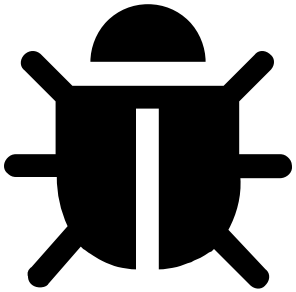
MOBSF

ANDROID STATIC ANALYSIS REPORT



Hims (4.47.0)

File Name:	com.himshers.hims_3843.apk
Package Name:	com.himshers.hims
Scan Date:	Aug. 30, 2025, 9:18 p.m.
App Security Score:	53/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	27	4	3	2

FILE INFORMATION

File Name: com.himshers.hims_3843.apk
Size: 33.85MB
MD5: 99ca86724b3e259796ac36b979cc6c58
SHA1: 8b9328f20c77791e4e896a7ed95a42217cd76740
SHA256: 33f898df6f44512dc4e6c5d7a9eec4e3dcf7024e93ed106dc89edba6d953d62c

APP INFORMATION

App Name: Hims
Package Name: com.himshers.hims
Main Activity: com.himshers.MainActivity
Target SDK: 34
Min SDK: 31
Max SDK:
Android Version Name: 4.47.0

Android Version Code: 3843

APP COMPONENTS

Activities: 50
Services: 14
Receivers: 17
Providers: 9
Exported Activities: 8
Exported Services: 1
Exported Receivers: 5
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-06-17 17:38:44+00:00
Valid To: 2052-06-17 17:38:44+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x712ed47d737056673294c3b223cdc3897c9d1201
Hash Algorithm: sha256
md5: fa1b2b5d3878d4e05d5b80465836845b
sha1: cfc8845db6783657c62341011c025c11781ae86c
sha256: d4753fc431857cd8db296e4f6b37ff9b1e811be683b8841f41da8bb80de254fb
sha512: a4dd430686ee38b936cdfa9737c37951d662420540b2418735482a9827e99964bdb8f4296da55b6e5e344bb10ecb67167a8e9336fcab18b716587494e7061bd0
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 71e12f85d256f03ca42677c83fd81ac107a7590777038a6ccd0f4267ec5f7aa7
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.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.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.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
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.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.
android.permission.DETECT_SCREEN_CAPTURE	normal	notifies when a screen capture of the app's windows is attempted.	Allows an application to get notified when a screen capture of its windows is attempted.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.himshers.hims.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.REORDER_TASKS	normal	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.BROADCAST_CLOSE_SYSTEM_DIALOGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.

PERMISSION	STATUS	INFO	DESCRIPTION
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>99ca86724b3e259796ac36b979cc6c58.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
network operator name check
device ID check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes2.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MANUFACTURER check possible Build.SERIAL check Build.TAGS check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

FILE	DETAILS
classes3.dex	

FINDINGS	DETAILS
yara_issue	yara issue - dex file recognized by apkid but not yara module
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check network operator name check possible ro.secure check possible VM check
Anti Debug Code	Debug.isDebuggerConnected() check
Compiler	unknown (please file detection issue!)

<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>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
network operator name check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.himshers.MainActivity	Schemes: @string/deep_link_scheme://, https://, Hosts: *, @string/BRANCH_LINK_DOMAIN, @string/BRANCH_LINK_ALTERNATE_DOMAIN, @string/BRANCH_LINK_OLD_DOMAIN,
com.auth0.android.provider.RedirectActivity	Schemes: com.himshers.hims.auth0://, Hosts: prod-forhims.us.auth0.com, Path Prefixes: /android/com.himshers.hims/callback,

ACTIVITY	INTENT
com.stripe.android.financialconnections.FinancialConnectionsSheetRedirectActivity	Schemes: stripe-auth://, stripe://, Hosts: link-accounts, link-native-accounts, native-redirect, auth-redirect, Paths: /com.himshers.hims/success, /com.himshers.hims/cancel, Path Prefixes: /com.himshers.hims/authentication_return, /com.himshers.hims,
com.stripe.android.link.LinkRedirectHandlerActivity	Schemes: link-popup://, Hosts: complete, Paths: /com.himshers.hims,
com.stripe.android.payments.StripeBrowserProxyReturnActivity	Schemes: stripesdk://, Hosts: payment_return_url, Paths: /com.himshers.hims,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	10.0.2.2 localhost	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

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: 15 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	Broadcast Receiver (androidx.media.session.MediaButtonReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
3	Activity (com.auth0.android.provider.RedirectActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity (com.stripe.android.financialconnections.FinancialConnectionsSheetRedirectActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Activity (com.stripe.android.link.LinkRedirectHandlerActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

