ANDROID STATIC ANALYSIS REPORT

Blue Shield (10.11.0.115)

File Name:	com.blueshieldca.prod_142.apk

Package Name:	com.blueshieldca.prod
Scan Date:	Aug. 29, 2025, 8:22 p.m.
App Security Score:	50/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	6/432

FINDINGS SEVERITY

HIGH	⚠ MEDIUM	ℹ INFO	✓ SECURE	HOTSPOT
4	19	3	3	1

FILE INFORMATION

File Name: com.blueshieldca.prod_142.apk
Size: 165.77MB
MD5: 8b2ab997c917decd5449f045c1cdde50
SHA1: 80598ef48f9a221bea451398e861c2ac1dcf15ed
SHA256: 5238a2a60f944c2caa719f48009853694caaeda297151286eb6f935b5059c605

APP INFORMATION

App Name: Blue Shield
Package Name: com.blueshieldca.prod
Main Activity: com.bsc.bsca.cem.ui.mvp.splash.SplashActivity
Target SDK: 34
Min SDK: 27
Max SDK:
Android Version Name: 10.11.0.115
Android Version Code: 142

APP COMPONENTS

Activities: 44
Services: 20

Receivers: 15
Providers: 7
Exported Activities: 2
Exported Services: 1
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=US, ST=California, L=San Francisco, O=Blue Shield of California, OU=Blue Shield of California Mobile, CN=Lawrence Fritz
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-10-29 09:38:11+00:00
Valid To: 2041-03-16 09:38:11+00:00
Issuer: C=US, ST=California, L=San Francisco, O=Blue Shield of California, OU=Blue Shield of California Mobile, CN=Lawrence Fritz
Serial Number: 0x28331df6
Hash Algorithm: sha256
md5: 62916413aaecba336c125cbe7e891759
sha1: 0ba5407f5ab5d47762993a1907e0afa166ff974a
sha256: 1802ecd477403a5a476068fbaa3e5ff6037cbd5981549b324b3fcce1581fc838
sha512: b453b50569d5388d9c5f678c349f1f3e635a12c61cc83b395c5322990eab13f65e5cca274ee072b6b4d9905e51812e0601e306f95513c9588ea5e0eb32ca7a72
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 02c2aea1d923d18e06a41b3fc8ac2d250486f8e22518c0c38ef5727c09294f43
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
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.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
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.
com.blueshieldca.prod.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check</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.MANUFACTURER check
Build.HARDWARE check
Build.TAGS check
SIM operator check
network operator name check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>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
possible Build.SERIAL check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
<tr><td>classes5.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
network operator name check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.bsc.bsca.cem.ui.mvp.splash.SplashActivity	Schemes: bscamobileapp://,
com.google.android.gms.tagmanager.TagManagerPreviewActivity	Schemes: tagmanager.c.com.blueshieldca.prod://,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	blueshieldca.com branch.io bscal.com google-analytics.com googleapis.com dynatrace.com gbqofs.io teladoc.com teladoc.io marketingcloudapis.com	warning	Domain config is configured to trust system certificates.

CERTIFICATE ANALYSIS

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

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

MANIFEST ANALYSIS

HIGH: **0** | WARNING: **8** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.1, minSdk=27]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
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	TaskAffinity is set for activity (com.salesforce.marketingcloud.notifications.NotificationOpenActivity)	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.
4	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.
5	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.
6	Activity (com.google.android.gms.tagmanager.TagManagerPreviewActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Broadcast Receiver (com.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.

