ANDROID STATIC ANALYSIS REPORT

UHC (2.71.0)

File Name:	com.mobile.uhc_9704.apk
Package Name:	com.mobile.uhc
Scan Date:	Aug. 31, 2025, 5:56 a.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	6/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
3	25	3	3	1

FILE INFORMATION

File Name: com.mobile.uhc_9704.apk
Size: 68.7MB
MD5: 791f708be684c96ad4939d106584754d
SHA1: 13031a585881eef0921067115c281929eb3cc37c
SHA256: 78cd1f847d7c63dd189ec696cd8e682b707a960cc6926a95811b02ce28c21b9b

APP INFORMATION

App Name: UHC
Package Name: com.mobile.uhc
Main Activity: com.mobile.uhc.SplashActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 2.71.0

Android Version Code: 9704

APP COMPONENTS

Activities: 23
Services: 23
Receivers: 18
Providers: 19
Exported Activities: 6
Exported Services: 3
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-02-14 17:11:27+00:00
Valid To: 2045-07-02 17:11:27+00:00
Issuer: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Serial Number: 0x315be49a
Hash Algorithm: sha256
md5: bdc9a58488540d24407a9bb8fd37b3a6
sha1: 2c7fbe3d18a9c1cf7e51be7767aa82ad10765552
sha256: 7e90a016a0ef61e7200f9eb9b009d0512c7882afc56fa06e433fe0c33a1bcea0
sha512: 6a68df6bfdbb05d0570b0b25f732c9426b612628b1345b284e801f7cdd9a545216fcc1204ca62b8f59ca63be457fa40a0a65fabd3cec2b54cfe537f760d3ca81
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: fef445f261dc0c3f0b04aa4b4510cb1f0065ca341a78be3952fdfc63f83faf16
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.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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
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.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications

PERMISSION	STATUS	INFO	DESCRIPTION
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.webkit.resource.AUDIO_CAPTURE	unknown	Unknown permission	Unknown permission from android reference
android.webkit.resource.VIDEO_CAPTURE	unknown	Unknown permission	Unknown permission from android reference
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
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.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
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.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.mobile.uhc.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
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.BROADCAST_CLOSE_SYSTEM_DIALOGS	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>791f708be684c96ad4939d106584754d.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.TAGS check
network operator name check
device ID 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.MANUFACTURER check
Build.BOARD check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

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

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

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.mobile.uhc.MainActivity	Schemes: uhc-mobile://, x-rally://, https://, Hosts: unitedhealthcare.app.link, unitedhealthcare-alternate.app.link, uhc.app, unitedhealthcare.test-app.link, unitedhealthcare-alternate.test-app.link, uhc.test-app,

ACTIVITY	INTENT
com.plaid.internal.LinkRedirectActivity	Schemes: plaid://, Hosts: complete, redirect,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION

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: **14** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.

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	Activity (com.mobile.uhc.MainActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity (com.mobile.uhc.SessionTimeoutWarningModalActivity) 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.plaid.internal.LinkRedirectActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Activity (com.plaid.internal.link.LinkActivity) 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 (io.invertase.firebase.messaging.ReactNativeFirebaseMessagingReceiver) 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	Service (androidx.health.platform.client.impl.sdkservice.HealthDataSdkService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	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.
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	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

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

NO	ISSUE	SEVERITY	DESCRIPTION
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.

CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				app/notifee/core/Logger.java cl/json/social/SingleShareIntent.java com/adobe/marketing/mobile/AbstractHitsDatabase.java com/adobe/marketing/mobile/Analytics.java com/adobe/marketing/mobile/AnalyticsHitSchema.java com/adobe/marketing/mobile/AndroidCompressedFileService.java com/adobe/marketing/mobile/AndroidDatabase.java com/adobe/marketing/mobile/AndroidDatabaseService.java com/adobe/marketing/mobile/AndroidFullscreenMessage.java com/adobe/marketing/mobile/AndroidJsonUtility.java com/adobe/marketing/mobile/AndroidLoggingService.java com/adobe/marketing/mobile/AssuranceFullScreenTakeover.java com/adobe/marketing/mobile/AssuranceFullScreenTakeoverActivity.java com/adobe/marketing/mobile/AssuranceW