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

NO	ISSUE	SEVERITY	DESCRIPTION
9	TaskAffinity is set for activity (com.braze.push.NotificationTrampolineActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
10	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
11	Activity (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
12	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) 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.
13	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
14	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.
15	Activity (app.notifee.core.NotificationReceiverActivity) 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.
16	Broadcast Receiver (app.notifee.core.AlarmPermissionBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 10 | INFO: 4 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a4/h.java a6/c.java a8/a.java a8/d.java a8/j.java ah/k.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				app/notifee/core/AlarmPermissionBroadcastReceiver.java app/notifee/core/Logger.java app/notifee/core/RebootBroadcastReceiver.java b4/d.java c1/c.java c1/g.java c4/a.java c8/e.java c8/f.java c8/o.java c8/p.java c8/r.java c8/s.java com/amplitude/api/AmplitudeLog.java com/auth0/android/provider/a.java com/auth0/android/provider/c.java com/auth0/android/provider/e.java com/auth0/android/provider/h.java com/auth0/android/provider/l.java com/auth0/android/provider/m.java com/auth0/android/provider/q.java com/auth0/android/request/internal/k.java com/braze/support/BrazeLogger.java com/brentvatne/react/b.java com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/c.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java com/datadog/android/rum/DdRumContentProvider.java com/himshers/RCTHimsTranscendModule.java com/ibits/react_native_in_app_review/AppReviewModule.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/d.java com/lugg/ReactNativeConfig/ReactNativeConfigModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/margelo/quickcrypto/QuickCryptoModule.java com/microsoft/codepush/react/k.java com/oblador/keychain/KeychainModule.java com/reactcommunity/rndatetimepicker/d.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/reactnativecommunity/webview/e.java com/reactnativecommunity/webview/i.java com/reactnativecommunity/webview/k.java com/reactnativemmkv/MmkvModule.java com/reactnativestripesdk/StripeSdkModule.java com/reactnativestripesdk/addresssheet/c.java com/reactnativestripesdk/f0.java com/reactnativestripesdk/k.java com/reactnativestripesdk/pushprovisioning/f.java com/reactnativestripesdk/pushprovisioning/h.java com/reactnativestripesdk/y.java com/stripe/android/IssuingCardPinService.java com/stripe/android/core/Logger.java com/stripe/android/core/storage/SharedPreferencesStorage.java com/stripe/android/core/utils/PluginDetector.java com/stripe/android/stripe3ds2/transaction/Logger.java com/stripe/android/ui/core/elements/LpmSerializer.java com/stripe/android/uicore/image/ImageLruDiskCache.java com/stripe/android/uicore/image/UiUtilsKt.java com/swmansion/gesturehandler/react/RNGestureHandlerModule.java com/swmansion/gesturehandler/react/i.java com/swmansion/gesturehandler/react/j.java com/swmansion/reanimated/NativeMethodsHelper.java com/swmansion/reanimated/ReanimatedModule.java com/swmansion/reanimated/ReanimatedUIManag

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	erFactory.java com/swmansion/reanimated/layoutReanimation/AnimationsManager.java com/swmansion/reanimated/layoutReanimation/ReanimatedNativeHierarchyManager.java com/swmansion/reanimated/layoutReanimation/SharedTransitionManager.java com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java com/swmansion/reanimated/sensor/ReanimatedSensorContainer.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/tencent/mmkv/MMKV.java com/th3rdwave/safeareacontext/k.java com/twilio/video/Logger.java com/twiliorn/library/TwilioRemotePreviewManager.java com/twiliorn/library/b.java com/twiliorn/library/h.java d8/d.java dc/d.java dc/g.java dc/h.java dc/j.java dc/l.java dc/m.java dc/y.java dm/b.java eh/a.java em/c.java f8/h.java g2/f0.java g8/d.java g8/k.java ge/d.java gl/a.java gl/b.java gl/c.java hk/d.java i8/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/branch/rnbranch/RNBranchModule.java io/invertase/notifee/l0.java io/transcend/webview/IABTranscendSharedPreferences.java io/transcend/webview/Storage/CacheManager.java io/transcend/webview/Storage/TelemetryManager.java io/transcend/webview/TranscendAPI.java io/transcend/webview/TranscendWebView.java io/transcend/webview/WebAppInterface.java jg/a.java k3/c.java k7/a.java k8/a.java kk/h.java kn/a.java ko/b.java ko/g.java ko/h.java ko/i.java l/g.java l4/i.java l6/a.java l7/d.java l7/e.java ln/a.java lo/c.java lo/f.java m/c.java m3/a.java m6/b.java m7/a.java mg/a.java mp/c.java na/m.java nj/t.java o5/j.java o6/b.java o7/c.java o7/e.java p6/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				p6/j.java p7/h.java p7/i.java p7/k.java p7/q.java p7/z.java pl/d.java q0/b.java q2/d.java q3/a.java q7/i.java q7/j.java qk/i.java r/a.java r/b.java r7/e.java r7/i.java rl/g.java rl/n.java rp/h.java rp/j.java rt/j.java s3/a.java s3/l.java s7/a.java sk/l.java sk/m.java t2/f.java t7/c.java t7/d.java t7/f.java t7/r.java t7/s.java tj/d.java tvi/webrtc/DefaultVideoEncoderFactory.java u1/l0.java u4/m0.java uo/a.java v7/a.java vo/i.java w7/b0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				w7/c.java w7/d.java w7/k.java w7/m.java w7/n.java w7/r.java w7/z.java we/a.java we/g.java wt/g.java xd/f.java y3/a.java yo/a.java
2	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/reactnativecommunity/webview/k.java dm/c.java uc/a.java
				bo/app/f5.java com/amplitude/api/AmplitudeClient.java com/braze/configuration/BrazeConfig.java com/himshers/BuildConfig.java com/stripe/android/EphemeralKey.java com/stripe/android/PaymentConfiguration.java com/stripe/android/auth/PaymentBrowserAuthContract.java com/stripe/android/core/injection/InjectorKt.java com/stripe/android/core/injection/NamedConstantsKt.java com/stripe/android/core/networking/AnalyticsFields.java com/stripe/android/core/networking/ApiRequest.java com/stripe/android/core/networking/NetworkConstantsKt.java com/stripe/android/financialconnections/FinancialConnectionsSheet.java com/stripe/android/financialconnections/analytics