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

CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a7/a.java aa/c.java aa/d0.java aa/g.java aa/j0.java aa/o.java aa/r.java aa/v.java aa/v0.java aa/z.java ad/x1.java ai/d.java am/a.java b3/f.java bg/z.java bh/c.java bm/a.java c3/h.java c7/b.java ca/b.java ci/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/activeandroid/e.java com/activeandroid/util/a.java com/azure/android/communication/calling/l.java com/azure/android/communication/calling/s1.java com/bsc/bsca/cem/data/model/utils/DataUtils.java com/bsc/bsca/cem/ui/mvp/makeapayment/MakeAPaymentActivity.java com/bsc/bsca/cem/ui/mvp/makeapayment/a.java com/bsc/bsca/cem/ui/mvp/makeapayment/b.java com/bsc/bsca/cem/ui/mvp/makeapayment/c.java com/bsc/bsca/cem/ui/mvp/makeapayment/j.java com/bsc/bsca/cem/util/p.java com/bumptech/glide/b.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java com/clarisite/mobile/n/a.java com/opentok/android/BaseVideoCapturer.java com/opentok/android/OtLog.java com/opentok/android/PublisherKit.java com/salesforce/marketingcloud/MCLogListener.java com/salesforce/marketingcloud/g.java com/salesforce/marketingcloud/sfmcsdk/components/encryption/Encryptor.java com/salesforce/marketingcloud/sfmcsdk/components/encryption/KeyStoreWrapper.java com/salesforce/marketingcloud/sfmcsdk/components/encryption/SalesforceKeyGenerator.java com/salesforce/marketingcloud/sfmcsdk/components/logging/LogListener.java com/salesforce/marketingcloud/sfmcsdk/components/logging/Logger.java com/salesforce/marketingcloud/tozny/AesCbcWithIntegrity.java com/skype/android/video/render/legacy/LegacyGLESBindingRenderer.java com/skype/android/video/render/pipeline/RenderController.java com/spearline/watchrtc/logger/WatchRTCLoggerImpl.java com/teladoc/members/sdk/VideoRoomActivity.java com/teladoc/members/sdk/views/spinner/androiddefault/SwipeRefreshLayout.java com/teladoc/rtcclient/screensharing/ScreenSharingService.java com/teladoc/videocallui/internal/CameraPreview.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/teladoc/videocallui/internal/CameraPreview.java di/d.java di/j.java e/c.java e0/c.java e1/b.java e8/n.java em/c.java fb/b.java g4/c.java gb/b.java gs/u1.java hb/a.java hi/a.java i3/d.java ih/a.java io/branch/referral/g.java io/branch/referral/i.java iw/d.java j2/l0.java j3/c.java j3/o.java jh/d.java jh/e.java l3/f.java l4/a.java l8/a.java lh/c.java lh/e.java m9/d0.java mh/h.java mh/i.java mh/k.java mh/q.java mh/z.java mi/a.java n3/a.java n3/c.java n3/d.java n3/f.java n6/a.java n6/b.java n9/k.java net/danlew/android/joda/TimeZoneChangedReceiver.java nh/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				nh/j.java o/d.java o/e.java o/f.java o/h.java o/i.java o/k.java o/l.java oh/e.java oh/i.java oj/f.java org/joda/time/tz/DateTimeZoneBuilder.java org/slf4j/helpers/Util.java ph/a.java pp/e.java q1/f.java q4/q.java qh/c.java qh/d.java qh/g.java qh/s.java qh/t.java qh/u.java qp/z1.java s6/n.java sf/b.java sh/h.java th/c.java th/d0.java th/f.java th/f0.java th/o.java th/q.java th/r.java th/v.java u3/d.java u6/o.java u6/r.java u6/u.java u6/y.java v2/f0.java w3/t.java w6/a.java wx/a.java xh/a.java xh/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				xh/d.java xh/j.java y/k0.java y6/h.java yi/e.java z/l0.java z3/c.java z6/d.java zh/e.java zh/q.java zh/r.java zl/e.java zl/f.java
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/azure/android/communication/chat/implementation/notifications/fcm/a.java com/bsc/bsca/cem/util/AppUtil.java sc/a.java xg/b0.java zf/x0.java
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	cj/b.java com/clarisite/mobile/u/b.java com/clarisite/mobile/u/f.java un/i.java
				az/a0.java az/f.java az/h.java bz/b.java c1/d0.java com/bsc/bsca/cem/data/model/request/ChangePasswordRequest.java com/bsc/bsca/cem/data/model/request/Credentials.java com/bsc/bsca/cem/data/model/request/MemberInfo.java com/bsc/bsca/cem/data/model/request/SubmitNewPasswordRequestBody.java com/bsc/bsca/cem/data/model/request/UserInformation.java com/bsc/bsca/cem/data/model/request/dbprequests/BenefitsSummaryRequest.java com/bsc/bsca/cem/data/model/request/dbprequests/DentalClaimSearchInputs.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bsc/bsca/cem/data/model/request/dbprequests/SearchInput.java com/bsc/bsca/cem/data/model/request/documentlising/DocumentListingSecurityCredentials.java com/bsc/bsca/cem/data/model/request/documentsearch/elasticsearch/Criteria.java com/bsc/bsca/cem/data/model/request/forgotpassword/ForgotPasswordRequestBody.java com/bsc/bsca/cem/data/model/request/messagecenter/Criteria.java com/bsc/bsca/cem/data/model/request/preloginflow/forgotpassword/changepassword/ResetPasswordRequestBody.java com/bsc/bsca/cem/data/model/request/updatePreferences/UpdateProfileBody.java com/bsc/bsca/cem/data/model/request/updateemailandphone/VerificationCodeActivationRequestBody.java com/bsc/bsca/cem/data/model/request/updateemailandphone/VerificationCodeRequestBody.java com/bsc/bsca/cem/data/model/request/userverification/SendActivationRequestBody.java com/bsc/bsca/cem/data/model/request/userverification/UserVerificationRequestBody.java com/bsc/bsca/cem/data/model/response/ForgotUsernameResponseBody.java com/bsc/bsca/cem/data/model/response/LoginProfile.java com/bsc/bsca/cem/data/model/response/UserProfile.java com/bsc/bsca/cem/data/model/response/claimsupload/FileUploadBody.java com/bsc/bsca/cem/data/model/response/dbpresposes/DbpIdentifiers.java com/bsc/bsca/cem/data/model/response/dbpresposes/DentalClaimMember.java com/bsc/bsca/cem/data/model/response/dbpresposes/DentalClaimMemberInfo.java com/bsc/bsca/cem/data/model/response/dbpresposes/EligibilityMemberDetails.java com/bsc/bsca/cem/data/model/response/forgotpassword/AccountRecoveryUserNameRequest.java com/bsc/bsca/cem/data/model/response/forgotpassword/CreateNewPasswordRequest.java com/bsc/bsca/cem/data/model/response/forgotpassword/FPFlowIdResponse.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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/bsc/bsca/cem/data/model/response/globalprofileresponse/GlobalProfileResponseBody.java com/bsc/bsca/cem/data/model/response/login/FlowIdResponse.java com/bsc/bsca/cem/data/model/response/pharmacyaccumulations/PharmacyAccumulationsResponseBody.java com/opentok/android/DefaultAudioDevice.java com/pubnub/api/models/consumer/PNStatus.java com/pubnub/api/models/consumer/access_manager/PNAccessManagerGrantResult.java com/pubnub/api/models/server/SubscribeMessage.java com/pubnub/api/models/server/files/FormField.java com/salesforce/marketingcloud/events/g.java com/salesforce/marketingcloud/events/h.java com/salesforce/marketingcloud/registration/Registration.java com/teladoc/members/sdk/data/e.java cz/a.java e1/h2.java e1/k1.java ez/v.java ez/x.java fa/e.java fo/a.java fo/b.java fo/c.java fo/d.java ft/h.java fz/c.java go/b.java gy/a.java gy/c0.java gy/e.java ho/c.java jz/r.java jz/s.java k7/d.java kh/g.java ko/a.java ko/b.java ko/d.java ko/e.java ko/h.java ko/i.java ko/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ko/m.java ko/r.java ks/a.java ks/b0.java ku/a.java kz/b.java kz/d.java lz/n.java mh/d.java mh/p.java mh/x.java no/a.java ny/d.java q7/a.java qx/g1.java ro/f.java ty/m.java u2/h.java u2/s0.java un/a.java vy/i.java wn/k5.java wy/d.java wy/q.java xs/a.java ys/j.java yy/h.java
5	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/v0.java com/azure/android/communication/calling/i4.java com/pubnub/api/vendor/Crypto.java gj/a.java gj/b.java i8/b.java v4/m1.java y00/e.java
6	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/pubnub/api/vendor/FileEncryptionUtil.java com/salesforce/marketingcloud/sfmcsdk/components/encryption/Encryptor.java com/salesforce/marketingcloud/sfmcsdk/components/encryption/SalesforceKeyGenerator.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	com/clarisite/mobile/e/a.java com/clarisite/mobile/e/b.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/clarisite/mobile/e/g.java com/clarisite/mobile/e/h.java com/salesforce/marketingcloud/storage/db/a.java com/salesforce/marketingcloud/storage/db/b.java com/salesforce/marketingcloud/storage/db/c.java com/salesforce/marketingcloud/storage/db/e.java com/salesforce/marketingcloud/storage/db/f.java com/salesforce/marketingcloud/storage/db/g.java com/salesforce/marketingcloud/storage/db/h.java com/salesforce/marketingcloud/storage/db/i.java com/salesforce/marketingcloud/storage/db/j.java com/salesforce/marketingcloud/storage/db/k.java com/salesforce/marketingcloud/storage/db/l.java com/salesforce/marketingcloud/storage/db/m.java com/salesforce/marketingcloud/storage/db/upgrades/a.java com/salesforce/marketingcloud/storage/db/upgrades/b.java com/salesforce/marketingcloud/storage/db/upgrades/c.java com/salesforce/marketingcloud/storage/db/upgrades/d.java com/salesforce/marketingcloud/storage/db/upgrades/e.java com/salesforce/marketingcloud/storage/db/upgrades/f.java com/salesforce/marketingcloud/storage/db/upgrades/g.java com/salesforce/marketingcloud/storage/db/upgrades/h.java com/salesforce/marketingcloud/storage/db/upgrades/i.java com/salesforce/marketingcloud/storage/db/upgrades/j.java hj/c.java hj/e.java z6/c.java
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	aj/u.java com/clarisite/mobile/model/factory/DeviceFactory.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/sun/jna/Native.java n6/b.java qp/d1.java u6/y.java z/r.java
11	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	b10/b.java com/pubnub/api/vendor/Crypto.java com/salesforce/marketingcloud/util/l.java
12	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	ag/e.java com/pubnub/api/vendor/Crypto.java o/i.java
13	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/bsc/bsca/cem/util/e0.java qp/d1.java xb/e.java
14	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	ju/a.java
15	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/clarisite/mobile/f.java com/teladoc/members/sdk/views/x7.java qp/s3.java
16	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/salesforce/marketingcloud/sfmcsdk/components/encryption/EncryptedSharedPreferences.java