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/adobe/marketing/mobile/AssuranceWebViewSocket.java com/adobe/marketing/mobile/CacheManager.java com/adobe/marketing/mobile/ContextDataUtil.java com/adobe/marketing/mobile/DataMarshaller.java com/adobe/marketing/mobile/Event.java com/adobe/marketing/mobile/EventData.java com/adobe/marketing/mobile/EventQueueWorker.java com/adobe/marketing/mobile/FileUtil.java com/adobe/marketing/mobile/FloatingButtonView.java com/adobe/marketing/mobile/FullscreenMessageActivity.java com/adobe/marketing/mobile/HexStringUtil.java com/adobe/marketing/mobile/Identity.java com/adobe/marketing/mobile/IdentityHitSchema.java com/adobe/marketing/mobile/InboundEventQueueWorker.java com/adobe/marketing/mobile/LifecycleMetricsBuilder.java com/adobe/marketing/mobile/LifecycleSession.java com/adobe/marketing/mobile/LifecycleV2DataStoreCache.java com/adobe/marketing/mobile/Matcher.java com/adobe/marketing/mobile/RangedResolver.java com/adobe/marketing/mobile/SignalHitSchema.java com/adobe/marketing/mobile/StringUtils.java com/adobe/marketing/mobile/Target.java com/adobe/marketing/mobile/TargetPreviewManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/adobe/marketing/mobile/TargetResponseParser.java com/adobe/marketing/mobile/TimerState.java com/adobe/marketing/mobile/URLBuilder.java com/adobe/marketing/mobile/UrlUtilities.java com/adobe/marketing/mobile/UserProfile.java com/adobe/marketing/mobile/V4ToV5Migration.java com/adobe/marketing/mobile/XDMLifecycleEnvironment.java com/airbnb/lottie/utils/LogcatLogger.java com/amplitude/api/AmplitudeLog.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/GlideExecutor.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	/GlideExecutor.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SingletonConnectivityReceiver.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/util/pool/FactoryPools.java com/dynatrace/android/agent/util/Utility.java com/github/amarcruz/rntextsize/RNTextSizeConf.java com/hookedonplay/decoviewlib/charts/ChartSeries.java com/hookedonplay/decoviewlib/events/DecoEvent.java com/imagepicker/ImageMetadata.java com/imagepicker/Metadata.java com/imagepicker/VideoMetadata.java com/learnium/RNDeviceInfo/RNInstallReferrerClient.java com/liveperson/api/response/model/ConversationHistoryDetails.java com/liveperson/infra/InternetConnectionService.java com/liveperson/infra/log/AndroidLoggingDelegate.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/liveperson/infra/network/socket/ResponseMap.java com/liveperson/infra/utils/MaskedMessage.java com/liveperson/infra/utils/ThreadPoolExecutor.java com/liveperson/lp_structured_content/logger/SCLogHandler.java com/liveperson/lpappointmentscheduler/logger/LPAppointmentLog.java com/liveperson/messaging/model/IncaGetConversationsListResponse.java com/lugg/ReactNativeConfig/ReactNativeConfigModule.java com/mobile/uhc/common/ReadableMapWrapper.java com/mrousavy/camera/core/outputs/PhotoOutput.java com/mrousavy/camera/core/outputs/SurfaceOutput.java com/mrousavy/camera/frameprocessor/FrameProcessorPluginRegistry.java com/plaid/internal/cc.java com/plaid/internal/x5.java com/qualtrics/digital/DateExpression.java com/qualtrics/digital/DayExpression.java com/qualtrics/digital/DurationExpression.java com/qualtrics/digital/InterceptDefinition.java com/qualtrics/digital/Properties.java com/qualtrics/digital/QualtricsLog.java com/qualtrics/digital/TimeExpression.java com/qualtrics/digital/ViewCountExpression.java com/qualtrics/digital/resolvers/CustomPropertyResolver.java com/qualtrics/digital/resolvers/DateTimeTypeResolvers.java com/qualtrics/digital/resolvers/QualtricsSurveyResolver.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/qualtrics/digital/resolvers/SamplingResolver.java com/qualtrics/digital/resolvers/TimeSpentInAppResolver.java com/qualtrics/digital/resolvers/ViewCountResolver.java com/reactcommunity/rndatetimepicker/Common.java com/reactcommunity/rndatetimepicker/MinuteIntervalSnappableTimePickerDialog.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java com/rnfs/Downloader.java com/rnmaps/maps/FileUtil.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java com/samsung/android/sdk/internal/healthdata/HealthResultHolderImpl.java com/samsung/android/sdk/internal/healthdata/a.java com/scottyab/rootbeer/RootBeer.java com/scottyab/rootbeer/RootBeerNative.java com/scottyab/rootbeer/util/QLog.java com/sendbird/android/Logger.java com/shockwave/pdfium/PdfiumCore.java com/swmansion/reanimated/sensor/ReanimatedSensorContainer.java com/tom_roush/pdfbox/cos/COSString.java com/tom_roush/pdfbox/io/ScratchFile.java com/tom_roush/pdfbox/pdfparser/XrefTrailerResolver.java io/branch/referral/BranchJsonConfig.java io/branch/referral/BranchLogger.java io/invertase/firebase/app/ReactNativeFirebaseApp.java org/devio/rn/splashscreen/SplashScreen.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/greenrobot/eventbus/Logger.java org/wonday/orientation/OrientationActivityLifecycle.java timber/log/Timber.java
2	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/adobe/marketing/mobile/AndroidDatabase.java com/amplitude/api/DatabaseHelper.java com/clarisite/mobile/e/h.java com/dynatrace/android/agent/db/ParmDbHelper.java com/liveperson/infra/database/tables/ConversationsTable.java com/liveperson/infra/database/tables/FilesTable.java com/liveperson/infra/database/tables/MessagesTable.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java
				coil/request/ImageResult.java coil/request/Parameters.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/datadog/android/rum/internal/domain/scope/RumRawEvent.java com/datadog/trace/api/Config.java com/dynatrace/android/agent/events/eventsapi/EnrichmentAttribute.java com/launchdarkly/sdk/LDContext.java com/liveperson/infra/otel/models/OtlpAttribute.java com/mobile/uhc/BuildConfig.java com/qualtrics/digital/EmbeddedFeedbackUtilsJava.java

