ANDROID STATIC ANALYSIS REPORT

CenterWell
Pharmacy

🤖 CenterWell Pharmacy (8.2.1)

File Name:	com.humana.pharmacy_2012111825.apk
Package Name:	com.humana.pharmacy
Scan Date:	Aug. 30, 2025, 10:05 p.m.
App Security Score:	59/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

🥧 FINDINGS SEVERITY

🐛 HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	🔍 HOTSPOT
0	20	4	3	1

📦 FILE INFORMATION

File Name: com.humana.pharmacy_2012111825.apk
Size: 50.74MB
MD5: abda432eced888693252da38a026a0a9
SHA1: 5eb387ccd2dea086618ac0e85cf7f8bc447cc5d4
SHA256: d088bdf16ff8a34a46a245ef6369341e3b89e738749170f7c427fb8ac1e94bde

ℹ APP INFORMATION

App Name: CenterWell Pharmacy
Package Name: com.humana.pharmacy
Main Activity: com.humana.pharmacy.MainActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 8.2.1

Android Version Code: 2012111825

■■ APP COMPONENTS

Activities: 9
Services: 15
Receivers: 17
Providers: 6
Exported Activities: 3
Exported Services: 2
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=40202, ST=Kentucky, L=Louisville, O=Humana, OU=Mobile IT, CN=Trish Fulk
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-04-25 19:25:32+00:00
Valid To: 2041-04-19 19:25:32+00:00
Issuer: C=40202, ST=Kentucky, L=Louisville, O=Humana, OU=Mobile IT, CN=Trish Fulk
Serial Number: 0x4660cf03
Hash Algorithm: sha256
md5: 256436f68300ae69d46bb19529afd34c
sha1: b8ea3590dd06268d47b55493bb9023147d9bd55e
sha256: 6c4df6821dfd64e2cd928853a54c6735f2537b9ed0f93b0b6ebc32e279205991
sha512: e3c2b5c0a4d0f4110d50a1a77d6dd5f1671ff75563b40c7ae0bc7a8ec657324de0bfdc9d8ef5b96920f732fdecc34c4adb29e53a6345bde3b657fb0d742b3513
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 6f0803c15cd06d7bea0cdc049658ef74773739d788f74f16d11544e23c40bed4
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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.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.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.launcher.permission.INSTALL_SHORTCUT	normal	permits installation of shortcuts in Launcher.	Allows an application to install a shortcut in Launcher.
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.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.humana.pharmacy.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.

PERMISSION	STATUS	INFO	DESCRIPTION
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference

🔍 APKID ANALYSIS

FILE	DETAILS
abda432eced888693252da38a026a0a9.apk	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>possible VM check</td></tr></table>
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check network operator name check possible VM check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

FILE	DETAILS
classes2.dex	**FINDINGS / DETAILS** **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 **Compiler**: r8 without marker (suspicious)
classes3.dex	**FINDINGS / DETAILS** **Anti-VM Code**: Build.FINGERPRINT check, Build.MANUFACTURER check, Build.HARDWARE check, possible Build.SERIAL check, Build.TAGS check **Anti Debug Code**: Debug.isDebuggerConnected() check **Compiler**: r8 without marker (suspicious)

FILE	DETAILS
classes4.dex	**FINDINGS** / **DETAILS** Anti-VM Code — Build.MANUFACTURER check Compiler — r8 without marker (suspicious)

🗂 BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.humana.pharmacy.MainActivity	Schemes: myhumana://, http://, https://, cwp://, com.humana.pharmacy://, Hosts: www., viewOrders, viewMedication, viewTransferRx, cwpappredirect, cwpappredirectqa,

🔒 NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

🪪 CERTIFICATE ANALYSIS

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

🔍 MANIFEST ANALYSIS

HIGH: **0** | WARNING: **10** | 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	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
3	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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	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
5	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.
6	Activity (com.verint.xm.sdk.predictive.tracker.app.invite.InviteActivity) 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	Activity (com.verint.xm.sdk.predictive.tracker.app.survey.SurveyActivity) 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
8	Activity (com.verint.xm.sdk.predictive.com.verint.xm.sdk.surveymanagement.survey.SurveyManagementActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	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
10	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: **0** | WARNING: **8** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/airbnb/android/react/lottie/LottieAnimationViewPropertyManager.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java com/bumptech/glide/GeneratedAppGlideModul