SHARED LIBRARY BINARY ANALYSIS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00016	Get location info of the device and put it to JSON object	location collection	ao/y1.java com/salesforce/marketingcloud/messages/d.java wn/b5.java wn/d1.java wn/i5.java wn/j4.java wn/w4.java
00091	Retrieve data from broadcast	collection	bh/j.java com/bsc/bsca/cem/ui/mvp/home/billingpayments/payment/EditCardPaymentActivity.java com/bsc/bsca/cem/ui/mvp/home/claims/ClaimsFilterActivity.java com/bsc/bsca/cem/ui/mvp/makeapayment/MakeAPaymentActivity.java com/bsc/bsca/cem/ui/mvp/multifactorauthentication/MFADevicesActivity.java com/bsc/bsca/cem/ui/mvp/searchfilter/selectfilters/SelectFilterActivity.java com/bsc/bsca/cem/ui/mvp/splash/SplashActivity.java com/salesforce/marketingcloud/alarms/b.java com/salesforce/marketingcloud/messages/push/a.java com/salesforce/marketingcloud/sfmcsdk/components/behaviors/BehaviorManagerImpl.java com/teladoc/members/sdk/MainActivity.java io/branch/referral/c.java rb/i.java ug/r.java wn/a3.java wn/f6.java
00202	Make a phone call	control	ao/h0.java bh/c.java cd/b0.java com/bsc/bsca/cem/util/AppUtil.java md/v.java rb/i.java sd/c.java vd/o.java xg/q0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00203	Put a phone number into an intent	control	ao/h0.java bh/c.java cd/b0.java com/bsc/bsca/cem/util/AppUtil.java md/v.java rb/i.java sd/c.java vd/o.java xg/q0.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	ao/h0.java bd/i.java bh/c.java bh/j.java cd/b0.java com/bsc/bsca/cem/common/AppController.java com/bsc/bsca/cem/util/AppUtil.java com/bsc/bsca/cem/util/h1.java com/bsc/bsca/cem/util/p.java com/bsc/bsca/cem/util/t1.java com/salesforce/marketingcloud/notifications/b.java com/teladoc/members/sdk/a.java com/teladoc/members/sdk/views/player/video/VideoActivity.java com/teladoc/members/sdk/views/rows/TableRow.java dd/s.java dg/u.java dh/b.java ec/i1.java ge/e0.java ge/m.java gg/c.java ht/c.java io/branch/referral/c.java iw/d.java jd/k0.java je/n1.java je/o2.java lb/f4.java lb/g.java md/v.java

RULE ID	BEHAVIOUR	LABEL	FILES
			ng/h.java of/p0.java pb/j0.java rb/i.java rd/r.java re/a0.java re/c.java sd/c.java su/a.java uo/b.java vd/o.java vf/d.java wc/t.java wn/a3.java wn/b.java wn/l2.java xg/q0.java yc/e.java yf/g.java zc/t.java zc/y.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	ao/h0.java bh/c.java cd/b0.java com/bsc/bsca/cem/common/AppController.java com/bsc/bsca/cem/util/AppUtil.java com/teladoc/members/sdk/views/rows/TableRow.java ge/m.java io/branch/referral/c.java je/n1.java md/v.java pb/j0.java rb/i.java re/c.java sd/c.java vd/o.java wn/b.java wn/l2.java xg/q0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	av/b.java com/clarisite/mobile/u/h.java com/salesforce/marketingcloud/media/q.java com/salesforce/marketingcloud/sfmcsdk/components/http/NetworkManager.java s4/k.java
00009	Put data in cursor to JSON object	file	com/salesforce/marketingcloud/storage/db/a.java com/salesforce/marketingcloud/storage/db/d.java com/salesforce/marketingcloud/storage/db/f.java com/salesforce/marketingcloud/storage/db/m.java com/salesforce/marketingcloud/storage/db/upgrades/a.java com/salesforce/marketingcloud/storage/db/upgrades/j.java qp/d3.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/j.java com/salesforce/marketingcloud/notifications/b.java s4/k.java
00036	Get resource file from res/raw directory	reflection	ao/h0.java com/salesforce/marketingcloud/notifications/b.java com/teladoc/members/sdk/a.java io/branch/referral/c.java iw/d.java s4/u.java uo/b.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/teladoc/members/sdk/data/y.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	a8/b.java com/bumptech/glide/load/a.java com/salesforce/marketingcloud/storage/f.java com/salesforce/marketingcloud/tozny/AesCbcWithIntegrity.java com/salesforce/marketingcloud/util/e.java com/salesforce/marketingcloud/util/f.java com/salesforce/marketingcloud/util/g.java ih/a.java okio/o.java org/joda/time/tz/ZoneInfoProvider.java qh/g.java qp/d1.java s4/c.java s4/u.java u6/y.java w6/b.java z/r.java z00/i.java z9/c.java zi/p.java
00022	Open a file from given absolute path of the file	file	com/salesforce/marketingcloud/storage/f.java com/salesforce/marketingcloud/util/e.java com/sun/jna/Native.java com/sun/jna/NativeLibrary.java n6/b.java u6/y.java wp/k.java xb/e.java z/r.java z6/d.java zi/p.java
00089	Connect to a URL and receive input stream from the server	command network	bj/a.java
00109	Connect to a URL and get the response code	network command	bj/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00183	Get current camera parameters and change the setting.	camera	com/vonage/webrtc/Camera1Session.java
00028	Read file from assets directory	file	com/clarisite/mobile/y/d.java com/opentok/android/PublisherKit.java s4/a.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	gq/l.java lh/c.java qp/d3.java
00056	Modify voice volume	control	com/vonage/webrtc/audio/WebRtcAudioTrack.java com/vonage/webrtc/voiceengine/WebRtcAudioTrack.java com/vonage/webrtc/voiceengine61/WebRtcAudioTrack.java
00003	Put the compressed bitmap data into JSON object	camera	qu/b.java
00078	Get the network operator name	collection telephony	io/branch/referral/h0.java nj/a.java
00112	Get the date of the calendar event	collection calendar	dd/s.java ed/c0.java fl/g0.java gd/v.java hl/y.java qp/d.java qp/d3.java re/n.java
00024	Write file after Base64 decoding	reflection file	com/bsc/bsca/cem/util/e0.java com/salesforce/marketingcloud/tozny/AesCbcWithIntegrity.java uo/d.java vf/h.java wf/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00125	Check if the given file path exist	file	com/bsc/bsca/cem/util/AppUtil.java me/j.java vf/h.java wf/g.java xb/c0.java
00132	Query The ISO country code	telephony collection	q4/k0.java
00161	Perform accessibility service action on accessibility node info	accessibility service	w3/t.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	w3/t.java
00192	Get messages in the SMS inbox	sms	qp/d3.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	qp/d3.java
00010	Read sensitive data(SMS, CALLLOG) and put it into JSON object	sms calllog collection	qp/d3.java
00187	Query a URI and check the result	collection sms calllog calendar	qp/d3.java
00004	Get filename and put it to JSON object	file collection	com/bsc/bsca/cem/util/AppUtil.java
00115	Get last known location of the device	collection location	com/clarisite/mobile/y/r.java
00191	Get messages in the SMS inbox	sms	nu/b.java
00102	Set the phone speaker on	command	com/opentok/android/DefaultAudioDevice.java vs/d.java
00094	Connect to a URL and read data from it	command network	com/clarisite/mobile/u/h.java s4/k.java

