io	ok	**IP:** 18.155.173.13 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
pollen-daily.alltrails.com	ok	**IP:** 18.238.109.42 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
scdn-stestsettings.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
cdn.branch.io	ok	**IP:** 18.238.109.61 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
embrace.io	ok	**IP:** 18.238.109.60 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sonelink.s	ok	No Geolocation information available.
picsum.photos	ok	**IP:** 104.26.5.30 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
wiki.eclipse.org	ok	**IP:** 198.41.30.195 **Country:** Canada **Region:** Ontario **City:** Ottawa **Latitude:** 45.345139 **Longitude:** -75.765076 **View:** Google Map
sapp.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
search.yahoo.com	ok	**IP:** 98.136.144.138 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.731323 **Longitude:** -73.990089 **View:** Google Map
www.alltrails.com	ok	**IP:** 18.238.96.124 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sviap.s	ok	No Geolocation information available.
apps.mapbox.com	ok	**IP:** 18.238.109.99 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api.lab.amplitude.com	ok	**IP:** 151.101.194.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
config.mapbox.com	ok	**IP:** 54.201.75.83 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
tiles-wtopo.alltrails.com	ok	**IP:** 18.238.109.27 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
onetreeplanted.org	ok	**IP:** 23.227.38.32 **Country:** Canada **Region:** Ontario **City:** Ottawa **Latitude:** 45.418877 **Longitude:** -75.696510 **View:** Google Map
sdk.iad-01.braze.com	ok	**IP:** 104.18.39.68 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 172.253.124.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.
cloudfront-staging.tilestream.net	ok	**IP:** 18.155.173.115 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
logback.qos.ch	ok	**IP:** 159.100.250.151 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map
api-events-staging.tilestream.net	ok	**IP:** 44.253.46.158 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	**IP:** 159.100.250.151 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map
scdn-ssettings.s	ok	No Geolocation information available.
netty.io	ok	**IP:** 104.21.3.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
httpbin.org	ok	**IP:** 54.224.121.164 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
sstats.s	ok	No Geolocation information available.
www.docs.developers.amplitude.com	ok	**IP:** 66.33.60.34 **Country:** Canada **Region:** Ontario **City:** Etobicoke **Latitude:** 43.623768 **Longitude:** -79.559723 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api2.branch.io	ok	**IP:** 18.238.109.117 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
svalidate.s	ok	No Geolocation information available.

EMAILS

EMAIL	FILE
this@copy.slice	io/ktor/util/NIOKt.java
support@embrace.io	io/embrace/android/embracesdk/EmbraceAutomaticVerification.java
support@embrace.io	io/embrace/android/embracesdk/ndk/EmbraceNdkService.java
automated@embrace.io	io/embrace/android/embracesdk/samples/VerificationActions.java
support@alltrails.com android-support@alltrails.com support@embrace.io	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Amplitude	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/125
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Apptentive	Analytics	https://reports.exodus-privacy.eu.org/trackers/115
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
OpenTelemetry (OpenCensus, OpenTracing)	Analytics	https://reports.exodus-privacy.eu.org/trackers/412

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"settings_legal_section_key" : "settings_legal_section"
"preference_key_display_speed" : "preference_display_speed"
"api_url" : "https://{host}/api/alltrails/"

POSSIBLE SECRETS
"preference_key_notifications" : "preference_key_notifications"
"api_subdomain" : "www"
"preference_key_version_number" : "preference_key_version_number"
"localization_key_en_US" : "en-US"
"preference_key_marketing_language" : "preference_key_marketing_language"
"localization_key_en_GB" : "en-GB"
"preference_key_email_us" : "preference_key_email_us"
"localization_key_fr" : "fr"
"apptentive_app_key" : "ANDROID-ALLTRAILS-HIKING-BIKING"
"preference_key_3d_maps" : "preference_key_3d_maps"
"preference_key_map_tile_layer" : "map_layer"
"com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key"
"api_production_baseurl" : "api-v5.alltrails.com"
"mapbox_access_token" : "pk.eyJ1IjoiYWxsdHJhaWxzIiwiYSI6IkZGaGhGLWsifQ.Fl0FrDM8-xonRV6x2HFqcw"
"preference_key_open_source_attribution" : "open_source_attribution"
"api_alpha_baseurl" : "alpha.mostpaths.com"
"com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key"