NO	ISSUE	SEVERITY	STANDARDS	FILES
				eImpl.java com/bumptech/glide/Glide.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/integration/avif/AvifByteBufferBitmapDecoder.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/ThumbFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/SourceGenerator.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 com/bumptech/glide/load/engine/executor/RuntimeCompat.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/engine/prefill/BitmapPrefillRunner.java
				~~com/bumptech/glide/load/model/ByteBufferEncoder.java~~
				com/bumptech/glide/load/model/ByteBufferFileLoader.java
				com/bumptech/glide/load/model/FileLoader.java
				com/bumptech/glide/load/model/ResourceLoader.java
				com/bumptech/glide/load/model/StreamEncoder.java
				com/bumptech/glide/load/resource/DefaultOnHeaderDecodedListener.java
				com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java
				com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java
				com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java
				com/bumptech/glide/load/resource/bitmap/Downsampler.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/load/resource/bitmap/VideoDecoder.java
				com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java
				com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java
				com/bumptech/glide/load/resource/gif/StreamGifDecoder.java
				com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java
				com/bumptech/glide/manager/RequestManagerFragment.java
				com/bumptech/glide/manager/RequestManage

NO	ISSUE	SEVERITY	STANDARDS	FILES
				rRetriever.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SingletonConnectivityReceiver.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/caverock/androidsvg/CSSParser.java com/caverock/androidsvg/SVG.java com/caverock/androidsvg/SVGAndroidRenderer.java com/caverock/androidsvg/SVGImageView.java com/caverock/androidsvg/SVGParser.java com/caverock/androidsvg/SimpleAssetResolver.java com/dieam/reactnativepushnotification/helpers/ApplicationBadgeHelper.java com/dieam/reactnativepushnotification/modules/RNPushNotification.java com/dieam/reactnativepushnotification/modules/RNPushNotificationActions.java com/dieam/reactnativepushnotification/modules/RNPushNotificationAttributes.java com/dieam/reactnativepushnotification/modules/RNPushNotificationBootEventReceiver.java com/dieam/reactnativepushnotification/modules/RNPushNotificationConfig.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				es/RNPushNotificationConfig.java com/dieam/reactnativepushnotification/modul es/RNPushNotificationHelper.java com/dieam/reactnativepushnotification/modul es/RNPushNotificationListenerService.java com/dieam/reactnativepushnotification/modul es/RNPushNotificationPicturesAggregator.java com/dieam/reactnativepushnotification/modul es/RNPushNotificationPublisher.java com/dieam/reactnativepushnotification/modul es/RNReceivedMessageHandler.java com/dynatrace/android/agent/util/Utility.java com/dynatrace/android/callback/HttpClientCall back.java com/emeraldsanto/encryptedstorage/RNEncryp tedStorageModule.java com/gantix/JailMonkey/AdbEnabled/AdbEnable d.java com/gantix/JailMonkey/MockLocation/MockLoc ationCheck.java com/github/penfeizhou/animation/FrameAnim ationDrawable.java com/github/penfeizhou/animation/apng/decod e/APNGDecoder.java com/github/penfeizhou/animation/decode/Fra meSeqDecoder.java com/henninghall/date_picker/DerivedData.java com/henninghall/date_picker/pickers/AndroidN ative.java com/horcrux/svg/Brush.java com/horcrux/svg/ClipPathView.java com/horcrux/svg/ImageView.java com/horcrux/svg/LinearGradientView.java com/horcrux/svg/PatternView.java com/horcrux/svg/RadialGradientView.java com/horcrux/svg/UseView.java com/horcrux/svg/VirtualView.java com/learnium/RNDeviceInfo/RNDeviceModule.j ava com/learnium/RNDeviceInfo/RNInstallReferrerC lient.java com/learnium/RNDeviceInfo/resolver/DeviceId

