ANDROID STATIC ANALYSIS REPORT

iSharing (11.19.2.2)

File Name:	iSharing_merged.apk
Package Name:	com.isharing.isharing
Scan Date:	Aug. 11, 2024, 10:56 a.m.

App Security Score:	46/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	8/432

FINDINGS SEVERITY

🐞 HIGH	⚠ MEDIUM	ℹ INFO	✓ SECURE	🔍 HOTSPOT
7	45	3	2	1

FILE INFORMATION

File Name: iSharing_merged.apk
Size: 58.18MB
MD5: 32f07a4c761f147bf65f16f6c64560c1
SHA1: 25a74838d116fc7718f7d36414ab59c7632eaec1
SHA256: e406e211d60e822348a5326670882919657494e5304a1065656d10cb328625ce

APP INFORMATION

App Name: iSharing
Package Name: com.isharing.isharing
Main Activity: com.isharing.isharing.ui.IntroActivity
Target SDK: 33
Min SDK: 24
Max SDK:
Android Version Name: 11.19.2.2
Android Version Code: 1680

APP COMPONENTS

Activities: 60
Services: 46
Receivers: 47
Providers: 19
Exported Activities: 6
Exported Services: 14
Exported Receivers: 11
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: L=seoul, O=isharing, OU=isharing, CN=yongjae
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-04-20 14:56:09+00:00
Valid To: 2112-03-27 14:56:09+00:00
Issuer: L=seoul, O=isharing, OU=isharing, CN=yongjae
Serial Number: 0x4f917909
Hash Algorithm: sha1
md5: 81f3a9672237aa45b7b7478c422bcdf9
sha1: 2d88831167adb4bb62cf277e6cc2222acf557e71

sha256: 3e1efb8491cad067937093a48c063758a2258414b46361faff494a08fa893058
sha512: 4459a370f2edb5ba1a95afa072689dc14c7a501a2d4b2e90605b4e3468091ab2a0d2bccd80ea8bf0bc3c6b2399fea142d7acfb295ed7e6ada1776f377f7278eb
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: e71391c2ea7650a3d25d5b2b2a64cd57b9293a74836b0ba1e25fe3dfb027f103
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.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_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
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.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.DISABLE_KEYGUARD	normal	disable keyguard	Allows applications to disable the keyguard if it is not secure.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.
android.permission.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.

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.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.isharing.isharing.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS	
	FINDINGS	DETAILS
classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check network operator name check ro.hardware check ro.kernel.qemu check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8 without marker (suspicious)

<table>
<tr><th>FILE</th><th>DETAILS</th></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
possible Build.SERIAL check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></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.TAGS 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>classes4.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
SIM operator check
network operator name check
subscriber ID check
ro.kernel.qemu 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>classes5.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
com.isharing.isharing.ui.IntroActivity	Schemes: isharing://, http://, https://, kakao8cd991e35fb326e134ccc9755d7b82d7://, Hosts: membership_screen, paywall_screen, manage_notification_screen, inbox_screen, friend_search_screen, group_creation_screen, share_my_location_screen, my_driving_report_screen, my_location_history_screen, open, invite, open_email, isharing.page.link, bnc.lt, isharing.onelink.me, app.isharing.me, kakaolink, Mime Types: image/*, text/plain, Path Prefixes: /IpBl, /qVcT,
com.isharing.isharing.ui.MainActivity	Schemes: isharing://, Hosts: get_shared_map_url,

ACTIVITY	INTENT
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.com.isharing.isharing,
com.kakao.sdk.auth.AuthCodeHandlerActivity	Schemes: kakao8cd991e35fb326e134ccc9755d7b82d7://, Hosts: oauth,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,
com.linecorp.linesdk.auth.internal.LineAuthenticationCallbackActivity	Schemes: lineauth://,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	10.0.2.2 localhost 34.232.55.43 44.209.243.231 3.223.107.206	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 SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **34** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
4	Activity (com.isharing.isharing.ui.MainActivity) 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	Activity (com.isharing.isharing.ui.ShareExtActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Broadcast Receiver (com.appsflyer.MultipleInstallBroadcastReceiver) 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.
7	Broadcast Receiver (com.isharing.isharing.receiver.InstallTrackerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [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.
8	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.
9	TaskAffinity is set for activity (com.isharing.isharing.avoidsmartmanager.AvoidSmartManagerActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
10	Broadcast Receiver (com.umlaut.crowd.receiver.InsightReceiver) 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.
11	Service (io.huq.sourcekit.service.HIVisitSubmissionJob) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
12	Service (io.huq.sourcekit.service.HIDeviceInformationSubmissionJob) 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	Service (io.huq.sourcekit.wifi.HIWifiJobService) 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.
14	Service (io.huq.sourcekit.wifi.HICellularJobService) 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.
15	Service (io.huq.sourcekit.wifi.HIRepeatingNetworkJobService) 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.
16	Service (io.huq.sourcekit.service.HIPeriodicListeningJobService) 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.
17	Broadcast Receiver (io.huq.sourcekit.location.HIGeofenceReceiver) 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.
18	Broadcast Receiver (io.huq.sourcekit.location.HILocationReceiver) 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.
19	Broadcast Receiver (io.huq.sourcekit.service.HIBootReceiver) 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.
20	TaskAffinity is set for activity (com.braze.push.NotificationTrampolineActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.

NO	ISSUE	SEVERITY	DESCRIPTION
21	Activity (com.google.firebase.auth.internal.GenericIdpActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
22	Activity (com.google.firebase.auth.internal.RecaptchaActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
23	Activity (com.linecorp.linesdk.auth.internal.LineAuthenticationCallbackActivity) 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.
24	Broadcast Receiver (com.cumberland.sdk.core.broadcast.receiver.BootReceiver) 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.
25	Service (com.cumberland.sdk.core.provider.HeartbeatProvider$HeartbeatJobService) 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.
26	Service (com.cumberland.sdk.core.service.StartSdkJobService) 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.
27	Service (com.cumberland.sdk.core.service.SyncJobService) 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.
28	Service (com.cumberland.sdk.core.domain.controller.sampling.SdkSamplingController$SdkSampleJobService) 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.
29	Service (com.cumberland.sdk.core.repository.kpi.web.WebAnalysisJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
30	Service (com.applozic.mobicomkit.uiwidgets.KmFirebaseMessagingService) 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.
31	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.
32	Broadcast Receiver (com.applozic.mobicomkit.broadcast.TimeChangeBroadcastReceiver) 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.
33	Broadcast Receiver (com.applozic.mobicomkit.broadcast.ConnectivityReceiver) 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.
34	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.
35	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.
36	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.

CODE ANALYSIS

HIGH: **3** | WARNING: **10** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a1/c.java a4/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a4/e.java ap/b.java ap/d.java b4/a.java b5/h0.java b7/d.java c5/g0.java com/amazonaws/logging/AndroidLog.java com/amazonaws/logging/LogFactory.java com/amazonaws/mobileconnectors/cognito/internal/storage/CognitoSyncStorage.java com/amazonaws/mobileconnectors/cognito/internal/storage/SQLiteLocalStorage.java com/applozic/mobicomkit/api/attachment/AttachmentTask.java com/applozic/mobicommons/commons/core/utils/DBUtils.java com/applozic/mobicommons/commons/core/utils/LocationUtils.java com/applozic/mobicommons/commons/image/ImageLoader.java com/applozic/mobicommons/commons/image/PhotoDecodeRunnable.java com/applozic/mobicommons/file/LocalStorageProvider.java com/appsflyer/internal/AFb1tSDK.java com/appsflyer/internal/AFc1oSDK.java com/appsflyer/internal/AFf1iSDK.java com/appsflyer/internal/AFg1oSDK.java com/braze/support/BrazeLogger.java com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/c.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java com/bumptech/glide/request/target/d.java com/bumptech/glide/request/target/k.java com/cumberland/sdk/core/broadcast/receiver/HeartbeatReceiver.java com/cumberland/sdk/core/broadcast/receiver/SdkReceiver.java com/cumberland/sdk/core/database/sdk/SdkDatabaseHelper.java com/cumberland/sdk/core/database/sdk/changes/WeplanSdkDatabaseChange.java com/cumberland/sdk/core/domain/controller/sampling/SdkSamplingController.java com/cumberland/sdk/core/domain/serializer/GsonSerializer.java com/cumberland/sdk/core/permissions/PermissionRepository.java com/cumberland/sdk/core/permissions/model/UsageStatsPermission.java com/cumberland/sdk/core/provider/HeartbeatProvider.java com/cumberland/sdk/core/provider/HostProvider.java com/cumberland/sdk/core/repository/kpi/mobility/ActivityRecognizedService.java com/cumberland/sdk/core/repository/kpi/web/WebAnalysisJavascriptReceiver.java com/cumberland/sdk/core/repository/kpi/web/WebAnalysisJobService.java com/cumberland/sdk/core/repository/kpi/web/WebViewWebAnalysisDataSource.java com/cumberland/sdk/core/repository/sqlite/OrmLiteBasicDataSource.java com/cumberland/sdk/core/repository/sqlite/sdk/SyncableSdkDataOrmLiteDataSource.java com/cumberland/sdk/core/repository/sqlite/sdk/datasource/OrmLiteLocationCellDataSource.java com/cumberland/sdk/core/repository/sqlite/sdk/datasource/OrmLitePingD