NO	ISSUE	SEVERITY	STANDARDS	FILES
				/DefaultFinancialConnectionsEventReporter.java com/stripe/android/financialconnections/di/NamedConstantsKt.java com/stripe/android/financialconnections/features/linkaccountpicker/LinkAccountPickerState.java com/stripe/android/financialconnections/features/linkstepupverification/LinkStepUpVerificationState.java com/stripe/android/financialconnections/features/networkinglinkverification/NetworkingLinkVerificationState.java com/stripe/android/financialconnections/features/networkingsavetolinkverification/NetworkingSaveToLinkVerificationState.java com/stripe/android/financialconnections/model/FinancialConnectionsSession.java com/stripe/android/financialconnections/model/GetFinancialConnectionsAcccountsParams.java com/stripe/android/financialconnections/network/NetworkConstants.java com/stripe/android/googlepaylauncher/GooglePayLauncherContract.java com/stripe/android/googlepaylauncher/GooglePayLauncherViewModel.java com/stripe/android/googlepaylauncher/GooglePayPaymentMethodLauncherContract.java com/stripe/android/googlepaylauncher/GooglePayPaymentMethodLauncherViewModel.java com/stripe/android/link/serialization/PopupPayload.java com/stripe/android/model/ConfirmPaymentIntentParams.java com/stripe/android/model/ConfirmSetupIntentParams.java com/stripe/android/model/ConfirmStripeIntentParams.java com/stripe/android/model/ConsumerSession.java com/stripe/android/model/CreateFinancialConnectionsSessionParams.java com/stripe/android/model/ElementsSessionParam