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/learnium/RNDeviceInfo/resolver/DeviceId Resolver.java com/onetrust/OneTrust.java
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/onetrust/otpublishers/headless/Internal/L og/OTLogger.java com/onetrust/otpublishers/headless/Public/OT PublishersHeadlessSDK.java com/reactlibrary/VerintXMSdkModule.java com/reactnativecommunity/webview/RNCWeb View.java com/reactnativecommunity/webview/RNCWeb ViewClient.java com/reactnativecommunity/webview/RNCWeb ViewManagerImpl.java com/scottyab/rootbeer/RootBeer.java com/scottyab/rootbeer/RootBeerNative.java com/scottyab/rootbeer/util/QLog.java com/sslpublickeypinning/SslPublicKeyPinningM odule.java com/swmansion/gesturehandler/react/RNGestu reHandlerModule.java com/swmansion/gesturehandler/react/RNGestu reHandlerRootHelper.java com/swmansion/gesturehandler/react/RNGestu reHandlerRootView.java com/swmansion/reanimated/NativeMethodsHe lper.java com/swmansion/reanimated/ReanimatedModu le.java com/swmansion/reanimated/ReanimatedUIMa nagerFactory.java com/swmansion/reanimated/layoutReanimatio n/AnimationsManager.java com/swmansion/reanimated/layoutReanimatio n/ReanimatedNativeHierarchyManager.java com/swmansion/reanimated/layoutReanimatio n/SharedTransitionManager.java com/swmansion/reanimated/nativeProxy/Nativ eProxyCommon.java com/swmansion/reanimated/sensor/Reanimate dSensorContainer.java com/swmansion/rnscreens/ScreenStackHeader