POSSIBLE SECRETS
"localization_key_pt_BR" : "pt-BR"
"preference_key_identity_service" : "identity_service"
"preference_key_logout" : "logout"
"settings_version_section_key" : "settings_version_section"
"facebook_client_token" : "3ee3630f3dc9f87382b8be9a70e8b201"
"preference_key_restore_purchase" : "restore_purchase"
"preference_key_calorie_info" : "preference_key_calorie_info"
"localization_key_es_ES" : "es-ES"
"settings_delete_account_section_key" : "settings_delete_account_section_key"
"input_password" : "Password"
"branch_io_key" : "key_live_pncDSeYT1WCuC2yVQ37WqhjmyrgHBgYt"
"preference_key_delete_account" : "delete_account"
"settings_section_key_open_source_attribution" : "settings_section_key_open_source_attribution"
"preference_key_privacy" : "preference_key_privacy"
"localization_key_nb_NO" : "nb-NO"
"preference_key_help_center" : "preference_key_help_center"
"localization_key_sv_SE" : "sv-SE"

POSSIBLE SECRETS
"localization_key_es_MX" : "es-MX"
"preference_key_advanced" : "preference_key_advanced"
"preference_key_downloaded_map_layers" : "preference_key_downloaded_map_layers"
"settings_logout_section_key" : "settings_logout_section"
"preference_key_health_connect" : "health_connect"
"preference_key_unit_system" : "units"
"localization_key_nl_NL" : "nl-NL"
"localization_key_pt_PT" : "pt-PT"
"google_api_key" : "AIzaSyBiDQWtJlGkCXxlk8Kw2mrhr-YQ_1_lO3g"
"mapbox_style_name_key" : "name_en"
"settings_section_key_identity_service" : "settings_section_key_identity_service"
"datadome_sdk_key" : "9D463B509A4C91FDFF39B265B3E2BC"
"com_appboy_api_key" : "466272d2-3f07-4dde-a222-0d0726e9dd85"
"preference_key_terms_of_use" : "preference_key_terms_of_use"
"amplitude_analytics_api_key" : "6ad463d0a0517d79a350cc1af0e37030"
"settings_support_section_key" : "settings_support_section"
"mapbox_style_n_key" : "n:en"

POSSIBLE SECRETS
"localization_key_en" : "en"
"preference_key_gps_tracking" : "preference_key_gps_tracking"
"settings_preferences_section_key" : "settings_preferences_section"
"settings_account_section_key" : "settings_account_section"
"datadog_client_token" : "pube783908e9408643d097eabb6b3b796cf"
"localization_key_pl_PL" : "pl-PL"
"localization_key_es" : "es"
"google_maps_v2_key" : "AIzaSyDskHlZuQm4EfJbHfjjFjTqw7eNvXhqOzI"
"preference_key_email_preferences" : "preference_key_email_preferences"
"privacy_preference_level_private" : "Private"
"api_key" : "4b4a5f6e0a5a7e6a5c0d1b7b5b2b3a8d"
"settings_data_section_key" : "settings_data_section"
"localization_key_de_DE" : "de-DE"
"preference_key_debug_drawer" : "preference_key_debug_drawer"
"garmin_access_token" : "https://connectapi.garmin.com/oauth-service-1.0/oauth/access_token?hl=en-gb"
"localization_key_it_IT" : "it-IT"
"com.google.firebase.crashlytics.mapping_file_id" : "1085a94089374bb78379915ba6f306dc"

POSSIBLE SECRETS
"preference_key_privacy_policy" : "preference_key_privacy_policy"
"preference_key_contact_settings" : "contact_settings"
"com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key"
"preference_key_download_preferred_network" : "download_preferred_network"
"preference_key_subscription" : "preference_key_subscription"
"google_crash_reporting_api_key" : "AIzaSyBiDQWtJlGkCXxlk8Kw2mrhr-YQ_1_lO3g"
"localization_key_da_DK" : "da-DK"
"preference_key_coordinate_system" : "coordinate_system"
"firebase_database_url" : "https://alltrails-com-api-project-127587500781.firebaseio.com"
"preference_key_garmin_connect" : "garmin_connect"
"preference_key_log_level" : "preference_key_log_level"
"amplitude_experiments_api_key" : "client-jGDFfUr9kSH6TBhMYMkAYqgg4lYFAoB5"
"private_achievement_cta" : "Done"
"com_appboy_firebase_cloud_messaging_sender_id" : "127587500781"
"localization_key_fr_FR" : "fr-FR"
"settings_debug_drawer_section_key" : "settings_debug_drawer_section"
"notification_channel_key_product_push_offers_discounts" : "product_push_offers_discounts"