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	com/qualtrics/digital/XMDUtils.java com/rally/megazord/choicerewards/interactor/ChoiceRewardsClientConfigCacheKey.java com/rally/megazord/choicerewards/interactor/ChoiceRewardsConfigCacheKey.java com/rally/megazord/choicerewards/interactor/ChoiceRewardsTemplateDataCacheKey.java com/rally/megazord/common/cache/StringCacheKey.java com/rally/megazord/common/interactor/CacheOptions.java com/rally/megazord/devices/interactor/ConnectedTrackerListCacheKey.java com/rally/megazord/devices/interactor/LastSuccessSyncCacheKey.java com/rally/megazord/devices/interactor/ManualTrackingCacheKey.java com/rally/megazord/devices/interactor/PartnerListCacheKey.java com/rally/megazord/devices/interactor/ProductSettingsCacheKey.java com/rally/megazord/devices/interactor/TrackerListOfDataTypeCacheKey.java com/rally/megazord/devices/network/model/DataUnitType.java com/rally/megazord/healthactivity/common/HealthActivityCompletedFlagsCacheKeys.java com/rally/megazord/healthactivity/common/HealthActivityInProgressFlagsCacheKeys.java com/rally/megazord/healthprofile/network/model/RallyAgeConfigResponse.java com/rally/megazord/healthprofile/presentation/main/HealthProfileContent.java com/rally/megazord/healthprofile/presentation/main/UserDataContent.java com/rally/megazord/network/benefits/model/Detail.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/rally/megazord/network/benefits/model/HealthCareClaimDetails.java com/rally/megazord/network/benefits/model/MemberTieringResponse.java com/rally/megazord/network/support/model/SupportRequestData.java com/rally/megazord/rallyrewards/interactor/DashboardConfigCacheKey.java com/rally/megazord/rallyrewards/interactor/POCacheKey.java io/invertase/firebase/common/TaskExecutorService.java
4	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/adobe/marketing/mobile/AssuranceWebViewSocket.java
5	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/rnmaps/maps/FileUtil.java com/tom_roush/pdfbox/io/ScratchFile.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/clarisite/mobile/u/b.java com/clarisite/mobile/u/f.java com/dynatrace/android/agent/comm/ssl/SimpleX509TrustManager.java org/conscrypt/DefaultSSLContextImpl.java
7	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/datadog/opentracing/StringCachingBigInteger.java com/dynatrace/android/agent/data/RandomFactory.java com/dynatrace/android/agent/data/Session.java com/qualtrics/digital/SamplingUtil.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	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	li/yunqi/rnsecurestorage/cipherstorage/CipherStorageKeystoreAESCBC.java
9	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/b.java
10	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	org/conscrypt/CertificatePriorityComparator.java org/conscrypt/ChainStrengthAnalyzer.java org/conscrypt/EvpMdRef.java org/conscrypt/OAEPParameters.java org/conscrypt/OidData.java org/conscrypt/ct/CTConstants.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	com/ReactNativeBlobUtil/ReactNativeBlobUtilUtils.java com/tom_roush/pdfbox/pdmodel/encryption/MessageDigests.java
12	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/tom_roush/pdfbox/pdmodel/encryption/MessageDigests.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
13	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/dynatrace/android/agent/RootDetector.java com/dynatrace/android/agent/events/eventsapi/EnrichmentAttributesGenerator.java com/dynatrace/android/agent/events/eventsapi/EventMetrics.java com/scottyab/rootbeer/RootBeer.java
14	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/plaid/internal/vf.java
15	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/ReactNativeBlobUtil/Utils/PathResolver.java