RULE ID	BEHAVIOUR	LABEL	FILES
00177	Check if permission is granted and request it	permission	com/clarisite/mobile/c/f.java
00209	Get pixels from the latest rendered image	collection	com/teladoc/rtcclient/screensharing/ScreenSharingService.java
00208	Capture the contents of the device screen	collection screen	com/vonage/webrtc/ScreenCapturerAndroid.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://bsca-ios.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/190422231672/namespaces/firebase:fetch?key=AIzaSyAbDfF7WJO1RvEY-Nwlesb_l2eZDSviLDA. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	13/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.READ_PHONE_STATE, android.permission.RECORD_AUDIO, android.permission.VIBRATE, android.permission.ACCESS_WIFI_STATE, android.permission.RECEIVE_BOOT_COMPLETED

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	9/44	android.permission.CALL_PHONE, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.BLUETOOTH, android.permission.READ_CALENDAR, android.permission.FOREGROUND_SERVICE, android.permission.CHANGE_NETWORK_STATE, com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, 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
member.eyemedvisioncare.com	ok	**IP:** 195.85.20.223 **Country:** Denmark **Region:** Hovedstaden **City:** Copenhagen **Latitude:** 55.675941 **Longitude:** 12.565530 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
config.teams.microsoft.com	ok	**IP:** 52.123.128.14 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
trap.skype.com	ok	**IP:** 52.112.39.28 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
prod.registrar.skype.com	ok	**IP:** 20.165.19.30 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
config.ecs.gov.teams.microsoft.us	ok	**IP:** 52.127.92.33 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
wisdomstudy.org	ok	**IP:** 3.33.251.168 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api.flightproxy.skype.com	ok	**IP:** 172.170.163.145 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.731323 **Longitude:** -73.990089 **View:** Google Map
crbug.com	ok	**IP:** 216.239.32.29 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
eu-ic3.events.data.microsoft.com	ok	**IP:** 40.79.150.120 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
federationwuat.cvshealth.com	ok	**IP:** 45.223.17.220 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
webpayments.billmatrix.com	ok	**IP:** 107.162.254.117 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.602402 **Longitude:** -122.325996 **View:** Google Map
mrktoa.blueshieldca.com	ok	**IP:** 104.17.70.206 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
docs.microsoft.com	ok	**IP:** 23.53.144.75 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
protected-api.branch.io	ok	**IP:** 18.238.96.27 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.coveredca.com	ok	**IP:** 13.107.253.71 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
broker.invalid	ok	No Geolocation information available.
edge.skype.com	ok	**IP:** 52.123.128.14 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
emea.prod.registrar.skype.com	ok	**IP:** 132.164.43.137 **Country:** United States of America **Region:** California **City:** West Covina **Latitude:** 34.066605 **Longitude:** -117.938507 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.caremark.com	ok	**IP:** 2.19.146.180 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
aka.ms	ok	**IP:** 184.27.213.254 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map
teams.microsoft.com	ok	**IP:** 52.123.128.14 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
healthysavings.com	ok	**IP:** 162.159.141.116 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
bsca-ios.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
mobile-api.teladoc.dk	ok	**IP:** 104.20.33.35 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
app.igodigital.com	ok	**IP:** 3.218.154.34 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.vsp.com	ok	**IP:** 18.238.96.35 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
yourdentalplan.com	ok	**IP:** 149.111.148.132 **Country:** United States of America **Region:** Minnesota **City:** Plymouth **Latitude:** 45.047699 **Longitude:** -93.425941 **View:** Google Map
www.ashlink.com	ok	**IP:** 20.14.115.169 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
app.wellvolution.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
collector.azure.microsoft.scloud	ok	No Geolocation information available.
pingfed-acpt.vsp.com	ok	**IP:** 198.135.203.132 **Country:** United States of America **Region:** California **City:** Dixon **Latitude:** 38.445461 **Longitude:** -121.823303 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
config.opentok.com	ok	**IP:** 18.238.109.85 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.e	ok	No Geolocation information available.
federationw.cvshealth.com	ok	**IP:** 45.223.17.220 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
config-enterprise.opentok.com	ok	**IP:** 168.100.107.43 **Country:** United States of America **Region:** New Jersey **City:** Holmdel **Latitude:** 40.383961 **Longitude:** -74.170563 **View:** Google Map
relaxng.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