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	s.java com/stripe/android/model/FinancialConnectionsSession.java com/stripe/android/model/PaymentIntent.java com/stripe/android/model/PaymentMethodCreateParams.java com/stripe/android/model/SetupIntent.java com/stripe/android/model/Source.java com/stripe/android/model/SourceParams.java com/stripe/android/model/Stripe3ds2AuthParams.java com/stripe/android/model/Stripe3ds2Fingerprint.java com/stripe/android/model/StripeIntent.java com/stripe/android/model/parsers/ConsumerSessionJsonParser.java com/stripe/android/model/parsers/EphemeralKeyJsonParser.java com/stripe/android/model/parsers/FinancialConnectionsSessionJsonParser.java com/stripe/android/model/parsers/NextActionDataParser.java com/stripe/android/model/parsers/PaymentIntentJsonParser.java com/stripe/android/model/parsers/SetupIntentJsonParser.java com/stripe/android/model/parsers/SourceJsonParser.java com/stripe/android/payments/PaymentFlowResult.java com/stripe/android/payments/bankaccount/CollectBankAccountLauncher.java com/stripe/android/payments/bankaccount/navigation/CollectBankAccountContract.java com/stripe/android/payments/bankaccount/ui/CollectBankAccountViewEffect.java com/stripe/android/payments/core/authentication/threeds2/Stripe3ds2TransactionContract.java com/stripe/android/payments/paymentlauncher/PaymentLauncherContract.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/stripe/android/paymentsheet/IntentConfirmationInterceptor.java com/stripe/android/paymentsheet/PaymentSheet.java com/stripe/android/paymentsheet/PaymentSheetContract.java com/stripe/android/paymentsheet/addresselement/AddressDetails.java com/stripe/android/paymentsheet/addresselement/AddressElementActivityContract.java com/stripe/android/paymentsheet/addresselement/AddressLauncher.java com/stripe/android/paymentsheet/flowcontroller/DefaultFlowController.java com/stripe/android/paymentsheet/flowcontroller/FlowControllerViewModel.java com/stripe/android/paymentsheet/paymentdatacollection/ach/USBankAccountFormViewModel.java com/stripe/android/paymentsheet/paymentdatacollection/polling/PollingContract.java com/stripe/android/paymentsheet/paymentdatacollection/polling/PollingViewModel.java com/stripe/android/polling/IntentStatusPoller.java com/stripe/android/stripe3ds2/observability/DefaultSentryConfig.java com/stripe/android/stripe3ds2/transaction/AcsData.java com/stripe/android/stripe3ds2/transaction/AuthenticationRequestParameters.java com/stripe/android/stripe3ds2/transaction/DefaultAcsDataParser.java com/stripe/android/stripe3ds2/transaction/IntentData.java com/stripe/android/uicore/elements/AddressType.java com/stripe/android/view/PaymentAuthWebViewClient.java f2/h.java f2/r0.java io/invertase/notifee/NotifeeEventSubscriber.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/transcend/webview/TranscendConstants.java j6/u.java j5/i.java j5/j.java me/g.java n5/j.java n7/g.java na/e.java na/k.java p7/d.java p7/p.java p7/x.java q0/i1.java q0/j2.java q4/d.java
4	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/learnium/RNDeviceInfo/RNDeviceModule.java sb/a.java com/reactnativecommunity/webview/k.java ed/a.java m6/a.java uc/a.java
5	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	b4/c.java com/amplitude/api/DatabaseHelper.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java ih/m0.java ih/t0.java mj/f.java mj/k.java ph/c.java ph/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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	bb/a.java br/a.java br/b.java com/braze/support/IntentUtils.java cr/a.java mj/r.java nh/p1.java qi/o0.java ti/b.java yb/c.java yb/h.java
7	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	bo/app/a0.java bo/app/c1.java bo/app/e.java bo/app/f6.java bo/app/h5.java bo/app/j0.java bo/app/j1.java bo/app/k0.java bo/app/l0.java bo/app/m.java bo/app/m4.java bo/app/n6.java bo/app/p1.java bo/app/q4.java bo/app/q6.java bo/app/t0.java bo/app/t3.java bo/app/w6.java bo/app/y0.java com/braze/configuration/RuntimeAppConfigurationProvider.java com/braze/managers/BrazeGeofenceManager.java nn/a.java p6/k.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	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	dm/b.java hd/c.java
9	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	fs/a.java gs/a.java hs/a.java is/a.java lc/a.java ws/e.java xn/a.java
10	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/braze/support/StringUtils.java x5/g.java
11	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/amplitude/api/PinnedAmplitudeClient.java
12	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	ng/b.java qk/w.java xo/b.java
13	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/reactnativecommunity/clipboard/ClipboardModule.java rp/l0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
14	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	vi/a.java
15	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	com/reactnativecommunity/clipboard/ClipboardModule.java
16	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	lg/a.java xo/a.java
17	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	io/transcend/webview/TranscendWebView.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	app/notifee/core/Notifee.java as/n.java com/auth0/android/provider/d.java com/auth0/android/provider/q.java com/braze/Braze.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/inappmessage/views/InAppMessageHtmlBaseView.java com/braze/ui/support/UriUtils.java com/stripe/android/financialconnections/FinancialConnectionsSheetActivity.java com/stripe/android/financialconnections/FinancialConnectionsSheetRedirectActivity.java com/stripe/android/financialconnections/FinancialConnectionsSheetViewModel.java com/stripe/android/financialconnections/browser/BrowserManager.java com/stripe/android/financialconnections/ui/FinancialConnectionsSheetNativeActivity.java com/stripe/android/link/LinkActivityResultKt.java com/stripe/android/link/LinkForegroundActivity.java com/stripe/android/payments/StripeBrowserLauncherViewModel.java com/stripe/android/uicore/text/HtmlKt.java com/stripe/android/view/PaymentAuthWebViewActivityViewModel.java com/stripe/android/view/PaymentAuthWebViewClient.java io/branch/rnbranch/RNBranchModule.java io/transcend/webview/TranscendWebView.java rp/d.java s3/a.java s3/l.java vp/a.java
00014	Read file into a stream and put it into a JSON object	file	dm/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	bo/app/m0.java com/airbnb/android/react/lottie/h.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java com/bumptech/glide/load/a.java com/microsoft/codepush/react/j.java com/microsoft/codepush/react/n.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/stripe/android/core/networking/FileUploadRequest.java dm/c.java ds/d2.java h9/e.java k7/a.java kn/a.java lj/g.java lj/l0.java nj/b.java okio/r.java pg/i.java sc/b.java t7/f.java x5/g.java x5/h.java y3/b.java
00028	Read file from assets directory	file	lj/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	b4/d.java bo/app/f6.java com/braze/Braze.java com/braze/images/DefaultBrazeImageLoader.java com/braze/support/BrazeFileUtils.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java com/microsoft/codepush/react/a.java com/microsoft/codepush/react/j.java com/microsoft/codepush/react/k.java com/microsoft/codepush/react/n.java e9/f.java ed/a.java fa/c.java n5/m.java o5/v.java og/d.java uc/f.java x5/g.java x5/h.java yc/c.java
00009	Put data in cursor to JSON object	file	com/amplitude/api/DatabaseHelper.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	app/notifee/core/Notifee.java as/o.java com/auth0/android/provider/q.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/support/UriUtils.java com/dylanvann/fastimage/f.java eg/a.java g5/c.java lj/l0.java qc/a.java rp/d.java s3/a.java
00183	Get current camera parameters and change the setting.	camera	com/twilio/video/CameraCapturer.java tvi/webrtc/Camera1Session.java
00078	Get the network operator name	collection telephony	bo/app/k0.java com/amplitude/api/DeviceInfo.java com/learnium/RNDeviceInfo/RNDeviceModule.java rp/n0.java
00137	Get last known location of the device	location collection	com/amplitude/api/DeviceInfo.java
00115	Get last known location of the device	collection location	com/amplitude/api/DeviceInfo.java
00132	Query The ISO country code	telephony collection	com/amplitude/api/DeviceInfo.java nj/p0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	bo/app/v0.java com/amplitude/api/ConfigManager.java com/bumptech/glide/load/data/j.java com/microsoft/codepush/react/h.java com/stripe/android/stripe3ds2/transaction/StripeHttpClient.java em/c.java lj/u.java
00030	Connect to the remote server through the given URL	network	bo/app/v0.java com/bumptech/glide/load/data/j.java com/stripe/android/stripe3ds2/transaction/StripeHttpClient.java lj/u.java x5/b.java
00109	Connect to a URL and get the response code	network command	bo/app/v0.java com/amplitude/api/ConfigManager.java com/bumptech/glide/load/data/j.java com/stripe/android/stripe3ds2/transaction/StripeHttpClient.java em/c.java lj/u.java
00189	Get the content of a SMS message	sms	hd/f.java
00188	Get the address of a SMS message	sms	hd/f.java
00200	Query data from the contact list	collection contact	hd/f.java
00201	Query data from the call log	collection calllog	hd/f.java
00012	Read data and put it into a buffer stream	file	com/microsoft/codepush/react/n.java h9/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	app/notifee/core/Notifee.java as/n.java com/stripe/android/financialconnections/FinancialConnectionsSheetRedirectActivity.java com/stripe/android/financialconnections/browser/BrowserManager.java com/stripe/android/link/LinkForegroundActivity.java com/stripe/android/payments/StripeBrowserLauncherViewModel.java com/stripe/android/uicore/text/HtmlKt.java io/branch/rnbranch/RNBranchModule.java rp/d.java s3/a.java
00208	Capture the contents of the device screen	collection screen	tvi/webrtc/ScreenCapturerAndroid.java
00096	Connect to a URL and set request method	command network	com/stripe/android/core/networking/ConnectionFactory.java com/stripe/android/stripe3ds2/transaction/StripeHttpClient.java em/c.java lj/u.java x5/b.java
00102	Set the phone speaker on	command	com/twiliorn/library/b.java
00003	Put the compressed bitmap data into JSON object	camera	tp/b.java
00123	Save the response to JSON after connecting to the remote server	network command	bo/app/u1.java bo/app/v0.java
00072	Write HTTP input stream into a file	command network file	com/microsoft/codepush/react/h.java