16	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	com/scottyab/rootbeer/Const.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	coil/content/Utils.java com/ReactNativeBlobUtil/Utils/PathResolver.java com/adobe/marketing/mobile/AbstractHitsDatabase.java com/adobe/marketing/mobile/AndroidCompressedFileService.java com/adobe/marketing/mobile/CacheManager.java com/airbnb/lottie/network/NetworkCache.java com/datadog/android/v2/core/internal/storage/BatchId.java com/tom_roush/pdfbox/io/ScratchFile.java
00089	Connect to a URL and receive input stream from the server	command network	com/amplitude/api/ConfigManager.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/dynatrace/android/agent/comm/CommHandler.java com/plaid/internal/y3.java com/rnfs/Downloader.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java
00109	Connect to a URL and get the response code	network command	com/amplitude/api/ConfigManager.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/dynatrace/android/agent/comm/CommHandler.java com/plaid/internal/y3.java com/rnfs/Downloader.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java
00036	Get resource file from res/raw directory	reflection	coil/map/ResourceIntMapper.java com/liveperson/messaging/wm/impl/WelcomeMessageUriUtilsKt.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/adobe/marketing/mobile/AndroidCompressedFileService.java com/adobe/marketing/mobile/AndroidFullscreenMessage.java com/adobe/marketing/mobile/FileUtil.java com/airbnb/lottie/network/NetworkCache.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/imagepicker/VideoMetadata.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/rnmaps/maps/FileUtil.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java org/conscrypt/DefaultSSLContextImpl.java org/conscrypt/FileClientSessionCache.java org/conscrypt/KeyManagerFactoryImpl.java
00012	Read data and put it into a buffer stream	file	org/conscrypt/DefaultSSLContextImpl.java
00163	Create new Socket and connecting to it	socket	org/conscrypt/AbstractConscryptSocket.java org/conscrypt/KitKatPlatformOpenSSLSocketImplAdapter.java org/conscrypt/PreKitKatPlatformOpenSSLSocketImplAdapter.java
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/rnfs/Downloader.java com/samsung/android/sdk/internal/healthdata/DeviceUtil.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	cl/json/social/SingleShareIntent.java com/samsung/android/sdk/healthdata/HealthConnectionErrorResult.java n/o/t/i/f/e/e/l.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
00028	Read file from assets directory	file	com/clarisite/mobile/y/d.java
00078	Get the network operator name	collection telephony	io/branch/referral/SystemObserver.java
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/plaid/internal/y3.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	n/o/t/i/f/e/e/l.java
00189	Get the content of a SMS message	sms	com/ReactNativeBlobUtil/Utils/PathResolver.java
00192	Get messages in the SMS inbox	sms	com/ReactNativeBlobUtil/Utils/PathResolver.java
00188	Get the address of a SMS message	sms	com/ReactNativeBlobUtil/Utils/PathResolver.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/ReactNativeBlobUtil/Utils/PathResolver.java
00191	Get messages in the SMS inbox	sms	com/ReactNativeBlobUtil/Utils/PathResolver.java
00200	Query data from the contact list	collection contact	com/ReactNativeBlobUtil/Utils/PathResolver.java
00201	Query data from the call log	collection calllog	com/ReactNativeBlobUtil/Utils/PathResolver.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/ReactNativeBlobUtil/Utils/PathResolver.java
00024	Write file after Base64 decoding	reflection file	com/mobile/uhc/mail/MailAttachment.java
00072	Write HTTP input stream into a file	command network file	com/rnfs/Downloader.java