POSSIBLE SECRETS
"preference_key_rate" : "preference_rate"
"garmin_request_token" : "https://connectapi.garmin.com/oauth-service-1.0/oauth/request_token?hl=en-gb"
"localization_key_de" : "de"
"preference_key_login_with_facebook" : "facebook_connect"
e3f1f98c9da02a93bb547f448b472d727e14b22455235796fe49863856252508
9douHjmTTjq3N4YYUdzzHaKyxIqsB5K92p8t26vKQB1HahpVak+32YHan4LmgLPE
V8P78mWO+MxnWR283vMX+BSDXEvrm8XlQCYXMpvUe5w=
c8c3bf7dabfed1b04cb67711d0fe4d41
3fysZeGzwX+hqd2f4+qtlSho+oF+DeFl9kzKrTFOSWo=
c56fb7d591ba6704df047fd98f535372fea00211
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
37a6259cc0c1dae299a7866489dff0bd
36864200e0eaf5284d884a0e77d31646
Rx5KxmHu63h8QT7T4cYR2mu7F4LQnYkocG/Azb9HP8ZHyjUHnRxxCuB99BIp3kbl
9b8f518b086098de3d77736f9458a3d2f6f95a37
QcEEfK1PwFv2Eb+NZQ+4kWKAUUVvycYqoBzmAjBexJV/sKEjaFlajeD5MAZYWXy5
cd1558d10f8b6f831bf6cd28516711e1

POSSIBLE SECRETS
JAIugkcNQRXP51pRzjbhWzeihtmzLSCJCmT0+GTbkts=
18f5703f0fff7a5ae57b7813270d22768bde6c9c
1uVTEMqJXNO1ycCqSNk6EYRiPtrme925F7DFntRPfMA
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
669eb6644dbbfe0059b2233b
avDZD6/xoSbFYvWCy23XLncB75oD5DxKdrTKFY2O0hY=
Kx8fghNUQq+sA+EfmK6qh0KjuKvw753ECuaCFV8szVM=
7d73d21f1bd82c9e5268b6dcf9fde2cb
t+CAjrsoEFEWDgC/oCfdqxFl31lIReQPqb6CaFb+1Y0=
fHaUCxrr3fcbpdQPVJw6OSoHeHoizr6wmxmAsnLvDUhuNG2u8ebKX4VPxAoXSx4W
6JHAw9/xzu8LcH4q9f7Udi9sTntehS9dfukXhX8DEHhp54WYBhd6ZhWkqnOAMGmY
eyJ1IjoiYWxsdHJhaWxzIiwiYSI6ImNqM294YW9scDAwaTUyeGxqZzMycDR6YTIifQ
a0784d7a4716f3feb4f64e7f4b39bf04
u7Ufq5yuXkEXg69T8jpWuOOX55Q9g2DSVI1gtbNUvY8=
ngqbGKXcQCvq0ft27xRzOzNoEVN+ei+Vq2+CNx9QQMc=
bFK3lRg0oaTUwYDrSsMiLa/j4LG9nRll5KKEyt63x08=
9c5cd697-f581-4667-a6b4-0eaf634f6839