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ataSource.java com/cumberland/sdk/core/repository/sqlite/sdk/datasource/SqlAppCellTrafficDataSource.java com/cumberland/sdk/core/repository/sqlite/sdk/datasource/SqlAppUsageDataSource.java com/cumberland/sdk/core/repository/sqlite/sdk/datasource/SqlBatteryDataSource.java com/cumberland/sdk/core/repository/sqlite/sdk/datasource/SqlCellDataDataSource.java com/cumberland/sdk/core/repository/sqlite/sdk/datasource/SqlCellIdentityDataSource.java com/cumberland/sdk/core/repository/sqlite/sdk/datasource/SqlLocationGroupDataSource.java com/cumberland/sdk/core/repository/sqlite/sdk/datasource/SqlPreferenceDataSource$getPreference$1.java com/cumberland/sdk/core/repository/sqlite/sdk/datasource/SqlWifiScanSnapshotDataSource.java com/cumberland/sdk/core/repository/sqlite/sdk/datasource/SqliteWifiProviderDataSource.java com/cumberland/sdk/core/repository/sqlite/user/datasource/OldAccessTokenDataSource.java com/cumberland/sdk/core/repository/sqlite/user/datasource/SqlSdkSimDataSource.java com/cumberland/sdk/core/repository/sqlite/user/datasource/SqlUserInfoDataSource.java com/cumberland/sdk/core/service/StartSdkJobService.java com/cumberland/sdk/core/service/SyncJobService.java com/cumberland/sdk/core/service/a.java com/cumberland/utils/location/repository/ApiLocationRepository.java com/cumberland/utils/location/repository/datasource/GoogleApiLocationClient$WrappedGoogleLocationResult$location$2.java com/cumberland/utils/location/repository/datasource/GoogleApiLocationClient.java com/cumberland/weplansdk/a6.java com/cumberland/weplansdk/az.java com/cumberland/weplansdk/b10.java com/cumberland/weplansdk/b5.java com/cumberland/weplansdk/be.java com/cumberland/weplansdk/c6.java com/cumberland/weplansdk/d.java com/cumberland/weplansdk/di.java com/cumberland/weplansdk/dq.java com/cumberland/weplansdk/e10.java com/cumberland/weplansdk/e3.java com/cumberland/weplansdk/e7.java com/cumberland/weplansdk/e9.java com/cumberland/weplansdk/ef.java com/cumberland/weplansdk/ek.java com/cumberland/weplansdk/el.java com/cumberland/weplansdk/ew.java com/cumberland/weplansdk/fa.java com/cumberland/weplansdk/fb.java com/cumberland/weplansdk/fc.java com/cumberland/weplansdk/fw.java com/cumberland/weplansdk/g10.java com/cumberland/weplansdk/gi.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/cumberland/weplansdk/gj.java com/cumberland/weplansdk/gq.java com/cumberland/weplansdk/gs.java com/cumberland/weplansdk/hn.java com/cumberland/weplansdk/hp.java com/cumberland/weplansdk/jp.java com/cumberland/weplansdk/ju.java com/cumberland/weplansdk/k.java com/cumberland/weplansdk/kb.java com/cumberland/weplansdk/kh.java com/cumberland/weplansdk/km.java com/cumberland/weplansdk/kv.java com/cumberland/weplansdk/l0.java com/cumberland/weplansdk/lb.java com/cumberland/weplansdk/lp.java com/cumberland/weplansdk/ls.java com/cumberland/weplansdk/mg.java com/cumberland/weplansdk/mn.java com/cumberland/weplansdk/n6.java com/cumberland/weplansdk/nd.java com/cumberland/weplansdk/nt.java com/cumberland/weplansdk/nw.java com/cumberland/weplansdk/op.java com/cumberland/weplansdk/ot.java com/cumberland/weplansdk/pl.java com/cumberland/weplansdk/ps.java com/cumberland/weplansdk/pt.java com/cumberland/weplansdk/py.java com/cumberland/weplansdk/q.java com/cumberland/weplansdk/q8.java com/cumberland/weplansdk/qg.java com/cumberland/weplansdk/r0.java com/cumberland/weplansdk/r8.java com/cumberland/weplansdk/rb.java com/cumberland/weplansdk/rf.java com/cumberland/weplansdk/rn.java com/cumberland/weplansdk/rx.java com/cumberland/weplansdk/rz.java com/cumberland/weplansdk/s2.java com/cumberland/weplansdk/s7.java com/cumberland/weplansdk/sb.java com/cumberland/weplansdk/sj.java com/cumberland/weplansdk/sm.java com/cumberland/weplansdk/t00.java com/cumberland/weplansdk/td.java com/cumberland/weplansdk/tw.java com/cumberland/weplansdk/tz.java com/cumberland/weplansdk/ub.java com/cumberland/weplansdk/uc.java com/cumberland/weplansdk/un.java com/cumberland/weplansdk/uo.java com/cumberland/weplansdk/ut.java com/cumberland/weplansdk/ve.java com/cumberland/weplansdk/vn.java com/cumberland/weplansdk/vp.java com/cumberland/weplansdk/wi.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/cumberland/weplansdk/wt.java com/cumberland/weplansdk/wx.java com/cumberland/weplansdk/xh.java com/cumberland/weplansdk/xx.java com/cumberland/weplansdk/y3.java com/cumberland/weplansdk/ye.java com/cumberland/weplansdk/ym.java com/cumberland/weplansdk/yp.java com/cumberland/weplansdk/z00.java com/cumberland/weplansdk/zk.java com/cumberland/weplansdk/zq.java com/cumberland/weplansdk/zw.java com/cumberland/weplansdk/zz.java com/imagepicker/b.java com/imagepicker/g.java com/isharing/AppReview.java com/isharing/DataCollector$requestConsentStatus$1$1.java com/isharing/DataCollector$requestJurisdictionNative$1.java com/isharing/DataCollector.java com/isharing/isharing/AddressBook.java com/isharing/isharing/AddressCache.java com/isharing/isharing/Analytics.java com/isharing/isharing/AsyncTask.java com/isharing/isharing/AutoRetry.java com/isharing/isharing/CRMManager.java com/isharing/isharing/ChatManager.java com/isharing/isharing/ChatStoreFS.java com/isharing/isharing/ClientFactory.java com/isharing/isharing/ClientManager.java com/isharing/isharing/DataStore.java com/isharing/isharing/DiskCache.java com/isharing/isharing/DrivingDataStore.java com/isharing/isharing/EmojiPagerAdapter.java com/isharing/isharing/EmojiReactionView.java com/isharing/isharing/EmojiUtil.java com/isharing/isharing/EmojiView.java com/isharing/isharing/EngageMonitor.java com/isharing/isharing/Executors.java com/isharing/isharing/ExecutorsRejectedHandler.java com/isharing/isharing/FriendManager.java com/isharing/isharing/FriendRefreshThreadPoolExecutor.java com/isharing/isharing/FriendRequest.java com/isharing/isharing/HistoryDataHelper.java com/isharing/isharing/InitProvider.java com/isharing/isharing/ItemConstants.java com/isharing/isharing/ItemManager.java com/isharing/isharing/LinkPreview.java com/isharing/isharing/LocalPush.java com/isharing/isharing/Location.java com/isharing/isharing/LocationManagerNative.java com/isharing/isharing/LocationPermissionActivity.java com/isharing/isharing/LocationRetryQueue.java com/isharing/isharing/LocationUpdateManager.java com/isharing/isharing/Log.java com/isharing/isharing/MainApplication.java com/isharing/isharing/MapSnapshot$takeSnapshot$bitmap$1.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/isharing/isharing/MapSnapshot$takeSnapshotWithMarker$2.java com/isharing/isharing/MapSnapshot.java com/isharing/isharing/MapSnapshotCache.java com/isharing/isharing/NativeAdsManager.java com/isharing/isharing/Notification.java com/isharing/isharing/OfferManager.java com/isharing/isharing/PersonImageHelper.java com/isharing/isharing/PushManager.java com/isharing/isharing/PushMessage.java com/isharing/isharing/RLog.java com/isharing/isharing/ReactActivity.java com/isharing/isharing/ReactBridge.java com/isharing/isharing/ReactCompassActivity.java com/isharing/isharing/ReactOfferActivity.java com/isharing/isharing/ReactStartActivity.java com/isharing/isharing/RemoteConfig.java com/isharing/isharing/RemotePref.java com/isharing/isharing/SensorEventStore.java com/isharing/isharing/ShareMap$generate$1.java com/isharing/isharing/ShareMap$getSharedMapURL$2.java com/isharing/isharing/ShareMap.java com/isharing/isharing/ShareShortCuts.java com/isharing/isharing/ShareStory$getStoryInvitationImage$1.java com/isharing/isharing/ShareStory.java com/isharing/isharing/Social.java com/isharing/isharing/TinyDB.java com/isharing/isharing/TransitionRecognitionGMS.java com/isharing/isharing/UserManager.java com/isharing/isharing/VoiceMessageHandler.java com/isharing/isharing/ads/InterstitialAdsAdmob.java com/isharing/isharing/ads/RewardAdsAdmob.java com/isharing/isharing/ads/RewardManager.java com/isharing/isharing/avoidsmartmanager/AvoidSmartManagerActivity.java com/isharing/isharing/avoidsmartmanager/AvoidSmartManagerReceiver.java com/isharing/isharing/aws/HttpClient.java com/isharing/isharing/aws/LambdaClient.java com/isharing/isharing/collector/CollectorA.java com/isharing/isharing/collector/CollectorH.java com/isharing/isharing/collector/CollectorO.java com/isharing/isharing/collector/CollectorP.java com/isharing/isharing/collector/CollectorW.java com/isharing/isharing/gms/ActivityRecognitionGMS.java com/isharing/isharing/gms/BillingServiceRevenueCat.java com/isharing/isharing/gms/LocationManagerGMS.java com/isharing/isharing/gms/PlaceGeofenceGMS.java com/isharing/isharing/gms/PushManagerGMS.java com/isharing/isharing/lu/helpers/LogCatLogPrinter.java com/isharing/isharing/map/GeocoderGMS.java com/isharing/isharing/map/MapAdapter.java com/isharing/isharing/map/MapAdapterGMS.java com/isharing/isharing/map/MapAdapterNaver.java com/isharing/isharing/map/MarkerInfo.java com/isharing/isharing/receiver/ActivityRecognitionReceiver.java com/isharing/isharing/receiver/BootReceiver.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/isharing/isharing/receiver/FcmListenerService.java com/isharing/isharing/receiver/InstallTrackerReceiver.java com/isharing/isharing/receiver/LocalPushReceiver.java com/isharing/isharing/receiver/LocationUpdateBroadcastReceiver.java com/isharing/isharing/receiver/NotificationBroadcastReceiver.java com/isharing/isharing/receiver/PackageUpdateReceiver.java com/isharing/isharing/receiver/PowerStatusReceiver.java com/isharing/isharing/receiver/TransitionRecognitionReceiver.java com/isharing/isharing/service/DeviceMotionForegroundService.java com/isharing/isharing/service/GeofenceService.java com/isharing/isharing/service/LocationHistoryUpdateForegroundService.java com/isharing/isharing/service/LocationSendForegroundService.java com/isharing/isharing/service/LocationUpdateForegroundService.java com/isharing/isharing/service/LocationUpdateServiceBase.java com/isharing/isharing/service/LocationUpdateServiceGMS.java com/isharing/isharing/service/LocationUpdateServiceNative.java com/isharing/isharing/ui/AllowLocationActivity.java com/isharing/isharing/ui/ChatActivity.java com/isharing/isharing/ui/ChatContentAdapter.java com/isharing/isharing/ui/ChatMessageAdapter.java com/isharing/isharing/ui/ChatNewMessageAdapter.java com/isharing/isharing/ui/FriendListAdapter.java com/isharing/isharing/ui/FriendListView.java com/isharing/isharing/ui/IntroActivity.java com/isharing/isharing/ui/MainActivity.java com/isharing/isharing/ui/MenuActivity.java com/isharing/isharing/ui/NotificationActionActivity.java com/isharing/isharing/ui/PremiumServiceActivity.java com/isharing/isharing/ui/PromoBannerButton.java com/isharing/isharing/ui/ShareExtActivity.java com/isharing/isharing/ui/SharedExtFriendAdapter.java com/isharing/isharing/ui/StreetViewActivity.java com/isharing/isharing/ui/locations/MapBaseActivity.java com/isharing/isharing/ui/walkietalkie/PlayListActivity.java com/isharing/isharing/ui/walkietalkie/TalkActivity.java com/isharing/isharing/util/AutostartUtil.java com/isharing/isharing/util/ConsentCollector.java com/isharing/isharing/util/ExtAudioRecorder.java com/isharing/isharing/util/LocationUpdateTracker.java com/isharing/isharing/util/LocationUtil.java com/isharing/isharing/util/PermissionUtil.java com/isharing/isharing/util/TransitionRecognitionUtil.java com/isharing/isharing/util/Util.java com/isharing/isharing/view/ChatContentView.java com/isharing/isharing/view/ChatNewMessageView.java com/isharing/isharing/view/ChatView.java com/isharing/isharing/view/FriendInfoView.java com/isharing/isharing/view/RateAccuracyDialog.java com/isharing/isharing/view/UserInfoView.java com/isharing/isharing/work/AvoidSmartManagerWorker.java com/isharing/isharing/work/LastActivityDetectWorker.java com/isharing/isharing/work/LocalPushWorker.java com/isharing/isharing/work/LocationSendRetryWorker.java com/isharing/isharing/work/LocationSendWorker.java com/isharing/isharing/work/LocationUpdateWorker.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/isharing/isharing/work/PromoBannerWorker.java com/isharing/isharing/work/StatusCheckerWorker.java com/j256/ormlite/android/AndroidLog.java com/j256/ormlite/android/apptools/OrmLiteConfigUtil.java com/j256/ormlite/table/BaseSchemaUtils.java com/naver/maps/map/log/a.java com/reactnative/ivpusic/imagepicker/f.java com/revenuecat/purchases/common/DefaultLogHandler.java com/umlaut/crowd/database/StatsDatabase.java com/umlaut/crowd/internal/BT.java com/umlaut/crowd/internal/CDC.java com/umlaut/crowd/internal/CLC.java com/umlaut/crowd/internal/CT.java com/umlaut/crowd/internal/a5.java com/umlaut/crowd/internal/a6.java com/umlaut/crowd/internal/a8.java com/umlaut/crowd/internal/aa.java com/umlaut/crowd/internal/ad.java com/umlaut/crowd/internal/b.java com/umlaut/crowd/internal/b6.java com/umlaut/crowd/internal/bc.java com/umlaut/crowd/internal/c.java com/umlaut/crowd/internal/d1.java com/umlaut/crowd/internal/dd.java com/umlaut/crowd/internal/e.java com/umlaut/crowd/internal/ee.java com/umlaut/crowd/internal/h9.java com/umlaut/crowd/internal/jc.java com/umlaut/crowd/internal/l7.java com/umlaut/crowd/internal/n.java com/umlaut/crowd/internal/p1.java com/umlaut/crowd/internal/pc.java com/umlaut/crowd/internal/q7.java com/umlaut/crowd/internal/s.java com/umlaut/crowd/internal/sd.java com/umlaut/crowd/internal/t.java com/umlaut/crowd/internal/u1.java com/umlaut/crowd/internal/uc.java com/umlaut/crowd/internal/v.java com/umlaut/crowd/internal/v3.java com/umlaut/crowd/internal/wd.java com/umlaut/crowd/internal/x.java com/umlaut/crowd/internal/y1.java com/umlaut/crowd/manager/VoWifiTestManager.java com/umlaut/crowd/service/ConnectivityJobService.java com/umlaut/crowd/service/InsightJobService.java com/umlaut/crowd/threads/ThreadManager.java d4/c.java d4/e.java e0/c.java e0/d.java e0/h.java e4/h.java e4/i.java e4/k.java e4/z.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				e4/z.java ee/b1.java ee/l4.java ek/a.java f0/k1.java f0/m0.java f0/n0.java f0/s0.java f4/i.java f4/k.java f5/l.java fk/a.java fk/f.java fq/g.java fr/a.java fr/greweb/reactnativeviewshot/RNViewShotModule.java fr/greweb/reactnativeviewshot/a.java g4/e.java g4/i.java g5/e.java g5/f.java gd/c.java gd/f.java gk/b.java h4/a.java hd/h.java hd/l.java hd/n.java hf/i.java i1/a.java i4/c.java i4/d.java i4/f.java i4/s.java i4/t.java i5/a.java ij/d.java io/didomi/sdk/Didomi.java io/didomi/sdk/Log.java io/didomi/sdk/a0.java io/didomi/sdk/b9.java io/didomi/sdk/c7.java io/didomi/sdk/e1.java io/didomi/sdk/e7.java io/didomi/sdk/f.java io/didomi/sdk/f0.java io/didomi/sdk/f6.java io/didomi/sdk/hh.java io/didomi/sdk/i1.java io/didomi/sdk/ja.java io/didomi/sdk/k6.java io/didomi/sdk/l.java io/didomi/sdk/l7.java io/didomi/sdk/m.java io/didomi/sdk/m6.java io/didomi/sdk/ng.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/didomi/sdk/pg.java io/didomi/sdk/qf.java io/didomi/sdk/r7.java io/didomi/sdk/s0.java io/didomi/sdk/s5.java io/didomi/sdk/s8.java io/didomi/sdk/t0.java io/didomi/sdk/ub.java io/didomi/sdk/uf.java io/didomi/sdk/x0.java io/didomi/sdk/xb.java io/didomi/sdk/y9.java io/didomi/sdk/zf.java k3/u.java k4/l.java k5/i.java kf/c0.java kg/n.java l4/c.java l4/e.java l4/h0.java l4/k0.java l4/m.java l4/t.java l4/u.java l4/z.java la/i.java li/a.java li/e.java li/h.java lk/c.java mj/e.java mj/k.java nd/e.java net/sqlcipher/AbstractCursor.java net/sqlcipher/BulkCursorToCursorAdaptor.java net/sqlcipher/DatabaseUtils.java net/sqlcipher/DefaultDatabaseErrorHandler.java net/sqlcipher/database/SQLiteDatabase.java net/sqlcipher/database/SQLiteDebug.java net/sqlcipher/database/SQLiteOpenHelper.java net/sqlcipher/database/SQLiteQueryBuilder.java net/sqlcipher/database/SqliteWrapper.java o0/x.java org/tinylog/writers/ConsoleWriter.java p4/a.java p4/d.java p4/j.java pc/q.java r4/e.java r4/f.java r4/o.java r4/p.java r4/r.java r4/s.java s/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				s0/c.java s4/e.java s6/f.java t/k.java t/l.java ti/d.java u4/j.java ua/a.java v/f.java w4/b.java x/a.java x/b.java x/c.java x/d.java y/e.java y/f.java y/g.java y/h.java y/j.java y/k.java y/l.java y/m.java y/p.java y/r.java y/s.java y/u.java y/v.java y0/a.java y0/b.java y1/e.java y4/a.java y7/e0.java
				bo/app/k5.java c4/h.java com/amazonaws/auth/CognitoCachingCredentialsProvider.java com/amazonaws/auth/policy/conditions/ConditionFactory.java com/amazonaws/auth/policy/conditions/S3ConditionFactory.java com/amazonaws/internal/keyvaluestore/AWSKeyValueStore.java com/amazonaws/internal/keyvaluestore/KeyProvider18.java com/amazonaws/mobileconnectors/cognito/internal/storage/SQLiteLocalStorage.java com/amazonaws/mobileconnectors/kinesis/kinesisrecorder/JSONRecordAdapter.java com/amazonaws/mobileconnectors/s3/transferutility/TransferObserver.java com/amazonaws/mobileconnectors/s3/transferutility/TransferTable.java com/amazonaws/services/s3/Headers.java com/amazonaws/services/s3/model/S3ObjectSummary.java com/applozic/mobicomkit/api/account/register/RegistrationResponse.java com/applozic/mobicomkit/api/account/user/UserClientService.java com/applozic/mobicomkit/api/attachment/FileMeta.java com/applozic/mobicomkit/api/attachment/urlservice/GoogleCloudURLService.java com/applozic/mobicomkit/api/attachment/urlservice/S3URLService.java com/applozic/mobicomkit/api/conversation/Message.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/applozic/mobicomkit/api/conversation/MessageClientService.java com/applozic/mobicomkit/api/conversation/database/MessageDatabaseService.java com/applozic/mobicomkit/api/people/ChannelInfo.java com/applozic/mobicomkit/feed/ChannelFeed.java com/applozic/mobicomkit/feed/ChannelUsersFeed.java com/applozic/mobicomkit/feed/GroupInfoUpdate.java com/applozic/mobicomkit/feed/MessageResponse.java com/applozic/mobicomkit/sync/SyncUserBlockFeed.java com/applozic/mobicomkit/uiwidgets/conversation/richmessaging/models/KmRichMessageModel.java com/applozic/mobicomkit/uiwidgets/conversation/richmessaging/models/v2/KmAutoSuggestion.java com/applozic/mobicommons/people/channel/Channel.java com/applozic/mobicommons/people/channel/ChannelUserMapper.java com/applozic/mobicommons/people/channel/Conversation.java com/braze/configuration/BrazeConfig.java com/braze/enums/CardKey.java com/cumberland/sdk/core/permissions/model/MarketSharePermission.java com/cumberland/sdk/core/repository/sqlite/sdk/model/AccountInfoEntity.java com/cumberland/sdk/core/repository/sqlite/sdk/model/CellDataEntity.java com/cumberland/sdk/core/repository/sqlite/sdk/model/SdkConfigEntity.java com/cumberland/sdk/core/repository/sqlite/sdk/model/SdkPreferenceEntity.java com/cumberland/sdk/core/repository/sqlite/user/model/AccountInfo.java com/isharing/ChatMessage.java com/isharing/isharing/Analytics.java com/isharing/isharing/ChatStoreFS.java com/isharing/isharing/DataStore.java com/isharing/isharing/FriendManager.java com/isharing/isharing/ItemManager.java com/isharing/isharing/Notification.java com/isharing/isharing/PlaceAlert.java com/isharing/isharing/Prefs.java com/isharing/isharing/ReactActivity.java com/isharing/isharing/RemoteConfigAPI.java com/isharing/isharing/RemotePref.java com/isharing/isharing/collector/CollectorH.java com/isharing/isharing/collector/CollectorP.java com/isharing/isharing/lu/Constants.java com/isharing/isharing/lu/daos/AndroidLastDataUpdateDao.java com/isharing/isharing/lu/initialization/AndroidLastLifecycleStateDao.java com/isharing/isharing/lu/initialization/AndroidProviderUserIdDao.java com/isharing/isharing/lu/initialization/InstallationIdDao.java com/isharing/isharing/receiver/LocalPushReceiver.java com/isharing/isharing/service/DeviceMotionForegroundService.java com/isharing/isharing/service/LocationHistoryUpdateForegroundService.java com/isharing/isharing/service/LocationSendForegroundService.java com/isharing/isharing/service/LocationUpdateForegroundService.java com/isharing/isharing/service/LocationUpdateServiceBase.java com/isharing/isharing/util/ConsentCollector.java com/isharing/isharing/work/LocalPushWorker.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/reactnative/ivpusic/imagepicker/PickerModule.java com/revenuecat/purchases/amazon/AmazonBillingKt.java com/revenuecat/purchases/amazon/AmazonCacheKt.java com/revenuecat/purchases/common/BackendKt.java com/revenuecat/purchases/common/BackgroundAwareCallbackCacheKey.java com/revenuecat/purchases/common/caching/DeviceCache.java com/revenuecat/purchases/common/diagnostics/DiagnosticsEntry.java com/revenuecat/purchases/common/diagnostics/DiagnosticsHelper.java com/revenuecat/purchases/common/diagnostics/DiagnosticsTracker.java com/revenuecat/purchases/common/offlineentitlements/ProductEntitlementMapping.java com/revenuecat/purchases/common/verification/DefaultSignatureVerifier.java com/revenuecat/purchases/common/verification/Signature.java com/revenuecat/purchases/common/verification/SigningManager.java com/revenuecat/purchases/strings/ConfigureStrings.java com/revenuecat/purchases/subscriberattributes/SubscriberAttribute.java com/revenuecat/purchases/subscriberattributes/SubscriberAttributeKt.java com/umlaut/crowd/internal/na.java e4/d.java e4/p.java e4/x.java e5/g.java io/didomi/sdk/DidomiInitializeParameters.java io/didomi/sdk/apiEvents/Source.java io/didomi/sdk/tb.java io/didomi/sdk/user/sync/model/RequestSource.java io/jsonwebtoken/JwsHeader.java io/kommunicate/preference/KmPreference.java io/kommunicate/services/KmUserClientService.java qk/m2.java wo/b1.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	b5/n.java bc/p0.java com/amazonaws/retry/PredefinedRetryPolicies.java com/appsflyer/internal/AFb1gSDK.java com/braze/support/IntentUtils.java com/cumberland/weplansdk/hc.java com/cumberland/weplansdk/kx.java com/cumberland/weplansdk/rj.java com/isharing/isharing/ChatStoreFS.java com/isharing/isharing/EmojiUtil.java com/isharing/isharing/LocalPush.java com/isharing/isharing/LocationPermissionActivity.java com/isharing/isharing/Notification.java com/isharing/isharing/avoidsmartmanager/AvoidSmartManagerReceiver.java com/isharing/isharing/work/AvoidSmartManagerWorker.java com/umlaut/crowd/IS.java com/umlaut/crowd/internal/CT.java com/umlaut/crowd/internal/o2.java com/umlaut/crowd/internal/u3.java com/umlaut/crowd/internal/v.java com/umlaut/crowd/internal/vc.java com/umlaut/crowd/internal/x2.java com/umlaut/crowd/internal/xa.java kg/o.java qk/c0.java qk/e0.java qk/z1.java ql/a.java ql/b.java qq/c.java qq/d.java rk/i.java rl/a.java wk/e.java wk/g.java wq/b.java y7/n0.java yp/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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/RNFetchBlob/a.java com/applozic/mobicommons/file/LocalStorageProvider.java com/isharing/isharing/VoiceMessage.java com/isharing/isharing/ui/ChatActivity.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/rnmaps/maps/MapModule.java com/rnmaps/maps/a.java f9/l.java fr/greweb/reactnativeviewshot/RNViewShotModule.java i1/b.java mj/k.java r5/a.java y0/a.java
5	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	c6/a.java com/RNFetchBlob/d.java com/applozic/mobicomkit/api/attachment/FileClientService.java com/applozic/mobicomkit/uiwidgets/conversation/ConversationUIService.java com/applozic/mobicommons/file/FileUtils.java com/applozic/mobicommons/file/LocalStorageProvider.java com/cumberland/weplansdk/nv.java com/isharing/isharing/TinyDB.java com/isharing/isharing/util/Util.java com/naver/maps/map/internal/FileSource.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnative/ivpusic/imagepicker/a.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/rnfs/RNFSManager.java com/umlaut/crowd/internal/CDC.java mj/k.java r5/a.java u2/a.java y7/n0.java
6	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	com/cumberland/sdk/core/repository/kpi/web/WebViewWebAnalysisDataSource.java com/umlaut/crowd/internal/af.java com/umlaut/crowd/internal/wd.java
7	Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	com/umlaut/crowd/internal/af.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	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	com/amazonaws/mobileconnectors/cognito/internal/storage/SQLiteLocalStorage.java com/amazonaws/mobileconnectors/s3/transferutility/TransferTable.java com/applozic/mobicomkit/api/conversation/database/MessageDatabaseService.java com/applozic/mobicomkit/database/MobiComDatabaseHelper.java com/cumberland/sdk/core/database/sdk/changes/WeplanSdkDatabaseChange.java com/cumberland/weplansdk/wx.java com/isharing/isharing/DataStore.java com/j256/ormlite/android/AndroidCompiledStatement.java com/j256/ormlite/android/AndroidDatabaseConnection.java com/j256/ormlite/android/compat/ApiCompatibility.java com/j256/ormlite/android/compat/BasicApiCompatibility.java com/j256/ormlite/android/compat/JellyBeanApiCompatibility.java com/umlaut/crowd/database/StatsDatabase.java com/umlaut/crowd/internal/u1.java ee/f.java ee/k4.java io/kommunicate/database/KmDatabaseHelper.java jj/e.java net/sqlcipher/database/SQLiteDatabase.java o1/a.java org/pgsqlite/SQLitePlugin.java si/e.java ya/m0.java ya/t0.java