RULE ID	BEHAVIOUR	LABEL	FILES
00094	Connect to a URL and read data from it	command network	com/samsung/android/sdk/internal/healthdata/DeviceUtil.java
00108	Read the input stream from given URL	network command	com/samsung/android/sdk/internal/healthdata/DeviceUtil.java
00162	Create InetSocketAddress object and connecting to it	socket	org/conscrypt/AbstractConscryptSocket.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://uhc-mobile-production.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/963609806996/namespaces/firebase:fetch?key=AIzaSyBomWZf0xRI6ULOCnrGA33OSppMqWxGxmw. This is indicated by the response: The response code is 403

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	13/25	android.permission.INTERNET, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_NETWORK_STATE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.ACCESS_FINE_LOCATION, android.permission.VIBRATE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_COARSE_LOCATION, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE, android.permission.WRITE_EXTERNAL_STORAGE
Other Common Permissions	8/44	android.permission.ACTIVITY_RECOGNITION, android.permission.CHANGE_NETWORK_STATE, android.permission.CALL_PHONE, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.FOREGROUND_SERVICE, 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

DOMAIN	STATUS	GEOLOCATION
pinterest.com	ok	**IP:** 151.101.192.84 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
link.uhg.com	ok	**IP:** 18.238.96.77 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
helpcenter.werally.com	ok	**IP:** 34.211.108.47 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
rewards-edge.uhc.com	ok	**IP:** 13.219.8.161 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
plus.google.com	ok	**IP:** 142.250.75.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.myuhc.com	ok	**IP:** 18.238.109.108 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
device.payfone.com	ok	**IP:** 74.63.181.56 **Country:** United States of America **Region:** North Carolina **City:** Charlotte **Latitude:** 35.137260 **Longitude:** -80.936119 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
sendbird.com	ok	**IP:** 75.2.60.5 **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
developer.android.com	ok	**IP:** 142.250.201.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
clientsdk.launchdarkly.com	ok	**IP:** 151.101.1.55 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
rally-prod.s3.amazonaws.com	ok	**IP:** 52.217.198.33 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
api3-eu.branch.io	ok	**IP:** 18.155.173.77 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
mobile.launchdarkly.com	ok	**IP:** 18.211.63.6 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
uhc-mobile-production.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
cdn.branch.io	ok	**IP:** 18.238.109.61 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api2.amplitude.com	ok	**IP:** 54.202.178.61 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
hub.samsungapps.com	ok	**IP:** 54.77.39.19 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
clientstream.launchdarkly.com	ok	**IP:** 76.223.31.44 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
plaid.com	ok	**IP:** 18.238.96.30 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api.uhg.com	ok	**IP:** 172.65.65.68 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
regionconfig.eu.amplitude.com	ok	**IP:** 18.238.96.5 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xmlpull.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
dashboard.plaid.com	ok	**IP:** 18.155.173.106 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **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
www.facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
www.rally.com	ok	**IP:** 64.190.63.222 **Country:** Germany **Region:** Nordrhein-Westfalen **City:** Koeln **Latitude:** 50.933331 **Longitude:** 6.950000 **View:** Google Map
s.qualtrics.com	ok	**IP:** 23.202.57.104 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map

EMAILS

EMAIL	FILE
info@werally.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Adobe Experience Cloud		https://reports.exodus-privacy.eu.org/trackers/229
Amplitude	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/125
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Qualtrics		https://reports.exodus-privacy.eu.org/trackers/306