POSSIBLE SECRETS
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
eUrWQVF8FAlcOLX3Auj55rxdEWjF+0P5JAPLCHVKKQw=
vvYcBqgl4aoC3GZZ7n1bdLp71k52s6EJLh0/nA6ME39LmvOZf3TBZ+H4xg1YfQXg
l4qa5EABhdRHJHltXD4U8dy0wNZl4oyoZ9TbFONnMI4=
ZdMwT5n8r4APV4u4GhQlb1VCwOIVHkTm7kF7LnArEpyZnsv+C3G3q6fVFgtTcqcc
af60eb711bd85bc1e4d3e0a462e074eea428a8
5kY1EQ+6snGNdZX1BEywItRy0EAwZ4DbRiPucqHAgfZR8kr75HzXIMEIf0cE9z11
eb050193f1d7c5cd5000f9ebbe5fbf42
c76b9b6a188d43a09957c13e835bc6a2fe7ac772-
0njjbCFUq6vJ1UgnErUI7KEtLgZLN7V9IJ5yZ3QtzXmjMaTjzKInpeDNakYTgh0P
KvkOAoll09ZSAixqGUOtipMDBdKXVlslzVnQOpfDZOEJW+xbFKrK173Gu3h1RVkI
308203c7308202afa003020102021500dc286b43b4ea12039958a00a6655eb84720e46c9300d06092a864886f70d01010b05003074310b3009060355040613025553311330110603550408130a43616c69666f726e69631163014060355040713074d6d6f756e7461696e2056696577311430120603550a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f6964311030 0e06035504031307416e64726f6964301e170d313730383034313635333337 5a170d343730383034313635333337 5a3074310b3009060355040613025553311330110603550408130a43616c69666f726e69631163014060355040713074d6d6f756e7461696e2056696577311430120603550a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f6964311030 0e06035504031307416e64726f696430820122300d06092a864886f70d01010105000382010f003082010a0282010100898646f47fc333db09644c303104ed183e904e351152aa66a603b77f63389d45d6fcffae3c94fadf1f28038e265d697fea347327f9081a7f0b9074d5b148db5bf357c611a77f87f844a15068818bdcd5b21d187e93fa2551676170eedce04a150c35ec0a791eef507fa9b406573c36f6f207764842e5677e35a281a422659e91e26eb4fecfb053b5c936d0976c37f8757adb57a37953da5844ea350695854d343a61ad341b63a1c425d22855af7ebfee018e1736cee98536be5b9947f288e2a26f99eb9f91b5de93fecc513019d2e90f12b38610d1f02eaa81deca4ce91c19cbce36d6c3025ce2432b3d178616beafaf437c08451bc469c6bc6f4517a714a5b0203010001a350304e300c0603551d13040530030101ff301d0603551d0e0416041419a864c0f2618c67c803a23da909bc70521f269b301f0603551d2304183016801419a864c0f2618c67c803a23da909bc70521f269b300d06092a864886f70d01010b05000382010100 5403fc56fdefc440376a0337815002b96a15bffc2fe42de6c58f52fae4d80652e3704455b885409eef81ffbb4c44dba104b6b8e24c9e2e0e7a04338ee73baa5b71bfb4488f8e04bef3d0eaf7d43aa42b03b278c33cc1f0dd3802571624baa161d851fab37db4bc92b9094b6885dff62b400ecd81f069d56a1be1db46d8198c50c9628cdb6e38686ef640fd386775f50376f957e24ea45ed1942968f20c82f189607fdb22f11cfdfd0760a77a60ceb3416cfb3f48f13f9f83f3834a01001750a7c78bc1fd81f0b53a7c41dcba9f5a0118259d083c32bb9ebb84d645d6f6b9c31923d8ab70e7f0a25940ecc9f4945144419f86e8c421d3b99774f4b8f3d09262e7

POSSIBLE SECRETS
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
71d36257d6aaafef511024c339ee3ab2
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
UUyjIKRMwm9dKsgSX9dILJo74EfxEEGHjLInD5uOP1Y
ab520490251b31f0671914d7d3e5e34b4a242d44179283a9fb5b8d3d73c9ffbc079f06e0ebc82442a08515439c95b5ef841d6b6c4331cc5e83882aad76954e36
SKSJAjN3UKeguXyEasCGg04d/yJuUN8XZYgactMp4rfMtHcIJcD0mydl5RKvI49M
cc2751449a350f668590264ed76692694a80308a
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
tnRfJM39LV6MDlXml8e8fAfi5JhKcsRyFSmagsP97rbE/0XgA5fRVLlLbAYUcu57
FLgp79R6LGLnWDio6G1XBjsjORgKSjLkdakyn5bigQludVyQtVZMhDAlppvakfKf
bae8e37fc83441b16034566b
5e82a9b1ef16278b4f3375f65d4c8276
O+vmm8flr2e7ZrTWUx/T8ClWwcEwLlJlfjM8sMGjZbg=
TvLSh+Eka5RyCXMK4IvAvP4vfksx/KqJwxjzSKu7qQs=
Kq6mcF8LH4HqXGyg5/DR3VvLtDExNTPXoCRIPhkdOGM=
470fa2b4ae81cd56ecbcda9735803434cec591fa
AMztxBQmasdCMrU1nlH2RhtlfSPsjcYFxTHFmKvCDYM=

POSSIBLE SECRETS
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
GC4CZUnPsyUcm5NrWw7C8gSktjb/gtBCDrSKBLlqImuOnQy7zHyo6XlIzkH3EMVH
gYgEHbtWs2qrOou4Pi9x8/evNQKl7xufkAwk8FBwpKpll2nmAbj5wvKo77J2SETY
648e62bb52b0ede1d54dcd77a6bab440
8E4cUkgIY9w8/0qt+Oeyh9wfu9tQKpeKsR+Ou+hsYewuB4uFdKW1FI4W+bAZwe0B
3071c8717539de5d5353f4c8cd59a032
f7fcf08ede68cd69702f6ee982576776
6jGSPrUM0+2YrTO2vsTOKq3+XL/IfUFs5oxZaSEvsQg=
WfvM4SeNDVyFarUKUVpVTE2MRQkjnaN4GpgwC5lMrmyQkCennlTSSkgCAZvzOVXK
5c4ece41241a1bb513f6e3e5df74ab7d5183dfffbd71bfd43127920d880569fd
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
alltrails/cjp90np3z44xz2rofjvdakfbh
YmluLm10LnNpZ25hdHVyZS5raWxsZXI=
K/sgHSTVeE1LLZ4HP+m5KF6ND+k7W4ID3M3VTul8bAI=