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/tealium/adobe/api/AdobeVisitorAPI.java com/tealium/core/Logger.java com/tealium/react/TealiumReact.java com/tealium/react/Utils.java com/th3rdwave/safeareacontext/SafeAreaView.java com/verint/xm/react/CustomDigitalListener.java com/verint/xm/react/CustomInviteListener.java com/verint/xm/react/CustomVerintSDKListener.java com/verint/xm/sdk/common/Logging.java com/verint/xm/sdk/common/configuration/ConfigurationLoader.java com/verint/xm/sdk/internal/PredictiveFacade.java expo/modules/ExpoModulesPackage.java expo/modules/adapters/react/services/UIManagerModuleWrapper.java expo/modules/apploader/AppLoaderProvider.java expo/modules/camera/next/CameraViewNextModule.java expo/modules/camera/next/ExpoCameraView.java expo/modules/camera/next/analyzers/BarcodeAnalyzer.java expo/modules/constants/ConstantsService.java expo/modules/constants/ExponentInstallationId.java expo/modules/core/logging/OSLogHandler.java expo/modules/filesystem/FileSystemModule$definition$1$17$1$1.java expo/modules/filesystem/FileSystemModule$definition$1$18$1.java expo/modules/filesystem/FileSystemModule$definition$1$19$4.java expo/modules/filesystem/FileSystemModule$downloadResumableTask$2.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				expo/modules/filesystem/FileSystemModule.ja va
				expo/modules/image/ExpoImageView.java
				expo/modules/image/ImageViewWrapperTarge t.java
				expo/modules/image/ThumbnailRequestCoordi natorExtensionKt.java
				expo/modules/image/events/GlideRequestListe ner.java
				expo/modules/notifications/badge/BadgeHelpe r.java
				expo/modules/notifications/notifications/Argu mentsNotificationContentBuilder.java
				expo/modules/notifications/notifications/JSON NotificationContentBuilder.java
				expo/modules/notifications/notifications/backg round/BackgroundRemoteNotificationTaskCons umer.java
				expo/modules/notifications/notifications/prese ntation/ExpoNotificationPresentationEffectsMa nager.java
				expo/modules/notifications/notifications/prese ntation/builders/CategoryAwareNotificationBuil der.java
				expo/modules/notifications/notifications/prese ntation/builders/ChannelAwareNotificationBuil der.java
				expo/modules/notifications/notifications/prese ntation/builders/ExpoNotificationBuilder.java
				expo/modules/notifications/serverregistration/I nstallationId.java
				expo/modules/notifications/service/Notification sService.java
				expo/modules/notifications/service/delegates/E xpoHandlingDelegate.java
				expo/modules/notifications/service/delegates/E xpoNotificationLifecycleListener.java
				expo/modules/notifications/service/delegates/E xpoPresentationDelegate.java
				expo/modules/notifications/service/delegates/E xpoSchedulingDelegate.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/invertase/firebase/app/ReactNativeFirebaseApp.java
				io/invertase/firebase/app/ReactNativeFirebaseAppModule.java
				io/invertase/firebase/common/RCTConvertFirebase.java
				io/invertase/firebase/common/ReactNativeFirebaseEventEmitter.java
				io/invertase/firebase/common/SharedUtils.java
				io/invertase/firebase/messaging/ReactNativeFirebaseMessagingModule.java
				io/invertase/firebase/messaging/ReactNativeFirebaseMessagingReceiver.java
				io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java
				me/leolin/shortcutbadger/ShortcutBadger.java
				net/time4j/android/ApplicationStarter.java
				net/time4j/base/ResourceLoader.java
				net/time4j/format/expert/ChronoFormatter.java
				net/time4j/format/expert/CustomizedProcessor.java
				net/time4j/format/expert/DecimalProcessor.java
				net/time4j/format/expert/FormatStep.java
				net/time4j/format/expert/FractionProcessor.java
				net/time4j/format/expert/IgnorableWhitespaceProcessor.java
				net/time4j/format/expert/Iso8601Format.java
				net/time4j/format/expert/LiteralProcessor.java
				net/time4j/format/expert/LocalizedGMTProcessor.java
				net/time4j/format/expert/LookupProcessor.java
				net/time4j/format/expert/MultiFormatParser.java
				net/time4j/format/expert/NumberProcessor.java
				net/time4j/format/expert/OrdinalProcessor.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				net/time4j/format/expert/SkipProcessor.java net/time4j/format/expert/StyleProcessor.java net/time4j/format/expert/TextProcessor.java
				net/time4j/format/expert/TimezoneGenericProcessor.java net/time4j/format/expert/TimezoneIDProcessor.java net/time4j/format/expert/TimezoneNameProcessor.java net/time4j/format/expert/TimezoneOffsetProcessor.java net/time4j/format/expert/TwoDigitYearProcessor.java net/time4j/i18n/WeekdataProviderSPI.java net/time4j/tz/spi/ZoneNameProviderSPI.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/bumptech/glide/manager/RequestManagerRetriever.java com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java com/dynatrace/android/agent/events/eventsapi/EnrichmentAttribute.java com/dynatrace/android/agent/events/eventsapi/EnrichmentAttributesGenerator.java com/humana/pharmacy/BuildConfig.java com/onetrust/otpublishers/headless/Internal/Helper/k.java com/onetrust/otpublishers/headless/Internal/a.java com/onetrust/otpublishers/headless/Public/Keys/OTUXParamsKeys.java com/onetrust/otpublishers/headless/UI/DataModels/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	[Files may contain hardcoded sensitive information like usernames, passwords, keys etc.](#)	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/onetrust/otpublishers/headless/UI/UIProperty.java com/sslpublickeypinning/SslPublicKeyPinningModule.java com/tealium/core/consent/TealiumConfigConsentManagerKt.java com/tealium/core/persistence/e0.java com/tealium/core/persistence/i0.java com/tealium/core/settings/c.java com/tealium/react/Constants.java com/verint/xm/sdk/common/environment/Environment.java defpackage/CoreConstant.java expo/modules/adapters/react/NativeModulesProxy.java expo/modules/camera/next/tasks/ResolveTakenPictureKt.java expo/modules/camera/tasks/ResolveTakenPictureAsyncTaskKt.java expo/modules/constants/ExponentInstallationId.java expo/modules/image/records/SourceMap.java expo/modules/interfaces/permissions/PermissionsResponse.java expo/modules/notifications/notifications/ArgumentsNotificationContentBuilder.java expo/modules/notifications/notifications/JSONNotificationContentBuilder.java expo/modules/notifications/notifications/background/BackgroundRemoteNotificationTaskConsumer.java expo/modules/notifications/notifications/channels/serializers/NotificationsChannelGroupSerializer.java expo/modules/notifications/notifications/channels/serializers/NotificationsChannelSerializer.java expo/modules/notifications/notifications/presentation/builders/ExpoNotificationBuilder.java expo/modules/notifications/permissions/Notifi