HARDCODED SECRETS

POSSIBLE SECRETS
"APP_STORE_PLACES_API_KEY" : "AIzaSyCl29Y3izUUAfT_KVyCWjHvWOkiu01RyAk"
"DEBUG_PLACES_API_KEY" : "AIzaSyCl29Y3izUUAfT_KVyCWjHvWOkiu01RyAk"
"INTERNAL_PLACES_API_KEY" : "AIzaSyCl29Y3izUUAfT_KVyCWjHvWOkiu01RyAk"
"UHCREWARDS_AWS_APPSYNC_API_KEY_PROD" : "BYYLswLSsxME3aZQrlkUt941J72PPr"
"UHCREWARDS_AWS_APPSYNC_AUTHENTICATION_TYPE_PROD" : "API_KEY"

POSSIBLE SECRETS
"UHCREWARDS_AWS_APPSYNC_GRAPHQL_ENDPOINT_PROD" : "https://link.uhg.com/graphql"
"UHCREWARDS_AWS_APPSYNC_REGION_PROD" : "us-east-1"
"UHCREWARDS_ENTERPRISE_REWARDS_SUPERGRAPH_CLIENT_SECRET_PROD" : "1oG9m2CtGC1D08HSkvbmxgiPkXvsI5pU1El"
"UHCREWARDS_ENTERPRISE_REWARDS_SUPERGRAPH_TOKEN_ENDPOINT_PROD" : "https://api.uhg.com/oauth2/token"
"UHCREWARDS_LD_PRODUCTION_API_KEY" : "mob-ba26e8b4-8bb9-4c61-8b16-6827c23ffcbc"
"UHCREWARDS_ONE_PORTAL_API_KEY_PROD" : "rdurwjde9vgrmjzba4dzcsys"
"UHCREWARDS_TRUST_COMMERCE_ID_LICENSE_KEY_PROD" : "BDNwfseBH0HBFD2eSdlt1E7GZoAq3s5m0gzrjuVi3SdHREDfvwqZ1hNqixE1iHo9"
"firebase_database_url" : "https://uhc-mobile-production.firebaseio.com"
"google_api_key" : "AIzaSyBomWZf0xRI6ULOCnrGA33OSppMqWxGxmw"
"google_crash_reporting_api_key" : "AIzaSyBomWZf0xRI6ULOCnrGA33OSppMqWxGxmw"
"places_api_key" : "AIzaSyDAadHlXWjVNP9xu-BtZvw0obAiB77KIOw"
"plaid_sentry_android_consumer_portal_api_key" : "2264cb9517ec4ddab918b90dd4126ae2"
"plaid_sentry_android_link_sdk_api_key" : "e7bf46248ac14774aecfe3a24811e6b4"
8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f

POSSIBLE SECRETS
000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F808182838485868788898A8B8C8D8E8F909192939495969798999A9B9C9D9E9FA0A1A2A3A4A5A6A7A8A9AAABACADAEAFB0B1B2B3B4B5B6B7B8B9BABBBCBDBEBFC0C1C2C3C4C5C6C7C8C9CACBCCCDCECFD0D1D2D3D4D5D6D7D8D9DADBDCDDDEDFE0E1E2E3E4E5E6E7E8E9EAEBECEDEEEFF0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF
47d6fd92e099cffe85bf56b188014cd60cb621c9
1oG9m2CtGC1D08HSkvbmxgiPkXvsI5pU1El
BDNwfseBH0HBFD2eSdlt1E7GZoAq3s5m0gzrjuVi3SdHREDfvwqZ1hNqixE1iHo9
b-ba26e8b4-8bb9-4c61-8b16-6827c23ffcbc
BYYLswLSsxME3aZQrlkUt941J72PPr

PLAYSTORE INFORMATION

Title: UnitedHealthcare

Score: 4.58408 **Installs:** 5,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.mobile.uhc

Developer Details: UNITED HEALTHCARE SERVICES, INC., UNITED+HEALTHCARE+SERVICES,+INC., None, http://uhc.com, uhcmobile@uhc.com,

Release Date: Sep 26, 2018 **Privacy Policy:** Privacy link

Description:

† Not all UHC plans are currently supported by the app, not all features are available for every plan Managing health care on the go just got easier with the UnitedHealthcare app! It's designed to save you time by providing easy access to your information. Features available are based on your personal health plan and can include: Find and Manage Providers - Find doctors, specialists, or health care facilities with our guided and location-based search. - Save your favorite doctors or facilities for easy access. Manage Claims† - Review your claims by member, provider, status, facility, service or date. - Review your claims payment breakdown and Explanation of Benefits. ID Card - Never lose your insurance card again! View and share your ID card. View Cost Estimates† - Know how much you could pay for treatments and specialty services. Reference Copays, deductibles, and out-of-pocket expenses† - View your copay, deductible, and out-of-pocket expenses. View Account Balances† - Know your health reimbursement, flexible spending, and Optum Bank health savings account balances. Easily Sign In - Use HealthSafe ID™ (a new, enhanced login that lets you access

nearly all UnitedHealthcare digital tools with one username and password) to securely access your app. - Never forget your password again with fingerprint login. Manage Your Health† - View personalized recommendations for preventative care.

SCAN LOGS

Timestamp	Event	Error
2025-08-31 05:56:23	Generating Hashes	OK
2025-08-31 05:56:28	Extracting APK	OK
2025-08-31 05:56:28	Unzipping	OK
2025-08-31 05:56:33	Parsing APK with androguard	OK
2025-08-31 05:56:33	Extracting APK features using aapt/aapt2	OK
2025-08-31 05:56:33	Getting Hardcoded Certificates/Keystores	OK
2025-08-31 05:56:39	Parsing AndroidManifest.xml	OK
2025-08-31 05:56:39	Extracting Manifest Data	OK

2025-08-31 05:56:39	Manifest Analysis Started	OK
2025-08-31 05:56:40	Reading Network Security config from network_security_config.xml	OK
2025-08-31 05:56:40	Parsing Network Security config	OK
2025-08-31 05:56:40	Performing Static Analysis on: UHC (com.mobile.uhc)	OK
2025-08-31 05:56:41	Fetching Details from Play Store: com.mobile.uhc	OK
2025-08-31 05:56:42	Checking for Malware Permissions	OK
2025-08-31 05:56:42	Fetching icon path	OK
2025-08-31 05:56:42	Library Binary Analysis Started	OK
2025-08-31 05:56:42	Reading Code Signing Certificate	OK
2025-08-31 05:56:43	Running APKiD 2.1.5	OK
2025-08-31 05:57:02	Detecting Trackers	OK

2025-08-31 05:57:09	Decompiling APK to Java with JADX	OK
2025-08-31 06:18:23	Decompiling with JADX timed out	TimeoutExpired(['/home/mobsf/.MobSF/tools/jadx/jadx-1.5.0/bin/jadx', '-ds', '/home/mobsf/.MobSF/uploads/791f708be684c96ad4939d106584754d/java_source', '-q', '-r', '--show-bad-code', '/home/mobsf/.MobSF/uploads/791f708be684c96ad4939d106584754d/791f708be684c96ad4939d106584754d.apk'], 999.9999770000577)
2025-08-31 06:18:23	Converting DEX to Smali	OK
2025-08-31 06:18:23	Code Analysis Started on - java_source	OK
2025-08-31 06:18:38	Android SBOM Analysis Completed	OK
2025-08-31 06:18:50	Android SAST Completed	OK
2025-08-31 06:18:50	Android API Analysis Started	OK
2025-08-31 06:18:58	Android API Analysis Completed	OK
2025-08-31 06:18:59	Android Permission Mapping Started	OK
2025-08-31 06:19:06	Android Permission Mapping Completed	OK

2025-08-31 06:19:07	Android Behaviour Analysis Started	OK
2025-08-31 06:19:16	Android Behaviour Analysis Completed	OK
2025-08-31 06:19:16	Extracting Emails and URLs from Source Code	OK
2025-08-31 06:19:20	Email and URL Extraction Completed	OK
2025-08-31 06:19:20	Extracting String data from APK	OK
2025-08-31 06:19:20	Extracting String data from Code	OK
2025-08-31 06:19:20	Extracting String values and entropies from Code	OK
2025-08-31 06:19:24	Performing Malware check on extracted domains	OK
2025-08-31 06:19:30	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.