9	This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files.	info	OWASP MASVS: MSTG-CRYPTO-1	net/sqlcipher/database/SupportHelper.java
10	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	com/isharing/isharing/util/SecurityUtil.java com/umlaut/crowd/internal/c.java fi/d.java
11	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	com/umlaut/crowd/internal/CT.java com/umlaut/crowd/internal/ha.java com/umlaut/crowd/internal/ia.java com/umlaut/crowd/internal/j3.java com/umlaut/crowd/internal/v2.java com/umlaut/crowd/internal/x2.java
12	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/umlaut/crowd/internal/z3.java pp/a.java yp/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
13	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/isharing/isharing/util/SimpleCrypto.java com/revenuecat/purchases/common/UtilsKt.java f6/c.java h8/a.java qp/e.java
14	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/isharing/isharing/BuildConfig.java com/isharing/isharing/aws/HttpClient.java com/umlaut/crowd/IC.java com/umlaut/crowd/internal/CT.java com/umlaut/crowd/internal/z7.java g9/a.java hq/b.java kq/b.java lq/b.java mq/j.java
15	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/cumberland/weplansdk/aa.java com/umlaut/crowd/internal/CDC.java hf/w.java kf/h.java
16	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	c5/d.java com/RNFetchBlob/h.java com/amazonaws/services/s3/AmazonS3Client.java com/amazonaws/services/s3/internal/MD5DigestCalculatingInputStream.java com/amazonaws/util/Md5Utils.java com/braze/support/StringUtils.java com/isharing/isharing/util/Util.java e3/g.java k5/l.java
17	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/applozic/mobicomkit/uiwidgets/conversation/fragment/MobiComConversationFragment.java com/isharing/isharing/ReactBridge.java com/isharing/isharing/ui/ChatMessageAdapter.java io/didomi/sdk/eg.java
18	Ensure that user controlled URLs never reaches the Webview. Enabling file access from URLs in WebView can leak sensitive information from the file system.	warning	CWE: CWE-200: Information Exposure OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/cumberland/sdk/core/repository/kpi/web/WebViewWebAnalysisDataSource.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	x86_64/libjsc.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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', '__read_chk']	False warning Symbols are available.
2	x86_64/libreact_render_leakchecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
3	x86_64/libreact_render_telemetry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86_64/libruntimeexecutor.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
5	x86_64/libreact_render_graphics.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
6	x86_64/libglog_init.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	x86_64/libreact_config.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
8	x86_64/libreact_render_templateprocessor.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
9	x86_64/libreactperfloggerjni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	x86_64/libreact_render_attributedstring.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
11	x86_64/libjsijniprofiler.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
12	x86_64/libturbomodulejsijni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	x86_64/librrc_textinput.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
14	x86_64/libreact_render_mounting.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
15	x86_64/libfolly_runtime.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memcpy_chk', '__vsnprintf_chk', '__memset_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	x86_64/libjsi.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.
17	x86_64/librrc_unimplementedview.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
18	x86_64/libucrop.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	x86_64/librrc_text.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
20	x86_64/libreact_debug.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
21	x86_64/libreact_render_core.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	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.	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']	False warning Symbols are available.
23	x86_64/libmapbufferjni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
24	x86_64/libreact_codegen_rncore.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
25	x86_64/libreactnativeblob.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.
26	x86_64/libfbjni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
27	x86_64/librrc_legacyviewmanagerinterop.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
28	x86_64/libyoga.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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']	False warning Symbols are available.
29	x86_64/libreact_render_mapbuffer.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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']	False warning Symbols are available.
30	x86_64/libnavermap.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memcpy_chk', '__memset_chk', '__strchr_chk', '__strcat_chk', '__vsnprintf_chk', '__vsprintf_chk', '__memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
31	x86_64/libreact_nativemodule_core.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.
32	x86_64/libjscexecutor.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.
33	x86_64/libglog.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__strncat_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
34	x86_64/libreact_render_componentregistry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
35	x86_64/librrc_image.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
36	x86_64/libreact_render_debug.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
37	x86_64/librrc_view.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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']	False warning Symbols are available.
38	x86_64/libnative-filters.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
39	x86_64/libreact_render_animations.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
40	x86_64/libreact_render_runtimescheduler.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.
41	x86_64/libreact_render_imagemanager.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
42	x86_64/libsqlcipher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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', '__strlen_chk', '__vsprintf_chk', '__vsnprintf_chk', '__memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
43	x86_64/libnative-imagetranscoder.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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', '__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.
44	x86_64/libfabricjni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
45	x86_64/libreact_render_scheduler.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
46	x86_64/librrc_scrollview.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
47	x86_64/liblogger.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
48	x86_64/libjsinspector.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
49	x86_64/libimagepipeline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
50	x86_64/libreactnativejni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.
51	x86_64/libreact_utils.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
52	x86_64/librrc_root.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
53	x86_64/libreact_newarchdefaults.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
54	x86_64/libreact_render_textlayoutmanager.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
55	x86_64/libfb.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
56	x86_64/libreact_render_uimanager.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.
57	x86_64/libjsc.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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', '__read_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
58	x86_64/libreact_render_leakchecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
59	x86_64/libreact_render_telemetry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
60	x86_64/libruntimeexecutor.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
61	x86_64/libreact_render_graphics.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
62	x86_64/libglog_init.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
63	x86_64/libreact_config.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
64	x86_64/libreact_render_templateprocessor.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
65	x86_64/libreactperfloggerjni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
66	x86_64/libreact_render_attributedstring.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
67	x86_64/libjsijniprofiler.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
68	x86_64/libturbomodulejsijni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
69	x86_64/librrc_textinput.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
70	x86_64/libreact_render_mounting.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
71	x86_64/libfolly_runtime.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memcpy_chk', '__vsnprintf_chk', '__memset_chk']	False warning Symbols are available.
72	x86_64/libjsi.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
73	x86_64/librrc_unimplementedview.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
74	x86_64/libucrop.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
75	x86_64/librrc_text.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
76	x86_64/libreact_debug.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
77	x86_64/libreact_render_core.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.
78	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.	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']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
79	x86_64/libmapbufferjni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
80	x86_64/libreact_codegen_rncore.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.
81	x86_64/libreactnativeblob.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
82	x86_64/libfbjni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
83	x86_64/librrc_legacyviewmanagerinterop.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
84	x86_64/libyoga.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
85	x86_64/libreact_render_mapbuffer.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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']	False warning Symbols are available.
86	x86_64/libnavermap.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__memcpy_chk', '__memset_chk', '__strchr_chk', '__strcat_chk', '__vsnprintf_chk', '__vsprintf_chk', '__memmove_chk']	False warning Symbols are available.
87	x86_64/libreact_nativemodule_core.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
88	x86_64/libjscexecutor.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.
89	x86_64/libglog.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__strncat_chk', '__vsnprintf_chk']	False warning Symbols are available.
90	x86_64/libreact_render_componentregistry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
91	x86_64/librrc_image.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
92	x86_64/libreact_render_debug.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
93	x86_64/librrc_view.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
94	x86_64/libnative-filters.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
95	x86_64/libreact_render_animations.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
96	x86_64/libreact_render_runtimescheduler.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
97	x86_64/libreact_render_imagemanager.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
98	x86_64/libsqlcipher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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', '__strlen_chk', '__vsprintf_chk', '__vsnprintf_chk', '__memmove_chk']	False warning Symbols are available.
99	x86_64/libnative-imagetranscoder.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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', '__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
100	x86_64/libfabricjni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
101	x86_64/libreact_render_scheduler.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
102	x86_64/librrc_scrollview.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
103	x86_64/liblogger.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
104	x86_64/libjsinspector.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
105	x86_64/libimagepipeline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
106	x86_64/libreactnativejni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.
107	x86_64/libreact_utils.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
108	x86_64/librrc_root.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
109	x86_64/libreact_newarchdefaults.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
110	x86_64/libreact_render_textlayoutmanager.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
111	x86_64/libfb.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
112	x86_64/libreact_render_uimanager.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk']	False warning Symbols are available.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	16/24	android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.READ_CONTACTS, android.permission.GET_ACCOUNTS, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.RECORD_AUDIO, android.permission.READ_PHONE_STATE, android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.CAMERA, android.permission.SYSTEM_ALERT_WINDOW, android.permission.WAKE_LOCK
Other Common Permissions	11/45	android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.BROADCAST_STICKY, android.permission.BLUETOOTH, android.permission.ACTIVITY_RECOGNITION, com.google.android.gms.permission.ACTIVITY_RECOGNITION, android.permission.CHANGE_WIFI_STATE, com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE, 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
sattr.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
helpcenter.kommunicate.io	ok	**IP:** 18.66.27.113 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.c	ok	No Geolocation information available.
live.isharing.me	ok	**IP:** 3.210.224.74 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
.facebook.com	ok	No Geolocation information available.
www.language	ok	No Geolocation information available.
ssl.pstatic.net	ok	**IP:** 23.205.181.214 **Country:** Switzerland **Region:** Zurich **City:** Glattbrugg **Latitude:** 47.431301 **Longitude:** 8.562720 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sdk.iad-01.braze.com	ok	**IP:** 104.18.28.202 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
isharingsoft.com	ok	**IP:** 192.0.78.193 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.748425 **Longitude:** -122.413673 **View:** Google Map
maps.google.com	ok	**IP:** 142.250.201.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developers.didomi.io	ok	**IP:** 104.18.1.81 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.ngs.ac.uk	ok	**IP:** 130.246.140.235 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Appleton **Latitude:** 51.709511 **Longitude:** -1.361360 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api-staging.isharingapp.com	ok	**IP:** 54.160.81.32 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
api.revenuecat.com	ok	**IP:** 107.23.217.131 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
graph-video.s	ok	No Geolocation information available.
help.isharingsoft.com	ok	**IP:** 104.16.51.111 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
slaunches.s	ok	No Geolocation information available.
iamcache.braze	ok	No Geolocation information available.
api-dev.isharingapp.com	ok	**IP:** 54.158.225.236 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
itunes.apple.com	ok	**IP:** 2.18.36.24 **Country:** Argentina **Region:** Ciudad Autonoma de Buenos Aires **City:** Buenos Aires **Latitude:** -34.613152 **Longitude:** -58.377232 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
iceportal.de	ok	**IP:** 81.200.196.75 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
configs.sdk.crowd-umlaut.com	ok	**IP:** 3.165.206.49 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
cloudfront.sdk.crowd-umlaut.com	ok	**IP:** 18.66.27.114 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.manifestations	ok	No Geolocation information available.
api-diagnostics.revenuecat.com	ok	**IP:** 107.23.217.131 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
ul.api.c0nnectthed0ts.com	ok	**IP:** 34.246.150.135 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
mobile-1811.api.privacy-center.org	ok	**IP:** 3.161.119.90 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.amazon.com	ok	**IP:** 18.66.20.54 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
naveropenapi.apigw.ntruss.com	ok	**IP:** 211.249.59.32 **Country:** Korea (Republic of) **Region:** Seoul-teukbyeolsi **City:** Seoul **Latitude:** 37.568260 **Longitude:** 126.977829 **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
www.zetetic.net	ok	**IP:** 13.32.110.92 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
www.icon	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.mobitexter.net	ok	**IP:** 198.177.120.25 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
www.google.com	ok	**IP:** 142.251.39.4 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.googleorganizationautocompleterequirementsconservative	ok	No Geolocation information available.
isharing.zendesk.com	ok	**IP:** 104.16.51.111 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
graph.s	ok	No Geolocation information available.
www.world	ok	**IP:** 99.83.155.228 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.youtube.com	ok	**IP:** 142.251.39.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
scdn-stestsettings.s	ok	No Geolocation information available.
sconversions.s	ok	No Geolocation information available.
sregister.s	ok	No Geolocation information available.
portal.imice.de	ok	No Geolocation information available.
www.braze.com	ok	**IP:** 104.17.228.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
.jpg	ok	No Geolocation information available.
api.mixpanel.com	ok	**IP:** 107.178.240.159 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
sondheim.braze.com	ok	**IP:** 104.18.43.4 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
s3.amazonaws.com	ok	**IP:** 52.217.36.118 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
exoplayer.dev	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
xmlpull.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
dus.sdk.crowd-umlaut.com	ok	**IP:** 54.155.132.107 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
www.in	ok	No Geolocation information available.
s3-us-west-1.amazonaws.com	ok	**IP:** 52.219.194.32 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.wencodeuricomponent	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
support.google.com	ok	**IP:** 142.251.39.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.hortcut	ok	No Geolocation information available.
developer.android.com	ok	**IP:** 142.250.180.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
.css	ok	No Geolocation information available.
api-paywalls.revenuecat.com	ok	**IP:** 107.23.217.131 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
sinapps.s	ok	No Geolocation information available.
webapi.sdk.crowd-umlaut.com	ok	**IP:** 34.252.234.93 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
www.slf4j.org	ok	**IP:** 195.15.222.169 **Country:** Switzerland **Region:** Basel-Stadt **City:** Basel **Latitude:** 47.558399 **Longitude:** 7.573270 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
upload-sdk-crowd-umlaut.s3-accelerate.amazonaws.com	ok	**IP:** 13.32.12.59 **Country:** Germany **Region:** Bayern **City:** Munich **Latitude:** 48.137428 **Longitude:** 11.575490 **View:** Google Map
docs.revenuecat.com	ok	**IP:** 3.165.206.70 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.
developers.facebook.com	ok	**IP:** 31.13.84.8 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
www.a	ok	No Geolocation information available.
maps.googleapis.com	ok	**IP:** 142.251.39.74 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
iabeurope.eu	ok	**IP:** 162.159.135.42 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
z8fnbjgij2.execute-api.us-east-1.amazonaws.com	ok	**IP:** 3.165.206.47 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.risktabsprev10pxrise25pxblueding300ballfordearnwildbox.fairlackverspairjunetechifpickevil	ok	No Geolocation information available.
www.css	ok	No Geolocation information available.
scdn-ssettings.s	ok	No Geolocation information available.
android.googlesource.com	ok	**IP:** 64.233.184.82 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
google.com	ok	**IP:** 142.251.208.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
rev.cat	ok	**IP:** 52.72.49.79 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
iabtcf.com	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sgcdsdk.s	ok	No Geolocation information available.
www.style	ok	**IP:** 99.83.155.228 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
api.weplananalytics.com	ok	**IP:** 104.26.12.138 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
isharing-9e4fa.firebaseio.com	ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
errors.rev.cat	ok	**IP:** 67.199.248.13 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
sviap.s	ok	No Geolocation information available.
svalidate.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
awsul3.api.c0nnectthed0ts.com	ok	**IP:** 52.31.78.147 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
facebook.com	ok	**IP:** 31.13.84.36 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
sdk.privacy-center.org	ok	**IP:** 3.165.206.91 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
ssdk-services.s	ok	No Geolocation information available.
de4.backend.librespeed.org	ok	No Geolocation information available.
sars.s	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.
github.com	ok	**IP:** 140.82.121.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.years	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
api.mapbox.com	ok	**IP:** 18.66.27.6 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
echoip.weplananalytics.com	ok	**IP:** 104.26.12.138 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
dust.k8s.test-001.d-usw-2.braze.com	ok	No Geolocation information available.
www.google-analytics.com	ok	**IP:** 142.251.208.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ispl.isharing.us	ok	**IP:** 3.165.206.26 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
sapp.s	ok	No Geolocation information available.
tools.ietf.org	ok	**IP:** 104.16.44.99 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
map.kakao.com	ok	**IP:** 121.53.85.44 **Country:** Korea (Republic of) **Region:** Seoul-teukbyeolsi **City:** Seoul **Latitude:** 37.568260 **Longitude:** 126.977829 **View:** Google Map
acs.amazonaws.com	ok	No Geolocation information available.
naveropenapi.sapigw.sntruss.com	ok	**IP:** 198.54.117.242 **Country:** United States of America **Region:** Georgia **City:** Atlanta **Latitude:** 33.727291 **Longitude:** -84.425377 **View:** Google Map
www.interpretation	ok	No Geolocation information available.
access.line.me	ok	**IP:** 23.203.126.67 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.714272 **Longitude:** -74.005966 **View:** Google Map
api.kommunicate.io	ok	**IP:** 18.204.251.163 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
smonitorsdk.s	ok	No Geolocation information available.
d32kquwbmqbf7t.cloudfront.net	ok	**IP:** 18.66.17.12 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
chat.kommunicate.io	ok	**IP:** 34.234.148.15 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
play.google.com	ok	**IP:** 142.250.180.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.isharingapp.com	ok	**IP:** 34.195.119.152 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.text-decoration	ok	No Geolocation information available.
www.recent	ok	No Geolocation information available.
api.line.me	ok	**IP:** 23.203.126.67 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.714272 **Longitude:** -74.005966 **View:** Google Map
ul.sdk.crowd-umlaut.com	ok	**IP:** 54.195.28.19 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://isharing-9e4fa.firebaseio.com	info App talks to a Firebase Database.