RULE ID	BEHAVIOUR	LABEL	FILES
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	o7/c.java
00016	Get location info of the device and put it to JSON object	location collection	com/amplitude/api/AmplitudeClient.java
00091	Retrieve data from broadcast	collection	com/braze/push/BrazeNotificationUtils.java com/braze/reactbridge/BrazeReactBridgeImpl.java com/stripe/android/link/LinkForegroundActivity.java rp/d.java xa/b.java
00043	Calculate WiFi signal strength	collection wifi	po/c.java
00024	Write file after Base64 decoding	reflection file	o5/v.java
00191	Get messages in the SMS inbox	sms	np/c.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00038	Query the phone number	collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00130	Get the current WIFI information	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00134	Get the current WiFi IP address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00082	Get the current WiFi MAC address	collection wifi	com/learnium/RNDeviceInfo/RNDeviceModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
00005	Get absolute path of file and put it to JSON object	file	com/microsoft/codepush/react/k.java
00056	Modify voice volume	control	tvi/webrtc/audio/WebRtcAudioTrack.java tvi/webrtc/voiceengine/WebRtcAudioTrack.java
00094	Connect to a URL and read data from it	command network	lj/u.java
00108	Read the input stream from given URL	network command	lj/u.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/211525694637/namespaces/firebase:fetch?key=AIzaSyAJ6SV3iMpFz4-tWyvdjOnoYO0sXS5G57Q. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.READ_EXTERNAL_STORAGE, android.permission.VIBRATE
Other Common Permissions	8/44	android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.gms.permission.AD_ID, android.permission.BLUETOOTH_ADMIN, android.permission.BLUETOOTH, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, android.permission.ACCESS_NOTIFICATION_POLICY, 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