DOMAIN	STATUS	GEOLOCATION
developers.google.com	ok	**IP:** 172.217.215.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gle	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
www.eyemed.com	ok	**IP:** 23.62.226.33 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
teams.events.data.microsoft.com	ok	**IP:** 20.189.173.23 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.buyblueshieldca.com	ok	**IP:** 3.33.139.32 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.myuhc.com	ok	**IP:** 18.238.109.40 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
issuetracker.google.com	ok	**IP:** 64.233.177.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
bsc-int.gosolera.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.mesvision.com	ok	**IP:** 195.85.21.187 **Country:** Denmark **Region:** Hovedstaden **City:** Copenhagen **Latitude:** 55.675941 **Longitude:** 12.565530 **View:** Google Map
api.flightproxy.teams.microsoft.com	ok	**IP:** 52.123.189.48 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
api.cc.teams.microsoftonline.cn	ok	**IP:** 159.27.164.218 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
dental.dhcs.ca.gov	ok	**IP:** 52.32.237.121 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
calling.teams.microsoft.com	ok	No Geolocation information available.
www.m	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
medi-calrx.dhcs.ca.gov	ok	**IP:** 18.155.173.2 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
odweb.clienttestmatrix.com	ok	**IP:** 107.162.254.117 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.602402 **Longitude:** -122.325996 **View:** Google Map
salesforce-marketingcloud.github.io	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.magellanassist.com	ok	**IP:** 104.18.25.113 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
provider.bcbs.com	ok	**IP:** 18.238.109.91 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.deltadentalins.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
www.ecndiscount.com	ok	No Geolocation information available.
go-eu.trouter.teams.microsoft.com	ok	**IP:** 52.112.100.58 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
ic3.events.data.microsoft.com	ok	**IP:** 20.189.173.23 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
mobile-api.sdk.integration.teladoc.io	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
ktor.io	ok	**IP:** 13.224.53.95 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
www.webrtc.org	ok	**IP:** 64.233.176.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
config.ecs.teams.microsoft.scloud	ok	No Geolocation information available.
dev-ext.blueshieldca.com	ok	**IP:** 165.253.64.87 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
pingone.com	ok	No Geolocation information available.
www.tensorflow.org	ok	**IP:** 64.233.176.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
gen3.opinionlab.com	ok	**IP:** 104.17.49.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
healthysavingsstaging.solutran.com	ok	**IP:** 172.64.150.7 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
default.url	ok	No Geolocation information available.
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
mobile-api2.teladoc.com	ok	**IP:** 104.17.80.218 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.yourdentalplan.com	ok	**IP:** 18.155.173.40 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.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
developer.android.com	ok	**IP:** 64.233.176.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
mczj66htpbh0d9555v1rmrppp5l0.device.marketingcloudapis.com	ok	**IP:** 13.111.67.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.788464 **Longitude:** -122.394608 **View:** Google Map
www.example.com	ok	**IP:** 23.220.73.43 **Country:** Colombia **Region:** Antioquia **City:** Medellin **Latitude:** 6.251840 **Longitude:** -75.563591 **View:** Google Map
www.jointcommission.org	ok	**IP:** 104.18.18.198 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api3-eu.branch.io	ok	**IP:** 18.155.173.33 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
config.ecs.teams.eaglex.ic.gov	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.engagementpoint.com	ok	**IP:** 35.82.138.5 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
member.teladoc.com	ok	**IP:** 104.17.31.172 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
npe-ext.blueshieldca.com	ok	**IP:** 23.62.226.167 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
bcbsglobalcore.com	ok	**IP:** 144.202.168.218 **Country:** United States of America **Region:** Missouri **City:** Saint Louis **Latitude:** 38.615940 **Longitude:** -90.445137 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
bscatest.healthsparq.com	ok	**IP:** 45.60.233.26 **Country:** United States of America **Region:** California **City:** Redwood City **Latitude:** 37.532440 **Longitude:** -122.248833 **View:** Google Map
www.abms.org	ok	**IP:** 141.193.213.21 **Country:** United States of America **Region:** Texas **City:** Austin **Latitude:** 30.271158 **Longitude:** -97.741699 **View:** Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.
api3.cc.skype.com	ok	**IP:** 52.123.185.125 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
www.hospitalsafetygrade.org	ok	**IP:** 44.195.57.119 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
registrar.gov.teams.microsoft.us	ok	**IP:** 52.127.94.253 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
cdn.branch.io	ok	**IP:** 18.238.109.80 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
qe.registrar.skype.net	ok	**IP:** 52.112.116.39 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map
teams.live.com	ok	**IP:** 52.113.194.132 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
schemas.microsoft.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
recommend.teams-t.trafficmanager.net	ok	No Geolocation information available.
eu-teams.events.data.microsoft.com	ok	**IP:** 40.79.150.120 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map
registrar.dod.teams.microsoft.us	ok	**IP:** 195.134.241.24 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.amazon.com	ok	**IP:** 23.222.206.109 **Country:** United States of America **Region:** Minnesota **City:** Minneapolis **Latitude:** 44.979969 **Longitude:** -93.263840 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
trap.gov.teams.microsoft.us	ok	**IP:** 52.127.92.191 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
www.medicare.gov	ok	**IP:** 23.32.109.213 **Country:** Sweden **Region:** Stockholms lan **City:** Stockholm **Latitude:** 59.332581 **Longitude:** 18.064899 **View:** Google Map
survey.vovici.com	ok	**IP:** 44.235.26.254 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
web.healthsparq.com	ok	**IP:** 45.60.233.26 **Country:** United States of America **Region:** California **City:** Redwood City **Latitude:** 37.532440 **Longitude:** -122.248833 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
aomediacodec.github.io	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
api.cc.gov.teams.microsoft.us	ok	**IP:** 52.127.94.245 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
maps.googleapis.com	ok	**IP:** 142.250.105.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
apiadvancemedical.quickblox.com	ok	**IP:** 18.195.42.240 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
collector.azure.eaglex.ic.gov	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
b.config.skype.com	ok	**IP:** 150.171.22.17 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
java.sun.com	ok	**IP:** 23.62.226.28 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
api.opentok.com	ok	**IP:** 168.100.106.197 **Country:** United States of America **Region:** New Jersey **City:** Holmdel **Latitude:** 40.383961 **Longitude:** -74.170563 **View:** Google Map
aimdp.microsoft.com	ok	**IP:** 20.42.128.105 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
global.mtgw.prod.communication.microsoft.com	ok	**IP:** 70.152.144.29 **Country:** United States of America **Region:** Georgia **City:** Atlanta **Latitude:** 33.818501 **Longitude:** -84.361015 **View:** Google Map
api.cc.dod.teams.microsoft.us	ok	**IP:** 195.134.240.24 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.673988 **Longitude:** -122.121513 **View:** Google Map
www.tokbox.com	ok	**IP:** 168.100.113.249 **Country:** United States of America **Region:** New Jersey **City:** Holmdel **Latitude:** 40.383961 **Longitude:** -74.170563 **View:** Google Map
play.google.com	ok	**IP:** 142.250.68.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.cc.teams.microsoft.scloud	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
memberashuat.eyemedvisioncare.com	ok	**IP:** 195.85.20.206 **Country:** Denmark **Region:** Hovedstaden **City:** Copenhagen **Latitude:** 55.675941 **Longitude:** 12.565530 **View:** Google Map
pf.events.data.microsoft.com	ok	**IP:** 52.245.136.46 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map
ping-ext.blueshieldca.com	ok	**IP:** 165.253.64.48 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
config.ecs.dod.teams.microsoft.us	ok	**IP:** 195.134.241.49 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.blueshieldca.com	ok	**IP:** 23.62.226.171 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
pingfed.vsp.com	ok	**IP:** 198.135.203.133 **Country:** United States of America **Region:** California **City:** Dixon **Latitude:** 38.445461 **Longitude:** -121.823303 **View:** Google Map
www.slf4j.org	ok	**IP:** 31.97.181.89 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Bowness-on-Windermere **Latitude:** 54.363312 **Longitude:** -2.918590 **View:** Google Map
www.thaiopensource.com	ok	**IP:** 119.81.18.13 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
blueshieldca.com	ok	**IP:** 23.62.226.163 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
recommend.teams.microsoft.com	ok	No Geolocation information available.
www1.deltadentalins.com	ok	**IP:** 54.151.51.45 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
api.cc.teams.eaglex.ic.gov	ok	No Geolocation information available.
bf59345rdj.bf.dynatrace.com	ok	**IP:** 54.191.83.121 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
gov.teams.microsoft.us	ok	**IP:** 104.212.46.177 **Country:** United States of America **Region:** Wyoming **City:** Cheyenne **Latitude:** 41.139980 **Longitude:** -104.820251 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
bsca.healthsparq.com	ok	**IP:** 45.60.233.26 **Country:** United States of America **Region:** California **City:** Redwood City **Latitude:** 37.532440 **Longitude:** -122.248833 **View:** Google Map
skype.com	ok	**IP:** 20.70.246.20 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
stage.app.igodigital.com	ok	**IP:** 3.212.165.186 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.calhospitalcompare.org	ok	**IP:** 205.186.136.193 **Country:** United States of America **Region:** California **City:** Culver City **Latitude:** 34.017185 **Longitude:** -118.392830 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
tb.events.data.microsoft.com	ok	**IP:** 20.140.95.0 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map
api.cc.skype.com	ok	**IP:** 52.112.86.80 **Country:** United States of America **Region:** Virginia **City:** Washington **Latitude:** 38.713451 **Longitude:** -78.159439 **View:** Google Map
dod.teams.microsoft.us	ok	**IP:** 195.134.241.49 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
pages.blueshieldca.com	ok	**IP:** 52.184.251.130 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api2.branch.io	ok	**IP:** 18.238.109.16 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
a.config.skype.com	ok	**IP:** 150.171.22.17 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