NO	ISSUE	SEVERITY	STANDARDS	FILES
				cationPermissionsModuleKt.java expo/modules/notifications/serverregistration/InstallationId.java
				expo/modules/notifications/service/NotificationsService.java expo/modules/notifications/service/delegates/ExpoPresentationDelegate.java expo/modules/notifications/tokens/PushTokenModuleKt.java expo/modules/webbrowser/OpenBrowserOptions.java expo/modules/webbrowser/WebBrowserModuleKt.java io/invertase/firebase/common/TaskExecutorService.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingHeadlessService.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingSerializer.java
3	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	net/time4j/tz/spi/WinZoneProviderSPI.java com/dynatrace/android/agent/RootDetector.java com/dynatrace/android/agent/events/eventsapi/EnrichmentAttributesGenerator.java com/dynatrace/android/agent/events/eventsapi/EventMetrics.java com/dynatrace/android/agent/metrics/AndroidMetrics.java com/gantix/JailMonkey/Rooted/GreaterThan23.java com/gantix/JailMonkey/Rooted/LessThan23.java com/scottyab/rootbeer/RootBeer.java expo/modules/device/DeviceModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	c/l.java com/dynatrace/android/agent/comm/ssl/SimpleX509TrustManager.java com/onetrust/otpublishers/headless/Internal/Helper/j.java com/onetrust/otpublishers/headless/Internal/Helper/k.java com/onetrust/otpublishers/headless/Internal/Helper/n.java com/onetrust/otpublishers/headless/Internal/Network/ConsentUploadWorker.java com/onetrust/otpublishers/headless/Internal/Network/g.java com/onetrust/otpublishers/headless/UI/fragment/v.java com/sslpublickeypinning/SslPublicKeyPinningModule.java
5	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/learnium/RNDeviceInfo/RNDeviceModule.java com/reactnativecommunity/webview/RNCWebViewModuleImpl.java com/tealium/core/collection/DeviceCollector.java com/verint/xm/sdk/common/LaunchArgumentsHelper.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.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	com/apiguard3/internal/AGState.java com/apiguard3/internal/setLayerPaint.java com/apiguard3/internal/setVerticalScrollbarThumbDrawable.java com/dynatrace/android/agent/data/RandomFactory.java com/dynatrace/android/agent/data/Session.java com/verint/xm/sdk/common/b.java com/verint/xm/sdk/common/configuration/a.java com/verint/xm/sdk/common/utils/UserSamplingSelection.java com/verint/xm/sdk/predictive/tracker/NotificationWorker.java com/verint/xm/sdk/predictive/tracker/services/a.java
7	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	com/gantix/JailMonkey/HookDetection/HookDetectionCheck.java com/scottyab/rootbeer/Const.java
8	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/airbnb/lottie/network/NetworkCache.java com/verint/xm/sdk/common/utils/Util.java expo/modules/filesystem/FileSystemModule.java
9	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/dynatrace/android/agent/Dynatrace.java com/verint/xm/sdk/digital/view/DigitalActivity.java com/verint/xm/sdk/predictive/tracker/app/survey/SurveyActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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/dynatrace/android/agent/db/EventsDbHelper.java com/dynatrace/android/agent/db/ParmDbHelper.java com/tealium/core/persistence/g0.java com/tealium/core/persistence/h.java com/verint/xm/sdk/common/eventLogging/persistence/SQLPersister.java
11	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/onetrust/otpublishers/headless/UI/fragment/g.java
12	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/verint/xm/sdk/PredictiveLaunchArgumentsHelper.java expo/modules/adapters/react/permissions/PermissionsService.java expo/modules/constants/ExponentInstallationId.java expo/modules/notifications/service/delegates/SharedPreferencesNotificationsStore.java
13	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/RNCWebViewModuleImpl.java