DOMAIN	STATUS	GEOLOCATION
merchant-ui-api.stripe.com	ok	**IP:** 54.203.175.79 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
support.link.co	ok	**IP:** 18.238.109.94 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
codepush.appcenter.ms	ok	No Geolocation information available.
goo.gle	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
api.stripe.com	ok	**IP:** 52.26.11.205 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sdk.iad-01.braze.com	ok	**IP:** 104.18.39.68 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
api.eu.amplitude.com	ok	**IP:** 3.120.50.62 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
www.logo2.com	ok	**IP:** 13.248.169.48 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
www.logo1.com	ok	**IP:** 76.223.54.146 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
connect.finicity.com	ok	**IP:** 45.223.18.70 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
twitter.com	ok	**IP:** 172.66.0.227 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
errors.stripe.com	ok	**IP:** 198.202.176.161 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.797550 **Longitude:** -73.946190 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.217.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
checkout.link.com	ok	**IP:** 18.238.96.67 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
cdn.transcend-mobile-consent.com	ok	**IP:** 172.64.147.18 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
exoplayer.dev	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
notifee.app	ok	**IP:** 52.52.192.191 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
docs.swmansion.com	ok	**IP:** 172.67.142.188 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.braze.com	ok	**IP:** 104.17.227.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
files.stripe.com	ok	**IP:** 54.191.201.88 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
www.logo3.com	ok	**IP:** 195.30.84.13 **Country:** Germany **Region:** Bayern **City:** Munich **Latitude:** 48.137428 **Longitude:** 11.575490 **View:** Google Map
ppm.stripe.com	ok	**IP:** 52.40.139.248 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
sondheim.braze.com	ok	**IP:** 172.64.144.252 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
m.stripe.com	ok	**IP:** 52.40.40.91 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
link.co	ok	**IP:** 13.224.53.58 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **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
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

DOMAIN	STATUS	GEOLOCATION
manage.auth0.com	ok	**IP:** 172.64.148.184 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.cdn.stripe.com	ok	No Geolocation information available.
bnc.lt	ok	**IP:** 18.238.109.120 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
static.afterpay.com	ok	**IP:** 104.19.176.211 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
cdn.branch.io	ok	**IP:** 18.238.109.76 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api2.amplitude.com	ok	**IP:** 44.240.205.178 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
developer.apple.com	ok	**IP:** 17.253.83.145 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
support.stripe.com	ok	**IP:** 198.202.176.161 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.797550 **Longitude:** -73.946190 **View:** Google Map
b.stripecdn.com	ok	**IP:** 151.101.192.176 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **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
dust.k8s.test-001.d-usw-2.braze.com	ok	No Geolocation information available.
hooks.stripe.com	ok	**IP:** 54.203.175.79 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
stripe.com	ok	**IP:** 54.189.200.54 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
www.finicity.com	ok	**IP:** 45.223.18.70 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
q.stripe.com	ok	**IP:** 54.187.159.182 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
api.forhims.com	ok	**IP:** 104.18.41.149 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.forhims.com	ok	**IP:** 104.18.41.149 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
dashboard.stripe.com	ok	**IP:** 35.166.203.173 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
regionconfig.eu.amplitude.com	ok	**IP:** 18.238.96.28 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
dashif.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
api2.branch.io	ok	**IP:** 18.238.109.117 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
regionconfig.amplitude.com	ok	**IP:** 18.155.173.79 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
aomedia.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
r.stripe.com	ok	**IP:** 54.187.119.242 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

EMAILS

EMAIL	FILE
support@stripe.com	com/stripe/android/networking/FraudDetectionDataRequest.java
support@stripe.com	com/stripe/android/core/exception/APIConnectionException.java
support@stripe.com	com/stripe/android/core/networking/ApiRequest.java
test@test.com	com/stripe/android/financialconnections/features/networkinglinksignup/NetworkingLinkSignupPreviewParameterProvider.java

EMAIL	FILE
shortemail@email.com hatcouldbreakalayout@email.com	com/stripe/android/financialconnections/features/linkstepupverification/ComposableSingletons$LinkStepUpVerificationScreenKt.java
email@gmail.com	com/stripe/android/financialconnections/features/networkinglinkverification/ComposableSingletons$NetworkingLinkVerificationScreenKt.java
lthatshouldellipsize@gmail.com	com/stripe/android/financialconnections/features/networkinglinkloginwarmup/ComposableSingletons$NetworkingLinkLoginWarmupScreenKt.java
email@email.com	com/stripe/android/paymentsheet/paymentdatacollection/bacs/ComposableSingletons$BacsMandateConfirmationFormKt.java
theop@email.com	com/stripe/android/link/ui/LinkButtonKt.java
email@me.co	com/stripe/android/link/ui/inline/ComposableSingletons$LinkInlineSignupKt.java
support@stripe.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Amplitude	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/125
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
Instabug	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/206