EMAILS

EMAIL	FILE
stopfraud@blueshieldca.com	jd/k0.java
pcpchangerequests@aegisglobal.com	f9/d.java
med-bill@blueshieldca.com premium@blueshieldca.com coverage-.ebusiness@blueshieldca.com	ad/w1.java
rxmbrportalemails@blueshieldca.com	of/t.java
mail@mail.com	com/teladoc/videocallui/internal/invite/InvitePanelView.java

EMAIL	FILE
irectoryinaccuracies@blueshieldca.com nformationenrollment@blueshieldca.com example@name.com providerdirectory@mesvision.com iderdataerror-dental@blueshieldca.com provdirectory@yourdentalplan.com iderdataerror-vision@blueshieldca.com blueshieldcoveredca@mesvision.com privacy@blueshieldca.com	Android String Resource
appro@openssl.org	lib/arm64-v8a/libopentok.so
appro@openssl.org	apktool_out/lib/arm64-v8a/libopentok.so

TRACKERS

TRACKER	CATEGORIES	URL
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105
Matomo (Piwik)	Analytics	https://reports.exodus-privacy.eu.org/trackers/138
Salesforce Marketing Cloud		https://reports.exodus-privacy.eu.org/trackers/220

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://bsca-ios.firebaseio.com"
"dummy_user_name" : "John"
"mapd_deniedclaimsmorethanzero_key" : "MAPD_DeniedClaimsMsg"
"mapd_contactus_key" : "MAPD_Contactus"
"mapd_apply_claim_key" : "MAPD_applealaclaim"
"prior_auth_filter" : "Filter"
"claim_appeal_key" : "ClaimAppeal"
"claim_appeals_and_grievances_key" : "ClaimAppealsAndGrievances"
"sfmcAccessToken" : "UujH44arHPg5vTCC24QaXCMp"
"google_api_key" : "AIzaSyAbDfF7WJO1RvEY-Nwlesb_l2eZDSviLDA"
"prior_auth_requests" : "Requests"
"username" : "Username"
"TeladocAPIKey" : "5e4a856e3232fb4c93cec2c9e8ca5dbb58f9cf60"
"mapd_deniedclaims_key" : "mapd_deniedclaim_message"
"prior_auth_patients_name" : "Patient"
"google_crash_reporting_api_key" : "AIzaSyAbDfF7WJO1RvEY-Nwlesb_l2eZDSviLDA"
"prior_auth_patients_status" : "Status"

POSSIBLE SECRETS
"googlemapskey" : "AIzaSyCcmA1PB9l5t_DP2RPqhjNMz5mZo1nEwg8"
"mapd_rememberthisisnotabill_key" : "MAPD_rememberthisisnotabill"
"prior_auth_providers_name" : "Providers"
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
23456789abcdefghjkmnpqrstvwxyz
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
362aa53c4499935d0f4d198115f16d2a055af9af
F6389234-1024-481F-9173-37D9D7F5051F
849f26e2-2df6-11e4-ab12-14109fdc48df
sha256/Ko8tivDrEjiY90yGasP6ZpBU4jwXvHqVvQI0GS3GNdA=
sha256/FEzVOUp4dF3gI0ZVPRJhFbSJVXR+uQmMH65xhs1glH4=
afe001f1-329e-4e58-8a36-4cc92d8a8b01
BB83E0E7-5F05-4C5F-9A85-150A318BE149
29200FA5-DF79-4C3F-BC0F-E2FF3CE6199A
0eTxqRIzSqAxN2gXP54SKfoOyrGKo33b2wEYv
sha256/++MBgDH5WGvL9Bcn5Be30cRcL0f5O+NyoXuWtQdX1aI=