🪪 NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

🖧 BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/tealium/adobe/api/network/HttpClient.java com/tealium/core/JsonLoader.java com/tealium/core/network/HttpClient.java com/tealium/remotecommanddispatcher/remotecommands/a.java com/verint/xm/sdk/common/network/d.java com/verint/xm/sdk/common/storyEngine/tasks/HttpAsyncTask.java com/verint/xm/sdk/predictive/tracker/tasks/HttpAsyncTask.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/dynatrace/android/agent/comm/CommHandler.java com/tealium/adobe/api/network/HttpClient.java com/tealium/core/JsonLoader.java com/tealium/core/network/HttpClient.java com/tealium/remotecommanddispatcher/remotecommands/a.java com/verint/xm/sdk/common/network/MultipartUtility.java com/verint/xm/sdk/common/network/b.java com/verint/xm/sdk/common/network/d.java com/verint/xm/sdk/common/storyEngine/tasks/HttpAsyncTask.java com/verint/xm/sdk/predictive/tracker/tasks/HttpAsyncTask.java com/verint/xm/sdk/predictive/tracker/tasks/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java com/dynatrace/android/agent/comm/CommHandler.java com/tealium/core/JsonLoader.java com/tealium/core/network/HttpClient.java com/tealium/remotecommanddispatcher/remotecommands/a.java com/verint/xm/sdk/common/network/MultipartUtility.java com/verint/xm/sdk/common/network/b.java com/verint/xm/sdk/common/network/d.java com/verint/xm/sdk/common/storyEngine/tasks/HttpAsyncTask.java com/verint/xm/sdk/predictive/tracker/tasks/HttpAsyncTask.java com/verint/xm/sdk/predictive/tracker/tasks/a.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/verint/xm/sdk/common/storyEngine/tasks/HttpAsyncTask.java com/verint/xm/sdk/predictive/tracker/tasks/HttpAsyncTask.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java com/humana/pharmacy/MainActivity.java com/verint/xm/sdk/common/utils/Util.java expo/modules/adapters/react/permissions/PermissionsService.java expo/modules/filesystem/FileSystemModule.java expo/modules/notifications/service/NotificationsService.java expo/modules/webbrowser/CustomTabsActivitiesHelperKt.java expo/modules/webbrowser/WebBrowserModule.java me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	expo/modules/adapters/react/permissions/PermissionsService.java expo/modules/webbrowser/CustomTabsActivitiesHelperKt.java expo/modules/webbrowser/WebBrowserModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
00078	Get the network operator name	collection telephony	com/dynatrace/android/agent/metrics/AndroidMetrics.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/tealium/core/collection/ConnectivityCollector.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	expo/modules/camera/next/tasks/ResolveTakenPicture.java expo/modules/camera/tasks/ResolveTakenPictureAsyncTask.java
00159	Use accessibility service to perform action getting node info by text	accessibility service	com/henninghall/date_picker/generated/NumberPicker.java
00013	Read file and put it into a stream	file	com/airbnb/android/react/lottie/LottieAnimationViewPropertyManager.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/apiguard3/internal/setContextClickable.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/resource/bitmap/ImageReader.java com/github/penfeizhou/animation/apng/decode/APNGParser.java com/github/penfeizhou/animation/gif/decode/GifParser.java com/github/penfeizhou/animation/io/FileReader.java com/github/penfeizhou/animation/webp/decode/WebPParser.java com/verint/xm/sdk/common/network/MultipartUtility.java expo/modules/core/logging/PersistentFileLog.java expo/modules/filesystem/FileSystemModule.java okio/Okio__JvmOkioKt.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