HARDCODED SECRETS

POSSIBLE SECRETS
"AMPLITUDE_API_KEY" : "73e87329fc87b9ed767fc1a55872fdc3"
"BRANCH_KEY" : "key_live_eeWKZRkWGT4B0oNqamhHWmgatxkcvQog"
"BRAZE_ANDROID_API_KEY" : "ee78e0b2-8f49-4d7c-b9df-3c791fec27b5"
"BRAZE_IOS_API_KEY" : "45f7c992-36a2-4907-ae81-a7ed6bc59aa1"
"CODEPUSH_API_TOKEN_ANDROID" : "aece649065c9c1d5a06ce9cf8831b3bf3b0f2dab"
"CODEPUSH_API_TOKEN_IOS" : "3245f10f2a30bcd839f99377e2d1852de430a5d8"
"CODEPUSH_KEY" : "KWxlwlb4WMd4eP7goDjxN9R5P7u5luVIZD3Kv"
"INSTABUG_APP_TOKEN" : "adfa397308538b155eb1335de524dbf6"
"com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key"
"com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key"
"com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key"
"google_api_key" : "AIzaSyAJ6SV3iMpFz4-tWyvdjOnoYO0sXS5G57Q"
"google_crash_reporting_api_key" : "AIzaSyAJ6SV3iMpFz4-tWyvdjOnoYO0sXS5G57Q"
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a

POSSIBLE SECRETS
nb24gUm9vdCBDQSAxMB4XDTE1MDUyNjAwMDAwMFoXDTM4MDExNzAwMDAwMFowOTEL
nVOujw5H5SNz/0egwLX0tdHA114gk957EWW67c4cX8jJGKLhD+rcdqsq08p8kDi1L
nb3QgQ0EgMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALJ4gHHKeNXj
nU5PMCCjjmCXPI6T53iHTfIUJrU6adTrCC2qJeHZERxhlbI1Bjjt/msv0tadQ1wUs
1157920892373161954235709850086879078532699846656405640394575840079088346716 63
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f
idBuYYR7tj2wsa4rmqng7OfmLfavH0Bh
2758019355995970587784901184038904809305690585636156852142870730198868924130986086513626076488374510776543976123057 5
n5Msl+yMRQ+hDKXJioaldXgjUkK642M4UwtBV8ob2xJNDd2ZhwLnoQdeXeGADbkpy
4105836372515214212932612978004726840911444101599372555483525631403946740129 1
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
adfa397308538b155eb1335de524dbf6
45f7c992-36a2-4907-ae81-a7ed6bc59aa1

POSSIBLE SECRETS
MIIDQTCCAimgAwIBAgITBmyfz5m/jAo54vB4ikPmljZbyjANBgkqhkiG9w0BAQsF
dd830701de922d30b1ff642a6019b1c5
dcb428fea25c40e7b99f81ae5981ee6a
3267051002075881697808308513050704318447127338065924327593890433575733748242 4
ae2044fb577e65ee8bb576ca48a2f06e
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
deca87e736574c5c83c07314051fd93a
KWxlwlb4WMd4eP7goDjxN9R5P7u5luVIZD3Kv
109384903807373427451111239076680556993620759895168374899458639449595311615073501601370873757375962324859213229670631330943845253159101291214232748847898598 4
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 4 3
37a6259cc0c1dae299a7866489dff0bd
9a04f079-9840-4286-ab92-e65be0885f95

POSSIBLE SECRETS
nIFAGbHrQgLKm+a/sRxmPUDgH3KKHOVj4utWp+UhnMJbulHheb4mjUcAwhmahRWa6
55066263022277343669578718895168534326250603453777594175500187360389116729240
484395612939064517590525852527979142027629495260417479958440807170824046352 86
nca9HgFB0fW7Y14h29Jlo91ghYPl0hAEvrAIthtOgQ3pOsqTQNroBvo3bSMgHFzZM
e2719d58-a985-b3c9-781a-b030af78d30e
375718002577002046354550722449118360359445513476976248669456777961554447744055631669123440501294553956214444453728942852258566672919658081012434427757837678 4
no/ufQJVtMVT8QtPHRh8jrdkPSHCa2XV4cdFyQzR1bldZwgJcJmApzyMZFo6IQ6XU
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186160697311231 6
1157920892373161954235709850086879078528375642790749043826051631415181614943 37
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186160697311231 9
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
nMAkGA1UEBhMCVVMxDzANBgNVBAoTBkFtYXpvbjEZMBcGA1UEAxMQQW1hem9uIFJv
73e87329fc87b9ed767fc1a55872fdc3
266174080205021706322876871672336096072985916875697314770667136841880294499642780849154508062777190235209424122506555866215711354557091681416163731589599984 6