POSSIBLE SECRETS
9ObkV+9nuY0gPBNLH25GoxM7YATuF1pi7IORvVFb3+Q=
s16u0iwtqlokf4v9cpgne8a2amdrxz735hjby
23456789abcdefghjkmnpqrstvwxyz
19a305b603e6fda59e410c021d4eabe5
5HcA415u1KU8m2yVlDZBhQQK+0IFNRmmWPxuAq0DnfPzSdJ/uWlnYMD1kKfkH6cZ
NtWyZSC7qBNyKPaXbOjRpNaZGUUAwpDpvYkB4v1ZH9M=
M2RhhRYJhjrQUa7n9jg23IBcTQvCkUFLA/9ZbQYvHFo=
0yxvRSsGg+/BBPRqwe1F54W0T+vv1NRnE+jebtT36Vo=
iz9pI8M74OdFMOjBXhk6CVKK/c29GtinDT3TfbuphLdYOSnoV+Rg8WuW9whaa7rD
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e696131163014060355040713074d6d6f756e7461696e20566965773114301206035504 0a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e060355040313074 16e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071307 30d4d6f756e7461696e20566965773114301206035504 0a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071307 30d4d6f756e7461696e20566965773114301206035504 0a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d01010405000382010100 6dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
71ef40d0900b3f24adbc1c55a95d6099

POSSIBLE SECRETS
9ea53b67ff01665eaab02fa48b7dbbe1
LYoHKR17UvbUNibqKPKJklawQJNaw1zk7CnhZAC68YBTzC7x4MYQVXp9Sihs98Ok
808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
B3EEABB8EE11C2BE770B684D95219ECB
SHfJbyMgI7MrHewwYoTmYsM7CTkziBSZ0pvzhPCRWcLGoNw6AaEZWLqlKa0dpKuD
Aoh1zDQKnhHKR6WU12sd1IK2kgbKdTw3gNy
d7YRusR2mxxBt1bBYjK2gXVvJl/MfqFw2IiZZVeFOFqksQBErGXLOKgf56kYtWpK
g3h/WBQ8k1SqFyNwcX6aXlyabMyZPKS0QgL4qcVfix1Xl+70++CdiHkDZKRlUPQw
lnMUlT0qopStslq/RfZHkyvg0xAUTVuMPsMot4SEaYA=
SkMlFTLt8H3eQLYvgf87g2pXBfp4xPpxL3RMs974XSU=
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d01010405003081943 10b3009060355040613025553311330110603550408130a43616c69666f726e6961 3116301406035504071 30d4d6f756e7461696e2056696577311030 0e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e060355040 31307416e64726f 6964312230200609 2a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333635365a170d333530393031323333635365a308194310b30 0906035504061302555331133011060355040813 0a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e2056696577311030 0e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e060355040 31307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d060 92a864886f70d01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3 990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56a ae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc8 7dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c 61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e2056696577311030 0e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e060355040 31307416e64726f6964312230200609 2a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff3 00d06092a864886f70d01010405000382010100 19d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca 1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8 aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff 6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b

POSSIBLE SECRETS
SxHy+zpC+eGmQUPW4BYYcldQdVxiSSVnY0gIrWauGKU=

PLAYSTORE INFORMATION

Title: AllTrails: Hike, Bike & Run

Score: 4.683502 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.alltrails.alltrails

Developer Details: AllTrails, LLC, AllTrails,+LLC, None, https://www.alltrails.com, android-support@alltrails.com,

Release Date: Sep 13, 2011 **Privacy Policy:** Privacy link

Description:

Whether you hike, bike, run, or walk, AllTrails is your companion and guide to the outdoors. Find detailed reviews and inspiration from a community of trail-goers like you. We'll help you plan, live, and share your outdoor adventures. AllTrails offers more than a running app or fitness activity tracker. It's built on the idea that the outside isn't a place to seek, but rather a part of us all. Custom route planning helps you search for dog-friendly, kid-friendly, stroller-friendly, or wheelchair-friendly trails, and more. ◆ Discover trails: Search over 450,000 trails around the world by location, interest, skill level, and more. ◆ Plan your next adventure: Get in-depth trail info, from reviews to conditions to GPS driving directions — and save your favorite trails for later. ◆ Stay on course: Stick to your planned route or chart your own course with confidence when you navigate on the trail with your phone or Wear OS device. Use Wear OS to leverage tiles and complications to start and monitor your activities. ◆ Grow your community: Celebrate outdoor adventures and find inspiration by connecting with trail-goers like you. ◆ Share your outdoor adventures: Easily post trails and activities on Facebook, Instagram, or WhatsApp. Discover trails that fit your nature. Trails for workout planners, hikers, walkers, mountain bikers, trail runners, and casual cyclists. Whether you're pushing your limits or pushing a stroller, there's something out there for everyone. Let AllTrails help you find it. ► Do more outdoors with AllTrails+ ► Spend less time figuring out where you want to be, and more time enjoying where you are. With offline maps, wrong-turn alerts, and extra safety and planning features, your annual subscription gives you more tools for more adventures. ◆ Search by distance from you to find the closest trails. ◆ Unplug completely or pack a backup with printed maps. ◆ Explore without service with map downloads for trails, parks, and entire areas. ◆ Live share your trail activity with friends and family. ◆ Prepare for the hills ahead: Follow topo maps and trail maps in 3D. ◆ Focus on the view, not the map, with wrong-turn alerts. ◆ Record your activity with stats and photos of your favorite hiking trails. ◆ Give back: AllTrails donates a portion of every subscription to 1% for the Planet. ◆ Explore ad-free: Remove occasional ads by subscribing ► New! Explore to the fullest with AllTrails Peak ► Make the most of your time on the trail with our newest premium membership. Chart your own course, plan ahead for conditions, and explore popular trails — with all the offline benefits of Plus. ◆ Create your own route from scratch, or modify one of 450,000+ existing trails. ◆ Plan for the elements like ground conditions, weather, air quality, UV index, and more. ◆ See how conditions change along the trail and preview by time of day. ◆ Explore the most popular places with heatmaps of recent trail activity. ◆ Access every Plus and Base feature, too. Whether you're geocaching in a national park, browsing bucket-list mountain bike routes, or planning a trail run to clear your head, AllTrails Plus and Peak make the great outdoors even greater.

SCAN LOGS

Timestamp	Event	Error

2025-08-29 19:29:05	Generating Hashes	OK
2025-08-29 19:29:05	Extracting APK	OK
2025-08-29 19:29:05	Unzipping	OK
2025-08-29 19:29:07	Parsing APK with androguard	OK
2025-08-29 19:29:07	Extracting APK features using aapt/aapt2	OK
2025-08-29 19:29:07	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 19:29:11	Parsing AndroidManifest.xml	OK
2025-08-29 19:29:11	Extracting Manifest Data	OK
2025-08-29 19:29:11	Manifest Analysis Started	OK
2025-08-29 19:29:11	Reading Network Security config from network_security_config.xml	OK
2025-08-29 19:29:11	Parsing Network Security config	OK
2025-08-29 19:29:11	Performing Static Analysis on: AllTrails (com.alltrails.alltrails)	OK

2025-08-29 19:29:12	Fetching Details from Play Store: com.alltrails.alltrails	OK
2025-08-29 19:29:12	Checking for Malware Permissions	OK
2025-08-29 19:29:12	Fetching icon path	OK
2025-08-29 19:29:13	Library Binary Analysis Started	OK
2025-08-29 19:29:13	Analyzing lib/arm64-v8a/libdatadog-native-lib.so	OK
2025-08-29 19:29:13	Analyzing lib/arm64-v8a/libarcore_sdk_c.so	OK
2025-08-29 19:29:13	Analyzing lib/arm64-v8a/libcrashlytics-trampoline.so	OK
2025-08-29 19:29:13	Analyzing lib/arm64-v8a/libmapbox-maps.so	OK
2025-08-29 19:29:13	Analyzing lib/arm64-v8a/libandroidx.graphics.path.so	OK
2025-08-29 19:29:13	Analyzing lib/arm64-v8a/libarcore_sdk_jni.so	OK
2025-08-29 19:29:13	Analyzing lib/arm64-v8a/libandroid-tests-support-code.so	OK
2025-08-29 19:29:13	Analyzing lib/arm64-v8a/libcrashlytics-handler.so	OK

2025-08-29 19:29:13	Analyzing lib/arm64-v8a/libc++_shared.so	OK
2025-08-29 19:29:14	Analyzing lib/arm64-v8a/libmapbox-common.so	OK
2025-08-29 19:29:14	Analyzing lib/arm64-v8a/libembrace-native.so	OK
2025-08-29 19:29:14	Analyzing lib/arm64-v8a/libcrashlytics.so	OK
2025-08-29 19:29:14	Analyzing lib/arm64-v8a/libcrashlytics-common.so	OK
2025-08-29 19:29:14	Analyzing lib/x86_64/libdatadog-native-lib.so	OK
2025-08-29 19:29:14	Analyzing lib/x86_64/libarcore_sdk_c.so	OK
2025-08-29 19:29:14	Analyzing lib/x86_64/libcrashlytics-trampoline.so	OK
2025-08-29 19:29:14	Analyzing lib/x86_64/libmapbox-maps.so	OK
2025-08-29 19:29:14	Analyzing lib/x86_64/libandroidx.graphics.path.so	OK
2025-08-29 19:29:14	Analyzing lib/x86_64/libarcore_sdk_jni.so	OK
2025-08-29 19:29:14	Analyzing lib/x86_64/libandroid-tests-support-code.so	OK