✉ EMAILS

EMAIL	FILE
example@example.com	com/umlaut/crowd/internal/na.java
contact@isharingsoft.com	com/isharing/isharing/util/Util.java
contact@isharingsoft.com	com/isharing/isharing/ui/MenuActivity.java
u0013android@android.com u0013android@android.com0	hd/g.java
support@mobitexter.net	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Didomi	Analytics	https://reports.exodus-privacy.eu.org/trackers/342
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
Huq Sourcekit	Analytics, Location	https://reports.exodus-privacy.eu.org/trackers/408

HARDCODED SECRETS

POSSIBLE SECRETS
"delivery_report_pref_key" : "DELIVERY_REPORT_ENABLE"
"webhook_enable_key" : "WEBHOOK_ENABLE_KEY"
"deleting_channel_user" : "Deleting…"
"google_api_key" : "AIzaSyBJ1nBorrjnogDH1NeGyodypKiA5o8qpXY"
"phone_number_key" : "phone_number_key"
"analytics_sdk_api_key" : "QUI6YVN5QQ"
"com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key"
"group_sms_freq_key" : "GROUP_SMS_FREQ_KEY"
"device_key_string" : "DEVICE_KEY_STRING"
"didomi_authorize" : "Authorize"
"com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key"
"baidu_key" : "QGbUh0jFuC8bHyZQxmV3EdFs"
"didomi_user_information_token" : "Token"
"firebase_database_url" : "https://isharing-9e4fa.firebaseio.com"
"com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key"
"library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/"
"received_sms_sync_pref_key" : "RECEIVED_SMS_SYNC_FLAG"
"kakao_app_key" : "8cd991e35fb326e134ccc9755d7b82d7"
"sent_sms_sync_pref_key" : "SENT_SMS_SYNC_FLAG"
"user_key_string" : "SU_USER_KEY_STRING"

POSSIBLE SECRETS
"removing_channel_user" : "Removing..."
"google_crash_reporting_api_key" : "AIzaSyBJ1nBorrjnogDH1NeGyodypKiA5o8qpXY"
"google_map_key" : "AIzaSyBJ1nBorrjnogDH1NeGyodypKiA5o8qpXY"
"facebook_client_token" : "276d6237592d6993a73b1056411a5997"
"adding_channel_user" : "Adding..."
"password" : "Password"
5667676A654B20754F356EA92017D946567C46675556F19556A04616B567D223A5E05656FB549016A96656A557
ffffffff00000000ffffffffffffffffbce6faada7179e84f3b9cac2fc632551
115792089210356248762697446949407573530086143415290314195533631308867097853951
12511cfe811d0f4e6bc688b4d
2GY9xtlRxNZciAIhICoIbv+iSeAm7ZM43xRzSyyZ7zc=
047B6AA5D85E572983E6FB32A7CDEBC14027B6916A894D3AEE7106FE805FC34B44
3086d221a7d46bcde86c90e49284eb15
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
7BC382C63D8C150C3C72080ACE05AFA0C2BEA28E4FB22787139165EFBA91F90F8AA5814A503AD4EB04A8C7DD22CE2826
036b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
fb940fc39e5a4f29ed4011e347066c57
0123456789bcdefghjkmnpqrstuvwxyz
8cda050e0673828d391fcd5b9f5a653b
2mbuydE9pw99Ld1EHQbedo6oUJcW1o/QWNiH9X+lcIw=
A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A7