POSSIBLE SECRETS
5181942b9ebc31ce68dacb56c16fd79f
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
ee78e0b2-8f49-4d7c-b9df-3c791fec27b5
e0616e248c455e4850c927275fb80b91
3245f10f2a30bcd839f99377e2d1852de430a5d8
1ddaa4b892e61b0f7010597ddc582ed3
1157920892103562487626974469494075735300861434152903141955336313088670978539 48
nN+gDS63pYaACbvXy8MWy7Vu33PqUXHeeE6V/Uq2V8viTO96LXFvKWlJbYK8U90vv
nAYYwHQYDVR0OBBYEFIQYzIU07LwMlJQuCFmcx7IQTgoIMA0GCSqGSIb3DQEBCwUA
832571096148902998554675128952010817928785304886131559470920590248050319988441922443864376039294733307808651162787 1
24b2477514809255df232947ce7928c4
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087
36134250956749795798585127919587881956611106672985015071877198253568414405109

POSSIBLE SECRETS
nADA5MQswCQYDVQQGEwJVUzEPMA0GA1UEChMGQW1hem9uMRkwFwYDVQQDExBBbWF6
aece649065c9c1d5a06ce9cf8831b3bf3b0f2dab

PLAYSTORE INFORMATION

Title: Hims: Telehealth for Men

Score: 4.6574345 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.himshers.hims

Developer Details: Hims & Hers, Hims+%26+Hers, None, None, oguzhan@forhims.com,

Release Date: Aug 15, 2022 **Privacy Policy:** Privacy link

Description:

Hims: Take control of your health and well-being with Hims—the future of healthcare. Get access to best-in-class treatments and support for: Hims: Telehealth for convenient, quality care 100% online. Get access to best-in-class treatment for men's health concerns like hair loss, sexual health, weight loss, mental health, and skincare. Hair Growth: Regrow hair and stop hair loss with clinically proven prescription ingredients. Sexual Health: Personalized treatment and effective medications for erectile dysfunction, PE, and other sexual health concerns from the comfort (and privacy) of home. Weight Loss: Prescription weight loss personalized to your lifestyle, eating pattern, health history, and goals so you can lose weight and keep it off. Mental Health: Manage stress, ease anxiety, and get depression help with trusted medication and professional support. Skincare: Put your best face forward with treatments for acne, wrinkles, and signs of aging. With the app you can enjoy the benefits of telehealth from anywhere. Get questions answered quickly (responses typically within 24 hours), manage your shipments, access exclusive men's health content, and more. Feel great through the power of better health, with Hims. Please note: Content in the Hims app is for informational purposes only and does not constitute medical advice. Consult with a healthcare provider for any questions about your treatment, medical condition, or need for medical advice.

SCAN LOGS

Timestamp	Event	Error

2025-08-30 21:18:27	Generating Hashes	OK
2025-08-30 21:18:27	Extracting APK	OK
2025-08-30 21:18:27	Unzipping	OK
2025-08-30 21:18:28	Parsing APK with androguard	OK
2025-08-30 21:18:28	Extracting APK features using aapt/aapt2	OK
2025-08-30 21:18:28	Getting Hardcoded Certificates/Keystores	OK
2025-08-30 21:18:30	Parsing AndroidManifest.xml	OK
2025-08-30 21:18:30	Extracting Manifest Data	OK
2025-08-30 21:18:30	Manifest Analysis Started	OK
2025-08-30 21:18:30	Reading Network Security config from network_security_config.xml	OK
2025-08-30 21:18:30	Parsing Network Security config	OK

2025-08-30 21:18:30	Performing Static Analysis on: Hims (com.himshers.hims)	OK
2025-08-30 21:18:31	Fetching Details from Play Store: com.himshers.hims	OK
2025-08-30 21:18:31	Checking for Malware Permissions	OK
2025-08-30 21:18:31	Fetching icon path	OK
2025-08-30 21:18:31	Library Binary Analysis Started	OK
2025-08-30 21:18:31	Reading Code Signing Certificate	OK
2025-08-30 21:18:32	Running APKiD 2.1.5	OK
2025-08-30 21:18:34	Detecting Trackers	OK
2025-08-30 21:18:38	Decompiling APK to Java with JADX	OK
2025-08-30 21:19:03	Converting DEX to Smali	OK
2025-08-30 21:19:03	Code Analysis Started on - java_source	OK

2025-08-30 21:19:09	Android SBOM Analysis Completed	OK
2025-08-30 21:19:22	Android SAST Completed	OK
2025-08-30 21:19:22	Android API Analysis Started	OK
2025-08-30 21:19:33	Android API Analysis Completed	OK
2025-08-30 21:19:34	Android Permission Mapping Started	OK
2025-08-30 21:19:44	Android Permission Mapping Completed	OK
2025-08-30 21:19:45	Android Behaviour Analysis Started	OK
2025-08-30 21:20:00	Android Behaviour Analysis Completed	OK
2025-08-30 21:20:00	Extracting Emails and URLs from Source Code	OK
2025-08-30 21:20:06	Email and URL Extraction Completed	OK
2025-08-30 21:20:06	Extracting String data from APK	OK

2025-08-30 21:20:06	Extracting String data from Code	OK
2025-08-30 21:20:06	Extracting String values and entropies from Code	OK
2025-08-30 21:20:10	Performing Malware check on extracted domains	OK
2025-08-30 21:20:13	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.