POSSIBLE SECRETS
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
sha256/JSMzqOOrtyOT1kmau6zKhgT676hGgczD5VMdRMyJZFA=
eyJqdGkiOiJNb2JpbGVfQmx1ZXNoaWVsZENBX1BST0QiLCJpYXQiOjE0OTk4NzQ0NTksInN1YiI6IkJsdWUgU2hpbGVkIG9mIENhbGlmb3JuaWFfUFJPRCIsImlzcyI6IkJsdWVzaGllbGRDQV9QUk9EIiwiZXhwIjoxNDk5ODgwNDU5fQ
MTU1NTQ0NTEyMDEyNX4zbnU3YkMxTTlCL3lLQWMrWTQ1U3hYRmR
eyJqdGkiOiJTZXJ2aWNlRGVza3RvcF9CbHVlc2hpZWxkQ0EiLCJpYXQiOjE0OTQyODY0NTMsInN1YiI6IkJsdWUgU2hpbGVkIG9mIENhbGlmb3JuaWEiLCJpc3MiOiJCbHVlc2hpZWxkQ0EiLCJleHAiOjE0OTQ1MDU0NTN9
d6bc7755-9011-4ef5-aa54-23dcad87867d
a593feb1-bff4-b273-2e02-ae94f9152980
xLnZXkt7eWMhMSUyt0KQZmgNsrL8RMrUUENZCk
p1tbKUVtreyvrnyrm2Ow7A92jbrue3WvaEaQL4KqUynaf7GYnbpqHhFvE8uqGbu7Kq182MduzwBStjscM
AIzaSyBwhl8D9mPnZiUBZEbTVOUG0avSQ7Kj
e2236651-3ab8-e2fa-b921-5837222f31c7
gBc8xboQq8SGRCIjogiBTxAPUTWqKkKCUaiH5EaJSUA0F2aKFd6yq8aGSTS5sKo53ULpU6gP35wBrjAshys3JpXq9k2lVK1kUArVXrTGxRpgvUSbGyym0DaEyuaon2QTz7jTT3YfhmMcCT3wBeFWKnw
T1==cGFydG5lcl9pZD00NTc2OTMxMiZzaWc9NDlkMWI3YTZiYjNhYmE3YWJiMTU3MTQzZTU0YmMyNmU1OGQ0ZGU0MTpyb2xlPXB1Ymxpc2hlciZjb25uZWN0aW9uX2RhdGE9JTdCJTIydXNlclR5cGUlMjIlM0ElMjJ0ZG9jX21lbWJlciUyMiUyQyUyMnVzZXJJZCUyMiUzQSUyMjI5MSUyMiUyQyUyMnJvbGUlMjIlM0ElMjJwdWJsaXNoZXIlMjIlN0Qmc2Vzc2lvbl9pZD0xX01YNDBOVGMyT1RNeE1uNS1NVFUxTlRRME5URXlNREV5Tlg0emJuVTNZa014VFRsQ0wzbExRV01yV1RRMVUzaFlSbVItZmcmY3JlYXRlX3RpbWU9MTU1NTYxNTM3MiZub25jZT0wLjE5NTI4ODgzMTE0NTUyMTImZXhwaXJlX3RpbWU9MjA1NTYxNTM3Mg==
3071c8717539de5d5353f4c8cd59a032
7d73d21f1bd82c9e5268b6dcf9fde2cb

POSSIBLE SECRETS
vwf8UH3h6cfphEJ0cXINl3BLY2CnZzcn7JwQGB3h2VrJDb7Xxjbeots
e60fc4cf-8ed7-4f3d-a7c0-9d4d5e93143d

PLAYSTORE INFORMATION

Title: Blue Shield of California

Score: 3.427451 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.blueshieldca.prod

Developer Details: Blue Shield of California, Blue+Shield+of+California, None, https://www.blueshieldca.com, mobile@blueshieldca.com,

Release Date: Oct 30, 2013 **Privacy Policy:** Privacy link

Description:

Manage your health care from anywhere with the Blue Shield of California app. View your ID card, search for doctors, track your claim information, understand your benefits and more. The Blue Shield of California app provides BSC and BSC Promise members enhanced 24/7 service and ease-of-access to the information that matters most. As a member of Blue Shield of California, or Blue Shield Promise, with our app you can view and access: Digital ID card - Your digital ID card enables you to always have access to your current ID and easily share it with your care team in person or by email. Depending on your plan Medical, Dental and Vision ID cards are easily accessible and can be downloaded to your Google Wallet and saved. Find care – Search for doctors and facilities, by doctor specialty, by location, and/or by name when and where you need it. Locate labs, Urgent Care, Emergency Rooms, hospitals, and other healthcare professionals in your plan's network. See your estimated costs before you receive care. Review your health care team, including your doctors' credentials, locations and contact information. This includes Virtual care for medical and mental health Prescriptions - Fill or refill most prescriptions, check costs, mail order options and see a list of all your medications Plan details – View Benefits related to you including understanding and track your share of the costs, deductible and copay information. Find out what's covered. Find programs that are related to your health journey. Many of these features easily available from your personalized dashboard View and submit claims – Easily track your claims including the status and your costs from outset to finalization. Submit out-of-network and Covid test kit claims. See your health insurance plan information, including important documents like your plan summary and Evidence of Coverage (EOC) View your medical history, including visits, medications, immunizations, health reminders, and more all in one place. Download it for easy access for doctor visits or share with care givers. Learn about our benefit discount programs, like dental, vision and pharmacy Pay your monthly premiums Quickly access your member information without having to type in your username password. Biometric is now available so you can login with fingerprint & facial recognition. This app is intended for use by Blue Shield of California or Blue Shield Promise members who are residents of California. ©Blue Shield of California is an independent member of the Blue Shield Association.