POSSIBLE SECRETS
vAwaartPSmuJV+jFjOXlfyM3UPFY8tl7jDP13kq4YYw=
4H+WN9tI0y+WKEjRpYWQhzjGaRdS7qtgrPx+7wzXofs=
a7bdadf3-5281-4d18-9990-d7e992ce7e53
FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551
e4437ed6010e88286f547fa90abfe4c42212
0432C4AE2C1F1981195F9904466A39C9948FE30BBFF2660BE1715A4589334C74C7BC3736A2F4F6779C59BDCEE36B692153D0A9877CC62A474002DF32E52139F0A0
000E0D4D696E6768756151750CC03A4473D03679
49f946663a8deb7054212b8adda248c6
03375D4CE24FDE434489DE8746E71786015009E66E38A926DD
10E723AB14D696E6768756151756FEBF8FCB49A9
04161FF7528B899B2D0C28607CA52C5B86CF5AC8395BAFEB13C02DA292DDED7A83
00C8619ED45A62E6212E1160349E2BFA844439FAFC2A3FD1638F9E
5363ad4cc05c30e0a5261c028812645a122e22ea20816678df02967c1b23bd72
04017232BA853A7E731AF129F22FF4149563A419C26BF50A4C9D6EEFAD612601DB537DECE819B7F70F555A67C427A8CD9BF18AEB9B56E0C11056FAE6A3
308201db30820144a00302010202044c707197300d06092a864886f70d01010505003031310b300906035504061302 6b6f310e300c060355040a13056b616b616f3112301006035504 0b13096b616b616f7465616d3020170d3130303832323030333834375a180f32313130303732393030333834375a3031310b300906035504061302 6b6f310e300c060355040a13056b616b616f3112301006035504 0b13096b616b616f7465616d30819f300d06092a864886f70d010101050003818d0030818902818100aef387bc86e022a87e66b8c42153284f18e0c468cf9c87a241b989729dfdad3dd9e1847546d01a2819ba77f3974a47b473c926acae173fd90c7e635000721feeef6705da7ae949a35b82900a0f67d9464d73ed8a98c37f4ac70729494a17469bc40d4ee06d043b09147ebadc55fa1020968d7036c5fb9b8c148cba1d8e9d9fc10203010001300d06092a864886f70d0101050500038181005569be704c68cff6221c1e04dd8a131110f9f5cd2138042286337fd6014a1b1d2d3eeb266ae1630afe56bf63c07dd0b5c8fad46dcb9f802f9a7802fb89eb3b4777b9665bb1ed9feaf1dc7cac4f91abedfc81187ff6d2f471dbd12335d2c0ef0e2ee719df6e763f814b9ac91f8be37fd11d40686700d66be6de22a1836f060f01
3045AE6FC8422F64ED579528D38120EAE12196D5
6A91174076B1E0E19C39C031FE8685C1CAE040E5C69A28EF
0400FAC9DFCBAC8313BB2139F1BB755FEF65BC391F8B36F8F8EB7371FD558B01006A08A41903350678E58528BEBF8A0BEFF867A7CA36716F7E01F81052
0443BD7E9AFB53D8B85289BCC48EE5BFE6F20137D10A087EB6E7871E2A10A599C710AF8D0D39E2061114FDD05545EC1CC8AB4093247F77275E0743FFED117182EAA9C77877AAAC6AC7D35245D1692E8EE1

POSSIBLE SECRETS
6C0107475609912222105691 1C77D77E77A777E7E7E77FCB
2AA058F73A0E33AB486B0F610410C53A7F132310
7167EFC92BB2E3CE7C8AAAFF34E12A9C557003D7C73A6FAF003F99F6CC8482E540F7
c39c6c3b3a36d7701b9c71a1f5804ae5d0003f4
686479766013060971498190079908139321726943530014330540939446345918554318339765539424505774633321719753296399637136332111386476861244038034037280889270700544 9
D6031998D1B3BBFEBF59CC9BBFF9AEE1
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d010104050003820101006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
0370F6E9D04D289C4E89913CE3530BFDE903977D42B146D539BF1BDE4E9C92
00BDDB97E555A50A908E43B01C798EA5DAA6788F1EA2794EFCF57166B8C14039601E55827340BE
3045AE6FC8422f64ED579528D38120EAE12196D5
00E8BEE4D3E2260744188BE0E9C723
0163F35A5137C2CE3EA6ED8667190B0BC43ECD69977702709B
NuaVE443qhtP6/N+u8tA8HilHNLFyQFq7pn4MjW5OGwcdLTSMQ1k8XjYehsxVeon
EE353FCA5428A9300D4ABA754A44C00FDFEC0C9AE4B1A1803075ED967B7BB73F
c49d360886e704936a6678e1139d26b7819f7e90
71169be7330b3038edb025f1
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186160697311231 9

POSSIBLE SECRETS
021085E2755381DCCCE3C1557AFA10C2F0C0C2825646C5B34A394CBCFA8BC16B22E7E789E927BE216F02E1FB136A5F
033C258EF3047767E7EDE0F1FDAA79DAEE3841366A132E163ACED4ED2401DF9C6BDCDE98E8E707C07A2239B1B097
Za6LxNnVxz2lEtZQYrJ2QLB5PwaCpmcdWBAdgk+Rc+b6fjcW8QKpJ7ITar8M3xU9
D35E472036BC4FB7E13C785ED201E065F98FCFA5B68F12A32D482EC7EE8658E98691555B44C59311
9162fbe73984472a0a9d0590
040369979697AB43897789566789567F787A7876A65400435EDB42EFAFB2989D51FEFCE3C80988F41FF883
74D59FF07F6B413D0EA14B344B20A2DB049B50C3
FmiCZESJMiUiPEVFp8/sySGg9zk5i1lJsy88E60+KsD4lJB1UVftaJnD830H1Cnc
E87579C11079F43DD824993C2CEE5ED3
4NlIZpWANWCeruMUGSc5tEkf3o6K0hyRt+/1nSu0QU8=
340E7BE2A280EB74E2BE61BADA745D97E8F7C300
71FE1AF926CF847989EFEF8DB459F66394D90F32AD3F15E8
bb85691939b869c1d087f601554b96b80cb4f55b35f433c2
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86297
D2C0FB15760860DEF1EEF4D696E6768756151754
00C9517D06D5240D3CFF38C74B20B6CD4D6F9DD4D9
sQRnRw5AtmLjG4zPuRRzbU9KCNWkvhkIESw7dU0UKjciZOTbDwuGbxSLRs8Rwqdx
1A827EF00DD6FC0E234CAF046C6A5D8A85395B236CC4AD2CF32A0CADBDC9DDF620B0EB9906D0957F6C6FEACD615468DF104DE296CD8F
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
0429A0B6A887A983E9730988A68727A8B2D126C44CC2CC7B2A6555193035DC76310804F12E549BDB011C103089E73510ACB275FC312A5DC6B76553F0CA

POSSIBLE SECRETS
7CBBBCF9441CFAB76E1890E46884EAE321F70C0BCB4981527897504BEC3E36A62BCDFA2304976540F6450085F2DAE145C22553B465763689180EA2571867423E
4099B5A457F9D69F79213D094C4BCD4D4262210B
03E5A88919D7CAFCBF415F07C2176573B2
kMdUJlXzMwplT8jSHASgWSZqedBabCsM4bGGMxTrHLk=
023809B2B7CC1B28CC5A87926AAD83FD28789E81E2C9E3BF10
7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9
004D696E67687561517512D8F03431FCE63B88F4
1f320637-2dba-47e5-bacc-e623dbe0282e
0108B39E77C4B108BED981ED0E890E117C511CF072
Hf8oHWnCgsj7Y9XZDlAl+qeEGkjuhCtSnXpSHq9fewc=
7A556B6DAE535B7B51ED2C4D7DAA7A0B5C55F380
00689918DBEC7E5A0DD6DFC0AA55C7
eyJ1IjoiaXNoYXJpbmciLCJhIjoiY2p6NjZqaWxvMGY4aDNob3V4dzZhd3VtbCJ9
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
YWI1NTU4MGItODQzYy00OTc5LWJkMjEtYmQyMzJlMjdmODgw
04B8266A46C55657AC734CE38F018F2192
wuFo2c62LxPcBxajXZblz51/QLk1c9RXgln2kF6l+tg=
tGUqnRBT0Z8VLsYZLT0IoD5T4HRaaLpJNvmxlM5fu89BQ2YOdHgaf4qUlK58s24H
072546B5435234A422E0789675F432C89435DE5242
FFFFFFFE0000000075A30D1B9038A115

POSSIBLE SECRETS
520883949DFDBC42D3AD198640688A6FE13F41349554B49ACC31DCCD884539816F5EB4AC8FB1F1A6
044BA30AB5E892B4E1649DD0928643ADCD46F5882E3747DEF36E956E97
b8adf1378a6eb73409fa6c9c637ba7f5
B4050A850C04B3ABF54132565044B0B7D7BFD8BA270B39432355FFB4
zzBoiLmCSl4qpONTaYkbu2H1+be7dFpyqhOnbG674OZpERvkqiVrsp9nWT5kU4lr
044AD5F7048DE709AD51236DE65E4D4B482C836DC6E410664002BB3A02D4AAADACAE24817A4CA3A1B014B5270432DB27D2
030024266E4EB5106D0A964D92C4860E2671DB9B6CC5
043B4C382CE37AA192A4019E763036F4F5DD4D7EBB938CF935318FDCED6BC28286531733C3F03C4FEE
5dATknTk87foLpzL0Dq3Gho5ELQoI7cNb0jy2DaFKNg=
fe0e87005b4e83761908c5131d552a850b3f58b749c37cf5b84d6768
6b016c3bdcf18941d0d654921475ca71a9db2fb27d1d37796185c2942c0a
26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
QnEQ5Lj6VZj+ZyIvg9+5D3/xHwfXHkc5MHdc8LLlnMs=
003088250CA6E7C7FE649CE85820F7
a23456789012345bcdef
03188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012
31a92ee2029fd10d901b113e990710f0d21ac6b6
A8sdbD2gq3QJm9nCRKcjFbiRtfVeqN3DwEtQPCnf
040D9029AD2C7E5CF4340823B2A87DC68C9E4CE3174C1E6EFDEE12C07D58AA56F772C0726F24C6B89E4ECDAC24354B9E99CAA3F6D3761402CD
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643

POSSIBLE SECRETS
00FD0D693149A118F651E6DCE6802085377E5F882D1B510B44160074C1288078365A0396C8E681
e8b4011604095303ca3b8099982be09fcb9ae616
7B425ED097B425ED097B425ED097B425ED097B425ED097B4260B5E9C7710C864
0340340340340340340340340340340340340340340340340340340323C313FAB50589703B5EC68D3587FEC60D161CC149C1AD4A91
6b8cf07d4ca75c88957d9d67059037a4
QTFg2pa0CDlg9dgYpioKGLNjWwgLSvJpA082RZAjjog=
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
470fa2b4ae81cd56ecbcda9735803434cec591fa
4D696E676875615175985BD3ADBADA21B43A97E2
0101D556572AABAC800101D556572AABAC8001022D5C91DD173F8FB561DA6899164443051D
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA70330870553E5C414CA92619418661197FAC10471DB1D381085DDADDB58796829CA90069
03eea2bae7e1497842f2de7769cfe9c989c072ad696f48034a
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B31F166E6CAC0425A7CF3AB6AF6B7FC3103B883202E9046565
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
3086d221a7d46bcde86c90e49284eb153dab
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
0228F9D04E900069C8DC47A08534FE76D2B900B7D7EF31F5709F200C4CA205
GsNdMg7ydPRZME6lhbr2mgr/qEeHLJHBW4TYBUuwzuP8n8dRXlAExueisFv9fzjL

POSSIBLE SECRETS
30820303308201eba003020102020452441f49300d06092a864886f70d01010b05003031310b3009060355040613026b6f310e300c060355040a13056b616b616f31123010060355040b13096b616b616f7465616d3020170d3137303631393039353135315a180f33303135313032313039353135315a3031310b3009060355040613026b6f310e300c060355040a13056b616b616f31123010060355040b13096b616b616f7465616d30820122300d06092a864886f70d01010105000382010f003082010a0282010100c2867a4e6fb76eaa00d5ecac63c897ebd924bb40d3f7dd90f73599a2049ae40abc4c7b1dce10dafbfdabbebf3653d7c6a18a3ade469dbe5bd0590748aae4151491001eadd8b02f7469646530595c028ed70feeacd7184fc5b0fd0ceb95addd03b7d18097a32a4afc830e209e25c65656587d891282c610429965cc44f3d63ea249d4df41453ac30ca1b3eaf4b1f8fc5cf41af4964f66f611b799f6246fcb1d6b42fff8cff202a433a90ccd25385c4d015ac770dedf8914d86c53b0eebdd4c5c5e3a509e360785fc38ee075b6d7faad19f7c876ff3949a85f601158f99c67ee14c20ff759d3057dc258146f579a5e3d90457d9996f004808f4aa625ab9a67dfc30203010001a321301f301d0603551d0e041604141487897f76c0e76161888c86336325b6e58fce5d300d06092a864886f70d01010b050003820101007bf867fa1b4ef0ea4d6de127238319c84dcae79398e60f960ab71a8bdf488b0aa07888e994bba531f4419037cd006b7d9a64860a6591b96534967444b8854bef6a6eff3161dbcbebfe5e6c979650c9d51f76676b217b8285992f4a172d4a857775c42dc3875796434b13b78d6cfb174bfaa0c59976fb7a1cd4d26527881cfd39a61cd35843dd2cd49afd7d3966947b2662fc44dbff3704094687ce70ccabeb8a9d93f39974bd11fdb1dcb9404d8a6408cae45c315ced013f088c5264ce9c8738715ecf83bc991d4e3971e4a2cc39bcd11be426d793638981455d083cfd7bfd3b88ecd11e581260ae7fbf27b8c9cdf0da49a467e375f4273d6e01d7114ac7126f
10B7B4D696E676875615175137C8A16FD0DA2211
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
0713612DCDDCB40AAB946BDA29CA91F73AF958AFD9
0402FE13C0537BBC11ACAA07D793DE4E6D5E5C94EEE80289070FB05D38FF58321F2E800536D538CCDAA3D9
00C9BB9E8927D4D64C377E2AB2856A5B16E3EFB7F61D4316AE
6b8cf07d4ca75c88957d9d670591
255705fa2a306654b1f4cb03d6a750a30c250102d4988717d9ba15ab6d3e
pKtNSmOFGZwq6j3D2KMdseTHIzIUPJ1h7RpKm9V2vyGtUkw8H5kzDwlVP1NbM1hPWsgwBewsfo3YIYOcJsuy6o
A7F561E038EB1ED560B3D147DB782013064C19F27ED27C6780AAF77FB8A547CEB5B4FEF422340353
04015D4860D088DDB3496B0C6064756260441CDE4AF1771D4DB01FFE5B34E59703DC255A868A1180515603AEAB60794E54BB7996A70061B1CFAB6BE5F32BBFA78324ED106A7636B9C5A7BD198D0158AA4F5488D08F38514F1FDF4B4F40D2181B3681C364BA0273C706
036768ae8e18bb92cfcf005c949aa2c6d94853d0e660bbf854b1c9505fe95a
04640ECE5C12788717B9C1BA06CBC2A6FEBA85842458C56DDE9DB1758D39C0313D82BA51735CDB3EA499AA77A7D6943A64F7A3F25FE26F06B51BAA2696FA9035DA5B534BD595F5AF0FA2C892376C84ACE1BB4E3019B71634C01131159CAE03CEE9D9932184BEEF216BD71DF2DADF86A627306ECFF96DBB8BACE198B61E00F8B332
0335d695-48b8-46bf-bec2-840830ca61c4
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
04BED5AF16EA3F6A4F62938C4631EB5AF7BDBCDBC31667CB477A1A8EC338F94741669C976316DA6321
00E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B