RULE ID	BEHAVIOUR	LABEL	FILES
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
00094	Connect to a URL and read data from it	command network	com/apiguard3/internal/setContextClickable.java com/verint/xm/sdk/common/network/MultipartUtility.java net/time4j/tz/spi/TimezoneRepositoryProviderSPI.java
00108	Read the input stream from given URL	network command	com/verint/xm/sdk/common/network/MultipartUtility.java
00022	Open a file from given absolute path of the file	file	com/airbnb/lottie/LottieCompositionFactory.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/apiguard3/internal/setFilterTouchesWhenObscured.java com/oblador/vectoricons/VectorIconsModuleImpl.java expo/modules/filesystem/FileSystemModule.java expo/modules/image/ExpoImageModule.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java
00028	Read file from assets directory	file	com/caverock/androidsvg/SimpleAssetResolver.java
00132	Query The ISO country code	telephony collection	com/tealium/core/collection/ConnectivityCollector.java
00121	Create a directory	file command	expo/modules/filesystem/FileSystemModule.java
00024	Write file after Base64 decoding	reflection file	com/airbnb/lottie/LottieCompositionFactory.java expo/modules/filesystem/FileSystemModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
00125	Check if the given file path exist	file	com/verint/xm/sdk/common/LaunchArgumentsHelper.java expo/modules/filesystem/FileSystemModule.java
00104	Check if the given path is directory	file	expo/modules/filesystem/FileSystemModule.java
00036	Get resource file from res/raw directory	reflection	com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java com/onetrust/otpublishers/headless/Internal/c.java com/verint/xm/sdk/common/utils/Util.java expo/modules/adapters/react/permissions/PermissionsService.java expo/modules/filesystem/FileSystemModule.java expo/modules/image/records/SourceMap.java expo/modules/notifications/service/NotificationsService.java io/invertase/firebase/common/SharedUtils.java me/leolin/shortcutbadger/impl/EverythingMeHomeBadger.java me/leolin/shortcutbadger/impl/HuaweiHomeBadger.java me/leolin/shortcutbadger/impl/NovaHomeBadger.java me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java
00091	Retrieve data from broadcast	collection	com/dieam/reactnativepushnotification/modules/RNPushNotification.java com/dieam/reactnativepushnotification/modules/RNPushNotificationPublisher.java com/verint/xm/sdk/common/LaunchArgumentsHelper.java expo/modules/notifications/service/NotificationsService.java
00175	Get notification manager and cancel notifications	notification	com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java expo/modules/notifications/badge/BadgeHelper.java expo/modules/notifications/service/delegates/ExpoPresentationDelegate.java
00153	Send binary data over HTTP	http	com/tealium/core/network/HttpClient.java

RULE ID	BEHAVIOUR	LABEL	FILES
00012	Read data and put it into a buffer stream	file	com/apiguard3/internal/setContextClickable.java
00189	Get the content of a SMS message	sms	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00188	Get the address of a SMS message	sms	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00191	Get messages in the SMS inbox	sms	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00200	Query data from the contact list	collection contact	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00187	Query a URI and check the result	collection sms calllog calendar	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00201	Query data from the call log	collection calllog	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00163	Create new Socket and connecting to it	socket	com/verint/xm/sdk/common/storyEngine/tasks/HttpAsyncTask.java com/verint/xm/sdk/predictive/tracker/tasks/HttpAsyncTask.java
00005	Get absolute path of file and put it to JSON object	file	com/airbnb/lottie/LottieCompositionFactory.java
00004	Get filename and put it to JSON object	file collection	com/airbnb/lottie/LottieCompositionFactory.java

🗄 FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://humanapharmacy-1316.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/984206957692/namespaces/firebase:fetch?key=AIzaSyClTYe-V8J5iVpT5MPyTHnFv2qgIDpw4Y4. This is indicated by the response: {'state': 'NO_TEMPLATE'}

⠿⠿ ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	10/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.CAMERA, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.VIBRATE, android.permission.WAKE_LOCK, android.permission.RECORD_AUDIO, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	4/44	com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