2025-08-29 19:29:14	Analyzing lib/x86_64/libcrashlytics-handler.so	OK
2025-08-29 19:29:14	Analyzing lib/x86_64/libc++_shared.so	OK
2025-08-29 19:29:14	Analyzing lib/x86_64/libmapbox-common.so	OK
2025-08-29 19:29:14	Analyzing lib/x86_64/libembrace-native.so	OK
2025-08-29 19:29:14	Analyzing lib/x86_64/libcrashlytics.so	OK
2025-08-29 19:29:14	Analyzing lib/x86_64/libcrashlytics-common.so	OK
2025-08-29 19:29:14	Analyzing lib/armeabi-v7a/libdatadog-native-lib.so	OK
2025-08-29 19:29:14	Analyzing lib/armeabi-v7a/libarcore_sdk_c.so	OK
2025-08-29 19:29:14	Analyzing lib/armeabi-v7a/libcrashlytics-trampoline.so	OK
2025-08-29 19:29:14	Analyzing lib/armeabi-v7a/libmapbox-maps.so	OK
2025-08-29 19:29:14	Analyzing lib/armeabi-v7a/libandroidx.graphics.path.so	OK
2025-08-29 19:29:14	Analyzing lib/armeabi-v7a/libarcore_sdk_jni.so	OK

2025-08-29 19:29:14	Analyzing lib/armeabi-v7a/libandroid-tests-support-code.so	OK
2025-08-29 19:29:14	Analyzing lib/armeabi-v7a/libcrashlytics-handler.so	OK
2025-08-29 19:29:14	Analyzing lib/armeabi-v7a/libc++_shared.so	OK
2025-08-29 19:29:14	Analyzing lib/armeabi-v7a/libmapbox-common.so	OK
2025-08-29 19:29:14	Analyzing lib/armeabi-v7a/libembrace-native.so	OK
2025-08-29 19:29:14	Analyzing lib/armeabi-v7a/libcrashlytics.so	OK
2025-08-29 19:29:14	Analyzing lib/armeabi-v7a/libcrashlytics-common.so	OK
2025-08-29 19:29:14	Analyzing lib/x86/libdatadog-native-lib.so	OK
2025-08-29 19:29:14	Analyzing lib/x86/libarcore_sdk_c.so	OK
2025-08-29 19:29:14	Analyzing lib/x86/libcrashlytics-trampoline.so	OK
2025-08-29 19:29:14	Analyzing lib/x86/libmapbox-maps.so	OK
2025-08-29 19:29:14	Analyzing lib/x86/libandroidx.graphics.path.so	OK

2025-08-29 19:29:14	Analyzing lib/x86/libarcore_sdk_jni.so	OK
2025-08-29 19:29:14	Analyzing lib/x86/libandroid-tests-support-code.so	OK
2025-08-29 19:29:14	Analyzing lib/x86/libcrashlytics-handler.so	OK
2025-08-29 19:29:14	Analyzing lib/x86/libc++_shared.so	OK
2025-08-29 19:29:14	Analyzing lib/x86/libmapbox-common.so	OK
2025-08-29 19:29:14	Analyzing lib/x86/libembrace-native.so	OK
2025-08-29 19:29:14	Analyzing lib/x86/libcrashlytics.so	OK
2025-08-29 19:29:14	Analyzing lib/x86/libcrashlytics-common.so	OK
2025-08-29 19:29:14	Analyzing apktool_out/lib/arm64-v8a/libdatadog-native-lib.so	OK
2025-08-29 19:29:14	Analyzing apktool_out/lib/arm64-v8a/libarcore_sdk_c.so	OK
2025-08-29 19:29:14	Analyzing apktool_out/lib/arm64-v8a/libcrashlytics-trampoline.so	OK
2025-08-29 19:29:14	Analyzing apktool_out/lib/arm64-v8a/libmapbox-maps.so	OK