POSSIBLE SECRETS
0202F9F87B7C574D0BDECF8A22E6524775F98CDEBDCB
C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86294
07B6882CAAEFA84F9554FF8428BD88E246D2782AE2
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
3d84f26c12238d7b4f3d516613c1759033b1a5800175d0b1
662C61C430D84EA4FE66A7733D0B76B7BF93EBC4AF2F49256AE58101FEE92B04
F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C03
0409487239995A5EE76B55F9C2F098A89CE5AF8724C0A23E0E0FF77500
0481AEE4BDD82ED9645A21322E9C4C6A9385ED9F70B5D916C1B43B62EEF4D0098EFF3B1F78E2D0D48D50D1687B93B97D5F7C6D5047406A5E688B352209BCB9F8227DDE385D566332ECC0EABFA9CF7822FDF209F70024A57B1AA000C55B881F8111B2DCDE494A5F485E5BCA4BD88A2763AED1CA2B2FA8F0540678CD1E0F3AD80892
07A526C63D3E25A256A007699F5447E32AE456B50E
oSBV0gkM1yTotHLC+K1O/2QESKvM1OzdR7LLRpJm660IC9CZK+wk8pHl5h8TdV48
4B337D934104CD7BEF271BF60CED1ED20DA14C08B3BB64F18A60888D
02F40E7E2221F295DE297117B7F3D62F5C6A97FFCB8CEFF1CD6BA8CE4A9A18AD84FFABBD8EFA59332BE7AD6756A66E294AFD185A78FF12AA520E4DE739BACA0C7FFEFF7F2955727A
D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E24
6A941977BA9F6A435199ACFC51067ED587F519C5ECB541B8E44111DE1D40
038D16C2866798B600F9F08BB4A8E860F3298CE04A5798
c218d3fd-ebe2-4b7e-b136-5eae93e56cf4
04DB4FF10EC057E9AE26B07D0280B7F4341DA5D1B1EAE06C7D9B2F2F6D9C5628A7844163D015BE86344082AA88D95E2F9D
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
e6wNdaLD6UNhzFmw+sulW0Dd6tS/ZIj4VP2rchYxgmyyl8SG0R852+ZvHvO065lU
D7C134AA264366862A18302575D0FB98D116BC4B6DDEBCA3A5A7939F

POSSIBLE SECRETS
020A601907B8C953CA1481EB10512F78744A3205FD
DB7C2ABF62E35E668076BEAD208B
0405F939258DB7DD90E1934F8C70B0DFEC2EED25B8557EAC9C80E2E198F8CDBECD86B1205303676854FE24141CB98FE6D4B20D02B4516FF702350EDDB0826779C813F0DF45BE8112F4
10C0FB15760860DEF1EEF4D696E676875615175D
114ca50f7a8e2f3f657c1108d9d44cfd8
046AB1E344CE25FF3896424E7FFE14762ECB49F8928AC0C76029B4D5800374E9F5143E568CD23F3F4D7C0D4B1E41C8CC0D1C6ABD5F1A46DB4C
B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF
7830A3318B603B89E2327145AC234CC594CBDD8D3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CA
041D1C64F068CF45FFA2A63A81B7C13F6B8847A3E77EF14FE3DB7FCAFE0CBD10E8E826E03436D646AAEF87B2E247D4AF1E8ABE1D7520F9C2A45CB1EB8E95CFD55262B70B29FEEC5864E19C054FF99129280E4646217791811142820341263C5315
13D56FFAEC78681E68F9DEB43B35BEC2FB68542E27897B79
z5NXQuc0uiNSVbndYdMaUlJv3uv2TfesAU8D9T9pl4E=
64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1
cc22d6dfb95c6b25e49c0d6364a4e5980c393aa21668d953
keEhYPq98yaHF5Dzpggt8ckKDSAXe9vFpWufiQ8oXDY=
04B6B3D4C356C139EB31183D4749D423958C27D2DCAF98B70164C97A2DD98F5CFF6142E0F7C8B204911F9271F0F3ECEF8C2701C307E8E4C9E183115A1554062CFB
C49D360886E704936A6678E1139D26B7819F7E90
7d7374168ffe3471b60a857686a19475d3bfa2ff
469A28EF7C28CCA3DC721D044F4496BCCA7EF4146FBF25C9
027B680AC8B8596DA5A4AF8A19A0303FCA97FD7645309FA2A581485AF6263E313B79A2F5
931c4d9e41634a48a96995ccd36cbbd8
103FAEC74D696E676875615175777FC5B191EF30

POSSIBLE SECRETS
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC53
010090512DA9AF72B08349D98A5DD4C7B0532ECA51CE03E2D10F3B7AC579BD87E909AE40A6F131E9CFCE5BD967
1053CDE42C14D696E67687561517533BF3F83345
127971af8721782ecffa3
My0oeSI1IzInbyA+LVFaW2wiNSokPAMiMipOLS4=
89d4f45b9bbb9625bb3e718c359e4eaf
1Q5N5QhnMtop76rkewUHBq0dfu+Fpixkwg9xHoBYaMc=
51DEF1815DB5ED74FCC34C85D709
bJ19ecmml/ZL+PAjNo6P4un4UIg2zol83OavxH1sy4lr9vgJAAspRAybhuIko55U
D09E8800291CB85396CC6717393284AAA0DA64BA
6277101735386680763835789423207666416083908700390324961279
c56fb7d591ba6704df047fd98f535372fea00211
dsH99Z2rkUKkIdFxul1Y0+14Lw9GA4hWLh0RcEKja+lMBEoQnGZF5kVhq/ImGdeP
0095E9A9EC9B297BD4BF36E059184F
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
01AF286BCA1AF286BCA1AF286BCA1AF286BCA1AF286BC9FB8F6B85C556892C20A7EB964FE7719E74F490758D3B
0620048D28BCBD03B6249C99182B7C8CD19700C362C46A01
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F0
005DDA470ABE6414DE8EC133AE28E9BBD7FCEC0AE0FFF2
6127C24C05F38A0AAAF65C0EF02C
E95E4A5F737059DC60DF5991D45029409E60FC09

POSSIBLE SECRETS
0017858FEB7A98975169E171F77B4087DE098AC8A911DF7B01
0021A5C2C8EE9FEB5C4B9A753B7B476B7FD6422EF1F3DD674761FA99D6AC27C8A9A197B272822F6CD57A55AA4F50AE317B13545F
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E27
SAUyhp29xMzgJ0ZztJOiGInn+oDyrZ4+r7quECKL/6s=
B99B99B099B323E02709A4D696E6768756151751
0400C6858E06B70404E9CD9E3ECB662395B4429C648139053FB521F828AF606B4D3DBAA14B5E77EFE75928FE1DC127A2FFA8DE3348B3C1856A429BF97E7E31C2E5BD66011839296A789A3BC0045C8A5FB42C7D1BD998F54449579B446817AFBD17273E662C97EE72995EF42640C550B9013FAD0761353C7086A272C24088BE94769FD16650
85E25BFE5C86226CDB12016F7553F9D0E693A268
e43bb460f0b80cc0c0b075798e948060f8321b7d
E95E4A5F737059DC60DFC7AD95B3D8139515620C
3ecc9878eea53964da710d4f16b8c393
DB7C2ABF62E35E7628DFAC6561C5
GLyIO6R2q01pjCn0D3/H49YHLEvqvbC5vDeJpi09sqQ=
0401F481BC5F0FF84A74AD6CDF6FDEF4BF6179625372D8C0C5E10025E399F2903712CCF3EA9E3A1AD17FB0B3201B6AF7CE1B05
401028774D7777C7B7666D1366EA432071274F89FF01E718
002757A1114D696E6768756151755316C05E0BD4
8jULXqwjN4p3qVyOWkn9K2tUG5k4XuLNgEq0xlRqu/g=
UC1upXWg5QVmyOSwozp755xLqquBKjjU+di6U8QhMlM=
64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1
BRgqZ9Vg4IM5miPoGPKIX+tShrXoisnhV1cWTsEoWNSALbfoi2OgJtSBw3h9+Bqo
1E589A8595423412134FAA2DBDEC95C8D8675E58

POSSIBLE SECRETS
790408F2EEDAF392B012EDEFB3392F30F4327C0CA3F31FC383C422AA8C16
BDB6F4FE3E8B1D9E0DA8C0D46F4C318CEFE4AFE3B6B8551F
04A3E8EB3CC1CFE7B7732213B23A656149AFA142C47AAFBC2B79A191562E1305F42D996C823439C56D7F7B22E14644417E69BCB6DE39D027001DABE8F35B25C9BE
1C97BEFC54BD7A8B65ACF89F81D4D4ADC565FA45
1l/ngTeh7Ob+HSjt2mKdxpX2SEfG+yjkE9qsfrYWj1c=
040503213F78CA44883F1A3B8162F188E553CD265F23C1567A16876913B0C2AC245849283601CCDA380F1C9E318D90F95D07E5426FE87E45C0E8184698E45962364E34116177DD2259
0400D9B67D192E0367C803F39E1A7E82CA14A651350AAE617E8F01CE94335607C304AC29E7DEFBD9CA01F596F927224CDECF6C
vT7QqRHPYW89dMOJkMQAS7XgxAAvbeOb6ybNiPRYWg8=
BD71344799D5C7FCDC45B59FA3B9AB8F6A948BC5
10D9B4A3D9047D8B154359ABFB1B7F5485B04CEB868237DDC9DEDA982A679A5A919B626D4E50A8DD731B107A9962381FB5D807BF2618
2E45EF571F00786F67B0081B9495A3D95462F5DE0AA185EC
2866537B676752636A68F56554E12640276B649EF7526267
044A96B5688EF573284664698968C38BB913CBFC8223A628553168947D59DCC912042351377AC5FB32
f7Ni+qJ74MqRBDIn5zt+Qvnt6llN8c82PMULXlCAep3wzIprbOB6YjqpQItX7QwB
0238af09d98727705120c921bb5e9e26296a3cdcf2f35757a0eafd87b830e7
71169be7330b3038edb025f1d0f9
BB8E5E8FBC115E139FE6A814FE48AAA6F0ADA1AA5DF91985
04B199B13B9B34EFC1397E64BAEB05ACC265FF2378ADD6718B7C7C1961F0991B842443772152C9E0AD
rTXKPo2rBMfcFZJZq2DoWaxVmJ9PAs5JVrUzsAyZnWnDuPJ5JtQCt7v60fKWeI2BNRTB21RSavcH55tp0VXOr6
617fab6832576cbbfed50d99f0249c3fee58b94ba0038c7ae84c8c832f2c
043AE9E58C82F63C30282E1FE7BBF43FA72C446AF6F4618129097E2C5667C2223A902AB5CA449D0084B7E5B3DE7CCC01C9

POSSIBLE SECRETS
040303001D34B856296C16C0D40D3CD7750A93D1D2955FA80AA5F40FC8DB7B2ABDBDE53950F4C0D293CDD711A35B67FB1499AE60038614F1394ABFA3B4C850D927E1E7769C8EEC2D19037BF27342DA639B6DCCFFFEB73D69D78C6C27A6009CBBCA1980F8533921E8A684423E43BAB08A576291AF8F461BB2A8B3531D2F0485C19B16E2F1516E23DD3C1A4827AF1B8AC15B
37a6259cc0c1dae299a7866489dff0bd
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC50
115792089210356248762697446949407573529996955224135760342422259061068512044369
B8qnIZWGEs7xms3SbQDilR0QM+SibSnQfZbTzlo06bE=
0479BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8
00FC1217D4320A90452C760A58EDCD30C8DD069B3C34453837A34ED50CB54917E1C2112D84D164F444F8F74786046A
02197B07845E9BE2D96ADB0F5F3C7F2CFFBD7A3EB8B6FEC35C7FD67F26DDF6285A644F740A2614
EQnlrBUlHjk2AEt0zmKDh6D/4LKq1nD5m8E6B+NGkhfc83YRi+bdMQpWJDofZ7UC
040081BAF91FDF9833C40F9C181343638399078C6E7EA38C001F73C8134B1B4EF9E150
5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B
010092537397ECA4F6145799D62B0A19CE06FE26AD
B4E134D3FB59EB8BAB57274904664D5AF50388BA
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d0101040500308194310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333635365a170d3335303930313233333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010019d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
QB5q1SF7dU7PAKl1Qfw/e+quDFkRrjwkZl4xOfEvluE=