SCAN LOGS

Timestamp	Event	Error

2025-08-29 20:22:37	Generating Hashes	OK
2025-08-29 20:22:38	Extracting APK	OK
2025-08-29 20:22:38	Unzipping	OK
2025-08-29 20:22:39	Parsing APK with androguard	OK
2025-08-29 20:22:41	Extracting APK features using aapt/aapt2	OK
2025-08-29 20:22:41	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 20:22:46	Parsing AndroidManifest.xml	OK
2025-08-29 20:22:46	Extracting Manifest Data	OK
2025-08-29 20:22:46	Manifest Analysis Started	OK
2025-08-29 20:22:46	Reading Network Security config from network_security_config.xml	OK
2025-08-29 20:22:46	Parsing Network Security config	OK
2025-08-29 20:22:46	Performing Static Analysis on: Blue Shield (com.blueshieldca.prod)	OK

2025-08-29 20:22:46	Fetching Details from Play Store: com.blueshieldca.prod	OK
2025-08-29 20:22:47	Checking for Malware Permissions	OK
2025-08-29 20:22:47	Fetching icon path	OK
2025-08-29 20:22:47	Library Binary Analysis Started	OK
2025-08-29 20:22:47	Analyzing lib/arm64-v8a/libACSCallingShared.so	OK
2025-08-29 20:22:47	Analyzing lib/arm64-v8a/libRtmMediaManagerDyn.so	OK
2025-08-29 20:22:47	Analyzing lib/arm64-v8a/libskypert.so	OK
2025-08-29 20:22:47	Analyzing lib/arm64-v8a/libc++_shared.so	OK
2025-08-29 20:22:47	Analyzing lib/arm64-v8a/libimage_processing_util_jni.so	OK
2025-08-29 20:22:47	Analyzing lib/arm64-v8a/librt-java-bindings.so	OK
2025-08-29 20:22:47	Analyzing lib/arm64-v8a/libolm.so	OK
2025-08-29 20:22:47	Analyzing lib/arm64-v8a/libjnidispatch.so	OK

2025-08-29 20:22:47	Analyzing lib/arm64-v8a/libopentok.so	OK
2025-08-29 20:22:47	Analyzing lib/armeabi-v7a/libACSCallingShared.so	OK
2025-08-29 20:22:48	Analyzing lib/armeabi-v7a/libRtmMediaManagerDyn.so	OK
2025-08-29 20:22:48	Analyzing lib/armeabi-v7a/libskypert.so	OK
2025-08-29 20:22:48	Analyzing lib/armeabi-v7a/libc++_shared.so	OK
2025-08-29 20:22:48	Analyzing lib/armeabi-v7a/libimage_processing_util_jni.so	OK
2025-08-29 20:22:48	Analyzing lib/armeabi-v7a/librt-java-bindings.so	OK
2025-08-29 20:22:48	Analyzing lib/armeabi-v7a/libolm.so	OK
2025-08-29 20:22:48	Analyzing lib/armeabi-v7a/libjnidispatch.so	OK
2025-08-29 20:22:48	Analyzing lib/armeabi-v7a/libopentok.so	OK
2025-08-29 20:22:48	Analyzing lib/armeabi/libjnidispatch.so	OK
2025-08-29 20:22:48	Analyzing apktool_out/lib/arm64-v8a/libACSCallingShared.so	OK

2025-08-29 20:22:48	Analyzing apktool_out/lib/arm64-v8a/libRtmMediaManagerDyn.so	OK
2025-08-29 20:22:48	Analyzing apktool_out/lib/arm64-v8a/libskypert.so	OK
2025-08-29 20:22:49	Analyzing apktool_out/lib/arm64-v8a/libc++_shared.so	OK
2025-08-29 20:22:49	Analyzing apktool_out/lib/arm64-v8a/libimage_processing_util_jni.so	OK
2025-08-29 20:22:49	Analyzing apktool_out/lib/arm64-v8a/librt-java-bindings.so	OK
2025-08-29 20:22:49	Analyzing apktool_out/lib/arm64-v8a/libolm.so	OK
2025-08-29 20:22:49	Analyzing apktool_out/lib/arm64-v8a/libjnidispatch.so	OK
2025-08-29 20:22:49	Analyzing apktool_out/lib/arm64-v8a/libopentok.so	OK
2025-08-29 20:22:49	Analyzing apktool_out/lib/armeabi-v7a/libACSCallingShared.so	OK
2025-08-29 20:22:49	Analyzing apktool_out/lib/armeabi-v7a/libRtmMediaManagerDyn.so	OK
2025-08-29 20:22:49	Analyzing apktool_out/lib/armeabi-v7a/libskypert.so	OK
2025-08-29 20:22:49	Analyzing apktool_out/lib/armeabi-v7a/libc++_shared.so	OK

2025-08-29 20:22:49	Analyzing apktool_out/lib/armeabi-v7a/libimage_processing_util_jni.so	OK
2025-08-29 20:22:49	Analyzing apktool_out/lib/armeabi-v7a/librt-java-bindings.so	OK
2025-08-29 20:22:49	Analyzing apktool_out/lib/armeabi-v7a/libolm.so	OK
2025-08-29 20:22:49	Analyzing apktool_out/lib/armeabi-v7a/libjnidispatch.so	OK
2025-08-29 20:22:49	Analyzing apktool_out/lib/armeabi-v7a/libopentok.so	OK
2025-08-29 20:22:50	Analyzing apktool_out/lib/armeabi/libjnidispatch.so	OK
2025-08-29 20:22:50	Reading Code Signing Certificate	OK
2025-08-29 20:22:50	Running APKiD 2.1.5	OK
2025-08-29 20:23:01	Detecting Trackers	OK
2025-08-29 20:23:06	Decompiling APK to Java with JADX	OK
2025-08-29 20:23:32	Converting DEX to Smali	OK
2025-08-29 20:23:32	Code Analysis Started on - java_source	OK

2025-08-29 20:23:40	Android SBOM Analysis Completed	OK
2025-08-29 20:23:51	Android SAST Completed	OK
2025-08-29 20:23:51	Android API Analysis Started	OK
2025-08-29 20:24:03	Android API Analysis Completed	OK
2025-08-29 20:24:03	Android Permission Mapping Started	OK
2025-08-29 20:24:22	Android Permission Mapping Completed	OK
2025-08-29 20:24:23	Android Behaviour Analysis Started	OK
2025-08-29 20:24:38	Android Behaviour Analysis Completed	OK
2025-08-29 20:24:38	Extracting Emails and URLs from Source Code	OK
2025-08-29 20:24:46	Email and URL Extraction Completed	OK
2025-08-29 20:24:46	Extracting String data from APK	OK
2025-08-29 20:24:47	Extracting String data from SO	OK

2025-08-29 20:24:49	Extracting String data from Code	OK
2025-08-29 20:24:49	Extracting String values and entropies from Code	OK
2025-08-29 20:24:56	Performing Malware check on extracted domains	OK
2025-08-29 20:25:19	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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