2025-08-29 19:29:14	Analyzing apktool_out/lib/arm64-v8a/libandroidx.graphics.path.so	OK
2025-08-29 19:29:14	Analyzing apktool_out/lib/arm64-v8a/libarcore_sdk_jni.so	OK
2025-08-29 19:29:14	Analyzing apktool_out/lib/arm64-v8a/libandroid-tests-support-code.so	OK
2025-08-29 19:29:14	Analyzing apktool_out/lib/arm64-v8a/libcrashlytics-handler.so	OK
2025-08-29 19:29:14	Analyzing apktool_out/lib/arm64-v8a/libc++_shared.so	OK
2025-08-29 19:29:14	Analyzing apktool_out/lib/arm64-v8a/libmapbox-common.so	OK
2025-08-29 19:29:14	Analyzing apktool_out/lib/arm64-v8a/libembrace-native.so	OK
2025-08-29 19:29:14	Analyzing apktool_out/lib/arm64-v8a/libcrashlytics.so	OK
2025-08-29 19:29:14	Analyzing apktool_out/lib/arm64-v8a/libcrashlytics-common.so	OK
2025-08-29 19:29:14	Analyzing apktool_out/lib/x86_64/libdatadog-native-lib.so	OK
2025-08-29 19:29:14	Analyzing apktool_out/lib/x86_64/libarcore_sdk_c.so	OK
2025-08-29 19:29:14	Analyzing apktool_out/lib/x86_64/libcrashlytics-trampoline.so	OK

2025-08-29 19:29:14	Analyzing apktool_out/lib/x86_64/libmapbox-maps.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/x86_64/libandroidx.graphics.path.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/x86_64/libarcore_sdk_jni.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/x86_64/libandroid-tests-support-code.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/x86_64/libcrashlytics-handler.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/x86_64/libc++_shared.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/x86_64/libmapbox-common.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/x86_64/libembrace-native.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/x86_64/libcrashlytics.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/x86_64/libcrashlytics-common.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/armeabi-v7a/libdatadog-native-lib.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/armeabi-v7a/libarcore_sdk_c.so	OK

2025-08-29 19:29:15	Analyzing apktool_out/lib/armeabi-v7a/libcrashlytics-trampoline.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/armeabi-v7a/libmapbox-maps.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/armeabi-v7a/libandroidx.graphics.path.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/armeabi-v7a/libarcore_sdk_jni.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/armeabi-v7a/libandroid-tests-support-code.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/armeabi-v7a/libcrashlytics-handler.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/armeabi-v7a/libc++_shared.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/armeabi-v7a/libmapbox-common.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/armeabi-v7a/libembrace-native.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/armeabi-v7a/libcrashlytics.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/armeabi-v7a/libcrashlytics-common.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/x86/libdatadog-native-lib.so	OK

2025-08-29 19:29:15	Analyzing apktool_out/lib/x86/libarcore_sdk_c.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/x86/libcrashlytics-trampoline.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/x86/libmapbox-maps.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/x86/libandroidx.graphics.path.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/x86/libarcore_sdk_jni.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/x86/libandroid-tests-support-code.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/x86/libcrashlytics-handler.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/x86/libc++_shared.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/x86/libmapbox-common.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/x86/libembrace-native.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/x86/libcrashlytics.so	OK
2025-08-29 19:29:15	Analyzing apktool_out/lib/x86/libcrashlytics-common.so	OK

2025-08-29 19:29:15	Reading Code Signing Certificate	OK
2025-08-29 19:29:16	Running APKiD 2.1.5	OK
2025-08-29 19:29:34	Detecting Trackers	OK
2025-08-29 19:29:47	Decompiling APK to Java with JADX	OK
2025-08-29 19:30:38	Converting DEX to Smali	OK
2025-08-29 19:30:38	Code Analysis Started on - java_source	OK
2025-08-29 19:30:57	Android SBOM Analysis Completed	OK
2025-08-29 19:31:17	Android SAST Completed	OK
2025-08-29 19:31:17	Android API Analysis Started	OK
2025-08-29 19:31:36	Android API Analysis Completed	OK
2025-08-29 19:31:37	Android Permission Mapping Started	OK
2025-08-29 19:31:53	Android Permission Mapping Completed	OK

2025-08-29 19:31:54	Android Behaviour Analysis Started	OK
2025-08-29 19:32:22	Android Behaviour Analysis Completed	OK
2025-08-29 19:32:22	Extracting Emails and URLs from Source Code	OK
2025-08-29 19:32:48	Email and URL Extraction Completed	OK
2025-08-29 19:32:48	Extracting String data from APK	OK
2025-08-29 19:32:48	Extracting String data from SO	OK
2025-08-29 19:32:50	Extracting String data from Code	OK
2025-08-29 19:32:50	Extracting String values and entropies from Code	OK
2025-08-29 19:33:11	Performing Malware check on extracted domains	OK
2025-08-29 19:33:21	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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.