POSSIBLE SECRETS
308201e53082014ea00302010202044f4ae542300d06092a864886f70d01010505003037310b30090603550406130255533110300e060355040a1307416e64726f6964311630140603550403130d416e64726f6964204465627567301e170d3132303232373032303635385a170d3432303231393032303635385a3037310b30090603550406130255533110300e060355040a1307416e64726f6964311630140603550403130d416e64726f6964204465627567301e170d31323032323730323036353835a170d34323032313930323036353835a3037310b30090603550406130255533110300e060355040a1307416e64726f6964311630140603550403130d416e64726f696420446562756730819f300d06092a864886f70d010101050003818d0030818902818100c0b41c25ef21a39a13ce89c82dc3a14bf9ef0c3094aa2ac1bf755c9699535e79119e8b980c0ecdcc51f259eb0d8b2077d41de8fcfdeaac3f386c05e2a684ecb5504b660ad7d5a01cce35899f96bcbd099c9dcb274c6eb41fef861616a12fb45bc57a19683a8a97ab1a33d9c70128878b67dd1b3a388ad5121d1d66ff04c065ff0203010001300d06092a864886f70d0101050500038181000418a7dacb6d13eb61c8270fe1fdd006eb66d0ff9f58f475defd8dc1fb11c41e34ce924531d1fd8ad26d9479d64f54851bf57b8dfe3a5d6f0a01dcad5b8c36ac4ac48caeff37888c36483c26b09aaa9689dbb896938d5afe40135bf7d9f1264304630186 7165d28be0baa3513a5084e182f7f9c044d5baa58bdce55fa1845241
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
1854BEBDC31B21B7AEFC80AB0ECD10D5B1B3308E6DBF11C1
00E0D2EE25095206F5E2A4F9ED229F1F256E79A0E2B455970D8D0D865BD94778C576D62F0AB7519CCD2A1A906AE30D
046B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C2964FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5
zo8V8X8kshYkxeE23t3OyXdoh3FPhn0ETnxP8vKAUZieFhalf6x5LNoDw8Q1oLRS
07A11B09A76B562144418FF3FF8C2570B8
D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FC
9b8f518b086098de3d77736f9458a3d2f6f95a37
XdACBmHPjNtNHtvuxJIzO5INAuD0sY2N7kIXkPlZf2/7KHZWQ+7Wr4DDubVydJNF
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
8834235323891921647916487503603088853144765972529603627924508606099839
00FDFB49BFE6C3A89FACADAA7A1E5BBC7CC1C2E5D831478814
04B70E0CBD6BB4BF7F321390B94A03C1D356C21122343280D6115C1D21BD376388B5F723FB4C22DFE6CD4375A05A07476444D5819985007E34
5EEEFCA380D02919DC2C6558BB6D8A5D
96341f1138933bc2f503fd44
36DF0AAFD8B8D7597CA10520D04B
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
0101BAF95C9723C57B6C21DA2EFF2D5ED588BDD5717E212F9D

POSSIBLE SECRETS
0257927098FA932E7C0A96D3FD5B706EF7E5F5C156E16B7E7C86038552E91D
b3fb3400dec5c4adceb8655d4c94
60dcd2104c4cbc0be6eeefc2bdd610739ec34e317f9b33046c9e4788
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
0051953EB9618E1C9A1F929A21A0B68540EEA2DA725B99B315F3B8B489918EF109E156193951EC7E937B1652C0BD3BB1BF073573DF883D2C34F1EF451FD46B503F00
22123dc2395a05caa7423daeccc94760a7d462256bd56916
c43ca946f48a0c06a7c362d4b8db9be1
027d29778100c65a1da1783716588dce2b8b4aee8e228f1896
03Rb8b+VDPWNz2ZsdwvaSzyRMvfwK65RukwsWnYSmw87NOTFb26HoizUZBquofyN
c103703e120ae8cc73c9248622f3cd1e
28E9FA9E9D9F5E344D5A9E4BCF6509A7F39789F515AB8F92DDBCBD414D940E93
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F3
985BD3ADBAD4D696E676875615175A21B43A97E3
E95E4A5F737059DC60DFC7AD95B3D8139515620F
QUl6YVN5RF9zX2hDS1Q1WVprMVZyT0lfeTNCMjVfbzQ1RXJkbVNz
04009D73616F35F4AB1407D73562C10F00A52830277958EE84D1315ED31886
4230017757A767FAE42398569B746325D45313AF0766266479B75654E65F
00F50B028E4D696E67687561517529047278 3FB1
0091A091F03B5FBA4AB2CCF49C4EDD220FB028712D42BE752B2C40094DBACDB586FB20
04A1455B334DF099DF30FC28A169A467E9E47075A90F7E650EB6B7A45C7E089FED7FBA344282CAFBD6F7E319F7C0B0BD59E2CA4BDB556D61A5
B3EEABB8EE11C2BE770B684D95219ECB

POSSIBLE SECRETS
0403F0EBA16286A2D57EA0991168D4994637E8343E3600D51FBC6C71A0094FA2CDD545B11C5C0C797324F1
AIzaSyAMlZBc3E3TnNiQWkzMmhTOVc1Nk9saXJRQVZHNWlhM3M
026108BABB2CEEBCF787058A056CBE0CFE622D7723A289E08A07AE13EF0D10D171DD8D
0418DE98B02DB9A306F2AFCD7235F72A819B80AB12EBD653172476FECD462AABFFC4FF191B946A5F54D8D0AA2F418808CC25AB056962D30651A114AFD2755AD336747F93475B7A1FCA3B88F2B6A208CCFE469408584DC2B2912675BF5B9E582928
1fofpOOYcFfS5YFFd3ctXz8Mp5NAKFN2TSgOzUMkaRdV9dKus3ViOY+jtkwxi6r2
2472E2D0197C49363F1FE7F5B6DB075D52B6947D135D8CA445805D39BC345626089687742B6329E70680231988
4A8C7DD22CE28268B39B55416F0447C2FB77DE107DCD2A62E880EA53EEB62D57CB4390295DBC9943AB78696FA504C11
0667ACEB38AF4E488C407433FFAE4F1C811638DF20
2580F63CCFE44138870713B1A92369E33E2135D266DBB372386C400B
04AA87CA22BE8B05378EB1C71EF320AD746E1D3B628BA79B9859F741E082542A385502F25DBF55296C3A545E3872760AB73617DE4A96262C6F5D9E98BF9292DC29F8F41DBD289A147CE9DA3113B5F0B8C00A60B1CE1D7E819D7A431D7C90EA0E5F
32010857077C5431123A46B808906756F543423E8D27877578125778AC76
0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78
0236B3DAF8A23206F9C4F299D7B21A9C369137F2C84AE1AA0D
BDB6F4FE3E8B1D9E0DA8C0D40FC962195DFAE76F56564677
3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CADC083E67984050B75EBAE5DD2809BD638016F723
0066647EDE6C332C7F8C0923BB58213B333B20E9CE4281FE115F7D8F90AD
4E13CA542744D696E67687561517552F279A8C84
DNoIUzNgQ+tGaWufl617pdeOeFxPy3ypVgJRNb/REDqvDPWkZ+hwt80uPBr78PA1
D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FF
0217C05610884B63B9C6C7291678F9D341

POSSIBLE SECRETS
040060F05F658F49C1AD3AB1890F7184210EFD0987E307C84C27ACCFB8F9F67CC2C460189EB5AAAA62EE222EB1B35540CFE902374601E369050B7C4E42ACBA1DACBF04299C3460782F918EA427E6325165E9EA10E3DA5F6C42E9C55215AA9CA27A5863EC48D8E0286B
04026EB7A859923FBC82189631F8103FE4AC9CA2970012D5D46024804801841CA44370958493B205E647DA304DB4CEB08CBBD1BA39494776FB988B47174DCA88C7E2945283A01C89720349DC807F4FBF374F4AEADE3BCA95314DD58CEC9F307A54FFC61EFC006D8A2C9D4979C0AC44AEA74FBEBBB9F772AEDCB620B01A7BA7AF1B320430C8591984F601CD4C143EF1C7A3
048BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A4453BD9ACE3262547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D54C72F046997
F1FD178C0B3AD58F10126DE8CE42435B53DC67E140D2BF941FFDD459C6D655E1
7fffffffffffffffffffffff800000cfa7e8594377d414c03821bc582063
0307AF69989546103D79329FCC3D74880F33BBE803CB
3EE30B568FBAB0F883CCEBD46D3F3BB8A2A73513F5EB79DA66190EB085FFA9F492F375A97D860EB4
cc2751449a350f668590264ed76692694a80308a
0289FDFBE4ABE193DF9559ECF07AC0CE78554E2784EB8C1ED1A57A
9ba48cba5ebcb9b6bd33b92830b2a2e0e192f10a
GsEHhtmZy7+TitdN6KLdSnSR7WpVlkZahwBwH9Jv1wQ=
0100FAF51354E0E39E4892DF6E319C72C8161603FA45AA7B998A167B8F1E629521
A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377
659EF8BA043916EEDE8911702B22
03F7061798EB99E238FD6F1BF95B48FEEB4854252B
bldCWkVDnh6c0tW17EB2ImW8Helv6jy9hD1h4hlV/96dlwBa7zb3YoFOuZ30CDAy
aZvf8nokSQAvHIIdmzwu8civ2+qb07zM1ZEz6qZf1UzLfoKt8BndVgmiOXFGATXV
02120FC05D3C67A99DE161D2F4092622FECA701BE4F50F4758714E8A87BBF2A658EF8C21E7C5EFE965361F6C2999C0C247B0DBD70CE6B7
0452DCB034293A117E1F4FF11B30F7199D3144CE6DFEAFFEF2E331F296E071FA0DF9982CFEA7D43F2E
04925BE9FB01AFC6FB4D3E7D4990010F813408AB106C4F09CB7EE07868CC136FFF3357F624A21BED5263BA3A7A27483EBF6671DBEF7ABB30EBEE084E58A0B077AD42A5A0989D1EE71B1B9BC0455FB0D2C3
04188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF101207192B95FFC8DA78631011ED6B24CDD573F977A11E794811

POSSIBLE SECRETS
1b3f9bd3-2f02-4a87-9a5d-5d9a4ef3715f
2ca644917392c098bb31cf87d02925ca
7F519EADA7BDA81BD826DBA647910F8C4B9346ED8CCDC64E4B1ABD11756DCE1D2074AA263B88805CED70355A33B471EE
020ffa963cdca8816ccc33b8642bedf905c3d358573d3f27fbbd3b3cb9aaaf
040356DCD8F2F95031AD652D23951BB366A80648F06D867940A5366D9E265DE9EB240F
pOaQvLfKZf5dsThfVIh6TApaB97M4UMIA+X62gSKW+Q=
DB7C2ABF62E35E668076BEAD2088
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5374
5037EA654196CFF0CD82B2C14A2FCF2E3FF8775285B545722F03EACDB74B
68A5E62CA9CE6C1C299803A6C1530B514E182AD8B0042A59CAD29F43
A335926AA319A27A1D00896A6773A4827ACDAC73
C302F41D932A36CDA7A3462F9E9E916B5BE8F1029AC4ACC1
WUfVTOsJHOND4XgPghL23YwTgyX5VPyE24WQrLHqNZz9nfhclwI4H/j9q0Mn+psv
MVJdjUEx+rB88W0UPnVsndOuLU6aovPyFF5b36lJGoA=
F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C00
QUl6YVN5QkoxbkJvcnJqbm9nREgxTmVHeW9keXBLaUE1bzhxcFhZ
77E2B07370EB0F832A6DD5B62DFC88CD06BB84BE
7ae96a2b657c07106e64479eac3434e99cf0497512f58995c1396c28719501ee
0401A57A6A7B26CA5EF52FCDB816479700B3ADC94ED1FE674C06E695BABA1D
c469684435deb378c4b65ca9591e2a5763059a2e

POSSIBLE SECRETS
04C0A0647EAAB6A48753B033C56CB0F0900A2F5C4853375FD614B690866ABD5BB88B5F4828C1490002E6773FA2FA299B8F
1243ae1b4d71613bc9f780a03690e
24B7B137C8A14D696E6768756151756FD0DA2E5C

PLAYSTORE INFORMATION

Title: iSharing: GPS Location Tracker

Score: 4.492771 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support:** **Category:** Communication **Play Store URL:** com.isharing.isharing

Developer Details: iSharingSoft, inc., 7387112277081121704, 200 Spectrum Center Drive, Suite 300, Irvine, CA 92618, United States, https://isharingsoft.com, contact@isharingsoft.com,

Release Date: Jun 16, 2012 **Privacy Policy:** Privacy link

Description:

iSharing is the worldwide location tracking app you've been looking for! With our Family Locator & GPS Tracker, you can ensure the safety of your family members while staying connected in real-time. Whatever your needs are, we have you covered, from keeping an eye on your kid after school to keeping an eye on an elderly relative. iSharing is a family GPS location tracker designed for child's safety and parents' peace of mind. The family sharing app provides a real-time location sharing service allowing parents and kids to privately share their location information and easily communicate. Find phones, family, and devices for your safety control Ensure family safety with our phone tracker app. Stay connected and secure with real-time tracking for all kids, family. FEATURES WE OFFER: ★ Kids GPS tracker detector: When your children are exploring, you may feel secure knowing they are safe with iSharing location tracker. For extra security, get real-time location updates. ★ Real-Time Location Tracker: Stay connected with your family by using My location sharing and private map feature, which provides real-time family member position monitoring. No matter where they are, be in touch and confident of their safety. ★ Real-Time Alerts: Get instant notifications as family members arrive or depart from destinations. Say goodbye to the constant questions of 'Where are you?' texts and stay informed effortlessly with our real-time alerts on the Tracking app. ★ Family Safety Notifications: Enhance kid safety with automated family member alerts, family sharing, and a family locator free. Stay informed and proactive, ensuring peace of mind for everyone's safety. ★ Lost Phone Tracker:Use our location finder and Find My Phone function to quickly locate your stolen or lost phone. For a speedy recovery and peace of mind, follow its whereabouts in real time. ★ Alert for Panic: Activate the Panic Alert by shaking your phone in emergencies. Instantly notify trusted contacts and authorities for immediate assistance, ensuring your safety is prioritized. ★ Walkie-Talkie Feature: Unlock the power of instant communication with iSharing Finder. Transform your phone into a walkie-talkie and enjoy seamless, free voice messaging for enhanced connectivity on the go. ★ Look Up Past Locations: Easily track your family's past locations with a comprehensive 90-day history feature. Stay informed and reassured about their whereabouts, enhancing safety and peace of mind for everyone. OUR PREMIUM SERVICES: 90-Day History Unlimited Places Alert 3D Street View Low Battery Alerts Driving Alerts Driving Speed Report Remove Ads You can always get in touch with iSharing's round-the-clock support team by email at contact@isharingsoft.com if you have any technical issues with our tracking app. * iSharing app should be used with the consent of each other.

SCAN LOGS

Timestamp	Event	Error
2024-08-11 10:56:39	Generating Hashes	OK
2024-08-11 10:56:39	Extracting APK	OK

2024-08-11 10:56:39	Unzipping	OK
2024-08-11 10:56:40	Getting Hardcoded Certificates/Keystores	OK
2024-08-11 10:56:43	Parsing AndroidManifest.xml	OK
2024-08-11 10:56:43	Parsing APK with androguard	OK
2024-08-11 10:56:43	Extracting Manifest Data	OK
2024-08-11 10:56:43	Performing Static Analysis on: iSharing (com.isharing.isharing)	OK
2024-08-11 10:56:43	Fetching Details from Play Store: com.isharing.isharing	OK
2024-08-11 10:56:44	Manifest Analysis Started	OK
2024-08-11 10:56:46	Reading Network Security config from network_security_config.xml	OK
2024-08-11 10:56:46	Parsing Network Security config	OK
2024-08-11 10:56:46	Checking for Malware Permissions	OK
2024-08-11 10:56:46	Fetching icon path	OK
2024-08-11 10:56:46	Library Binary Analysis Started	OK
2024-08-11 10:56:46	Analyzing lib/x86_64/libjsc.so	OK

2024-08-11 10:56:47	Analyzing lib/x86_64/libreact_render_leakchecker.so	OK
2024-08-11 10:56:47	Analyzing lib/x86_64/libreact_render_telemetry.so	OK
2024-08-11 10:56:47	Analyzing lib/x86_64/libruntimeexecutor.so	OK
2024-08-11 10:56:47	Analyzing lib/x86_64/libreact_render_graphics.so	OK
2024-08-11 10:56:47	Analyzing lib/x86_64/libglog_init.so	OK
2024-08-11 10:56:47	Analyzing lib/x86_64/libreact_config.so	OK
2024-08-11 10:56:47	Analyzing lib/x86_64/libreact_render_templateprocessor.so	OK
2024-08-11 10:56:47	Analyzing lib/x86_64/libreactperfloggerjni.so	OK
2024-08-11 10:56:47	Analyzing lib/x86_64/libreact_render_attributedstring.so	OK
2024-08-11 10:56:47	Analyzing lib/x86_64/libjsijniprofiler.so	OK
2024-08-11 10:56:47	Analyzing lib/x86_64/libturbomodulejsijni.so	OK
2024-08-11 10:56:47	Analyzing lib/x86_64/librrc_textinput.so	OK
2024-08-11 10:56:48	Analyzing lib/x86_64/libreact_render_mounting.so	OK
2024-08-11 10:56:48	Analyzing lib/x86_64/libfolly_runtime.so	OK
2024-08-11 10:56:48	Analyzing lib/x86_64/libjsi.so	OK

2024-08-11 10:56:49	Analyzing lib/x86_64/librrc_unimplementedview.so	OK
2024-08-11 10:56:49	Analyzing lib/x86_64/libucrop.so	OK
2024-08-11 10:56:49	Analyzing lib/x86_64/librrc_text.so	OK
2024-08-11 10:56:49	Analyzing lib/x86_64/libreact_debug.so	OK
2024-08-11 10:56:49	Analyzing lib/x86_64/libreact_render_core.so	OK
2024-08-11 10:56:50	Analyzing lib/x86_64/libc++_shared.so	OK
2024-08-11 10:56:51	Analyzing lib/x86_64/libmapbufferjni.so	OK
2024-08-11 10:56:51	Analyzing lib/x86_64/libreact_codegen_rncore.so	OK
2024-08-11 10:56:52	Analyzing lib/x86_64/libreactnativeblob.so	OK
2024-08-11 10:56:52	Analyzing lib/x86_64/libfbjni.so	OK
2024-08-11 10:56:52	Analyzing lib/x86_64/librrc_legacyviewmanagerinterop.so	OK
2024-08-11 10:56:52	Analyzing lib/x86_64/libyoga.so	OK
2024-08-11 10:56:52	Analyzing lib/x86_64/libreact_render_mapbuffer.so	OK
2024-08-11 10:56:52	Analyzing lib/x86_64/libnavermap.so	OK

2024-08-11 10:57:10	Analyzing lib/x86_64/libreact_nativemodule_core.so	OK
2024-08-11 10:57:10	Analyzing lib/x86_64/libjscexecutor.so	OK
2024-08-11 10:57:11	Analyzing lib/x86_64/libglog.so	OK
2024-08-11 10:57:11	Analyzing lib/x86_64/libreact_render_componentregistry.so	OK
2024-08-11 10:57:11	Analyzing lib/x86_64/librrc_image.so	OK
2024-08-11 10:57:11	Analyzing lib/x86_64/libreact_render_debug.so	OK
2024-08-11 10:57:11	Analyzing lib/x86_64/librrc_view.so	OK
2024-08-11 10:57:12	Analyzing lib/x86_64/libnative-filters.so	OK
2024-08-11 10:57:12	Analyzing lib/x86_64/libreact_render_animations.so	OK
2024-08-11 10:57:12	Analyzing lib/x86_64/libreact_render_runtimescheduler.so	OK
2024-08-11 10:57:12	Analyzing lib/x86_64/libreact_render_imagemanager.so	OK
2024-08-11 10:57:12	Analyzing lib/x86_64/libsqlcipher.so	OK
2024-08-11 10:57:12	Analyzing lib/x86_64/libnative-imagetranscoder.so	OK
2024-08-11 10:57:12	Analyzing lib/x86_64/libfabricjni.so	OK
2024-08-11 10:57:14	Analyzing lib/x86_64/libreact_render_scheduler.so	OK

2024-08-11 10:57:14	Analyzing lib/x86_64/librrc_scrollview.so	OK
2024-08-11 10:57:14	Analyzing lib/x86_64/liblogger.so	OK
2024-08-11 10:57:14	Analyzing lib/x86_64/libjsinspector.so	OK
2024-08-11 10:57:15	Analyzing lib/x86_64/libimagepipeline.so	OK
2024-08-11 10:57:15	Analyzing lib/x86_64/libreactnativejni.so	OK
2024-08-11 10:57:16	Analyzing lib/x86_64/libreact_utils.so	OK
2024-08-11 10:57:16	Analyzing lib/x86_64/librrc_root.so	OK
2024-08-11 10:57:16	Analyzing lib/x86_64/libreact_newarchdefaults.so	OK
2024-08-11 10:57:16	Analyzing lib/x86_64/libreact_render_textlayoutmanager.so	OK
2024-08-11 10:57:16	Analyzing lib/x86_64/libfb.so	OK
2024-08-11 10:57:16	Analyzing lib/x86_64/libreact_render_uimanager.so	OK
2024-08-11 10:57:16	Analyzing apktool_out/lib/x86_64/libjsc.so	OK
2024-08-11 10:57:18	Analyzing apktool_out/lib/x86_64/libreact_render_leakchecker.so	OK
2024-08-11 10:57:18	Analyzing apktool_out/lib/x86_64/libreact_render_telemetry.so	OK

2024-08-11 10:57:18	Analyzing apktool_out/lib/x86_64/libruntimeexecutor.so	OK
2024-08-11 10:57:18	Analyzing apktool_out/lib/x86_64/libreact_render_graphics.so	OK
2024-08-11 10:57:18	Analyzing apktool_out/lib/x86_64/libglog_init.so	OK
2024-08-11 10:57:18	Analyzing apktool_out/lib/x86_64/libreact_config.so	OK
2024-08-11 10:57:18	Analyzing apktool_out/lib/x86_64/libreact_render_templateprocessor.so	OK
2024-08-11 10:57:18	Analyzing apktool_out/lib/x86_64/libreactperfloggerjni.so	OK
2024-08-11 10:57:18	Analyzing apktool_out/lib/x86_64/libreact_render_attributedstring.so	OK
2024-08-11 10:57:18	Analyzing apktool_out/lib/x86_64/libjsijniprofiler.so	OK
2024-08-11 10:57:18	Analyzing apktool_out/lib/x86_64/libturbomodulejsijni.so	OK
2024-08-11 10:57:18	Analyzing apktool_out/lib/x86_64/librrc_textinput.so	OK
2024-08-11 10:57:18	Analyzing apktool_out/lib/x86_64/libreact_render_mounting.so	OK
2024-08-11 10:57:19	Analyzing apktool_out/lib/x86_64/libfolly_runtime.so	OK
2024-08-11 10:57:19	Analyzing apktool_out/lib/x86_64/libjsi.so	OK
2024-08-11 10:57:20	Analyzing apktool_out/lib/x86_64/librrc_unimplementedview.so	OK

2024-08-11 10:57:20	Analyzing apktool_out/lib/x86_64/libucrop.so	OK
2024-08-11 10:57:20	Analyzing apktool_out/lib/x86_64/librrc_text.so	OK
2024-08-11 10:57:20	Analyzing apktool_out/lib/x86_64/libreact_debug.so	OK
2024-08-11 10:57:20	Analyzing apktool_out/lib/x86_64/libreact_render_core.so	OK
2024-08-11 10:57:21	Analyzing apktool_out/lib/x86_64/libc++_shared.so	OK
2024-08-11 10:57:22	Analyzing apktool_out/lib/x86_64/libmapbufferjni.so	OK
2024-08-11 10:57:22	Analyzing apktool_out/lib/x86_64/libreact_codegen_rncore.so	OK
2024-08-11 10:57:23	Analyzing apktool_out/lib/x86_64/libreactnativeblob.so	OK
2024-08-11 10:57:23	Analyzing apktool_out/lib/x86_64/libfbjni.so	OK
2024-08-11 10:57:23	Analyzing apktool_out/lib/x86_64/librrc_legacyviewmanagerinterop.so	OK
2024-08-11 10:57:23	Analyzing apktool_out/lib/x86_64/libyoga.so	OK
2024-08-11 10:57:23	Analyzing apktool_out/lib/x86_64/libreact_render_mapbuffer.so	OK
2024-08-11 10:57:23	Analyzing apktool_out/lib/x86_64/libnavermap.so	OK
2024-08-11 10:57:38	Analyzing apktool_out/lib/x86_64/libreact_nativemodule_core.so	OK
2024-08-11 10:57:38	Analyzing apktool_out/lib/x86_64/libjscexecutor.so	OK

2024-08-11 10:57:39	Analyzing apktool_out/lib/x86_64/libglog.so	OK
2024-08-11 10:57:39	Analyzing apktool_out/lib/x86_64/libreact_render_componentregistry.so	OK
2024-08-11 10:57:39	Analyzing apktool_out/lib/x86_64/librrc_image.so	OK
2024-08-11 10:57:39	Analyzing apktool_out/lib/x86_64/libreact_render_debug.so	OK
2024-08-11 10:57:39	Analyzing apktool_out/lib/x86_64/librrc_view.so	OK
2024-08-11 10:57:39	Analyzing apktool_out/lib/x86_64/libnative-filters.so	OK
2024-08-11 10:57:39	Analyzing apktool_out/lib/x86_64/libreact_render_animations.so	OK
2024-08-11 10:57:40	Analyzing apktool_out/lib/x86_64/libreact_render_runtimescheduler.so	OK
2024-08-11 10:57:40	Analyzing apktool_out/lib/x86_64/libreact_render_imagemanager.so	OK
2024-08-11 10:57:40	Analyzing apktool_out/lib/x86_64/libsqlcipher.so	OK
2024-08-11 10:57:40	Analyzing apktool_out/lib/x86_64/libnative-imagetranscoder.so	OK
2024-08-11 10:57:40	Analyzing apktool_out/lib/x86_64/libfabricjni.so	OK
2024-08-11 10:57:42	Analyzing apktool_out/lib/x86_64/libreact_render_scheduler.so	OK
2024-08-11 10:57:42	Analyzing apktool_out/lib/x86_64/librrc_scrollview.so	OK
2024-08-11 10:57:42	Analyzing apktool_out/lib/x86_64/liblogger.so	OK

2024-08-11 10:57:42	Analyzing apktool_out/lib/x86_64/libjsinspector.so	OK
2024-08-11 10:57:42	Analyzing apktool_out/lib/x86_64/libimagepipeline.so	OK
2024-08-11 10:57:42	Analyzing apktool_out/lib/x86_64/libreactnativejni.so	OK
2024-08-11 10:57:43	Analyzing apktool_out/lib/x86_64/libreact_utils.so	OK
2024-08-11 10:57:43	Analyzing apktool_out/lib/x86_64/librrc_root.so	OK
2024-08-11 10:57:43	Analyzing apktool_out/lib/x86_64/libreact_newarchdefaults.so	OK
2024-08-11 10:57:43	Analyzing apktool_out/lib/x86_64/libreact_render_textlayoutmanager.so	OK
2024-08-11 10:57:44	Analyzing apktool_out/lib/x86_64/libfb.so	OK
2024-08-11 10:57:44	Analyzing apktool_out/lib/x86_64/libreact_render_uimanager.so	OK
2024-08-11 10:57:44	Reading Code Signing Certificate	OK
2024-08-11 10:57:44	Failed to get signature versions	CalledProcessError(1, ['/jdk-20.0.2/bin/java', '-Xmx1024M', '-Djava.library.path=', '-jar', '/home/mobsf/Mobile-Security-Framework-MobSF/mobsf/StaticAnalyzer/tools/apksigner.jar', 'verify', '--verbose', '/home/mobsf/.MobSF/uploads/32f07a4c761f147bf65f16f6c64560c1/32f07a4c761f147bf65f16f6c64560c1.apk'])
2024-08-11 10:57:44	Running APKiD 2.1.5	OK
2024-08-11 10:57:50	Detecting Trackers	OK
2024-08-11 10:57:55	Decompiling APK to Java with jadx	OK

2024-08-11 10:58:42	Converting DEX to Smali	OK
2024-08-11 10:58:42	Code Analysis Started on - java_source	OK
2024-08-11 11:00:56	Android SAST Completed	OK
2024-08-11 11:00:56	Android API Analysis Started	OK
2024-08-11 11:02:36	Android Permission Mapping Started	OK
2024-08-11 11:09:56	Android Permission Mapping Completed	OK
2024-08-11 11:10:03	Finished Code Analysis, Email and URL Extraction	OK
2024-08-11 11:10:03	Extracting String data from APK	OK
2024-08-11 11:10:03	Extracting String data from SO	OK
2024-08-11 11:10:04	Extracting String data from Code	OK
2024-08-11 11:10:04	Extracting String values and entropies from Code	OK
2024-08-11 11:10:09	Performing Malware check on extracted domains	OK
2024-08-11 11:10:20	Saving to Database	OK

Report Generated by - MobSF v4.0.6

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.