❗ OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

🔍 DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
expo.dev	ok	**IP:** 104.18.5.104 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
gateway.foresee.com	ok	**IP:** 18.238.109.98 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
survey-stg.foresee.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
stg-analytics.foresee.com	ok	**IP:** 3.230.28.211 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
analytics.foresee.com	ok	**IP:** 98.85.98.71 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
xml.org	ok	**IP:** 104.239.142.8 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
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:** 140.82.114.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.foresee.com	ok	**IP:** 23.185.0.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.792030 **Longitude:** -122.406853 **View:** Google Map
www.verint.com	ok	**IP:** 23.185.0.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.792030 **Longitude:** -122.406853 **View:** Google Map
tags.tiqcdn.com	ok	**IP:** 18.238.96.110 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
stg-gateway.foresee.com	ok	**IP:** 18.238.96.51 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
hoover-eu.verint-api.com	ok	**IP:** 35.156.49.248 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
collect.tealiumiq.com	ok	**IP:** 35.83.48.23 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.foresee.com	ok	**IP:** 52.70.206.228 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
st.foresee.com	ok	No Geolocation information available.
geolocation.1trust.app	ok	**IP:** 104.18.36.7 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
stg-cx.foresee.com	ok	No Geolocation information available.
survey.foresee.com	ok	No Geolocation information available.
hoover-eu-stg.verint-api.com	ok	**IP:** 34.252.104.243 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
hoover.foresee.com	ok	**IP:** 52.202.249.233 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
stg-cxsurvey.foresee.com	ok	No Geolocation information available.
cxsurvey.foresee.com	ok	No Geolocation information available.
services-edge.foresee.com	ok	**IP:** 54.156.68.125 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
cx.foresee.com	ok	**IP:** 18.238.96.24 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
cagf-dt.humana.com	ok	**IP:** 205.145.80.187 **Country:** United States of America **Region:** Kentucky **City:** Louisville **Latitude:** 38.252769 **Longitude:** -85.751556 **View:** Google Map
visitor-service.tealiumiq.com	ok	**IP:** 52.32.4.156 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
s.foresee.com	ok	**IP:** 18.238.96.31 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
humanapharmacy-1316.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
mobile-data.onetrust.io	ok	**IP:** 104.18.32.25 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
xmlpull.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
shopify.github.io	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
cookies2-ds.dev.otdev.org	ok	No Geolocation information available.
stg-hoover.foresee.com	ok	**IP:** 3.212.86.107 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
services-edge-stg.foresee.com	ok	**IP:** 54.243.236.204 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

✉ EMAILS

EMAIL	FILE
name@domain.com	Android String Resource

🕵 TRACKERS

TRACKER	CATEGORIES	URL
Dynatrace	Analytics	https://reports.exodus-privacy.eu.org/trackers/137
Tealium	Analytics	https://reports.exodus-privacy.eu.org/trackers/32

🔑 HARDCODED SECRETS

POSSIBLE SECRETS

"firebase_database_url" : "https://humanapharmacy-1316.firebaseio.com"

"google_api_key" : "AIzaSyClTYe-V8J5iVpT5MPyTHnFv2qgIDpw4Y4"

"google_crash_reporting_api_key" : "AIzaSyClTYe-V8J5iVpT5MPyTHnFv2qgIDpw4Y4"

11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650

16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a

6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151

258EAFA5-E914-47DA-95CA-C5AB0DC85B11

4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n

3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3

5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66

3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186160697311 2319

POSSIBLE SECRETS

aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7

051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00

0136024004378801593602050505

1157920892103562487626974469494075735300861434152903141955336313088670978539511

d3610855-748f-4365-9bb1-f036451fac27

3071c8717539de5d5353f4c8cd59a032

7d73d21f1bd82c9e5268b6dcf9fde2cb

686479766013060971498190079908139321726943530014330540939446345918554318339765539424505774633321719753296399637136332111386476861244038034037280889270700544 9

b5972162-1c03-4a5c-825a-5ddd587208c7

6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

1157920892103562487626974469494075735299969552241357603424222590610685512044369

▷ PLAYSTORE INFORMATION

Title: CenterWell Pharmacy

Score: 3.920297 **Installs:** 500,000+ **Price:** 0 **Android Version Support: Category:** Health & Fitness **Play Store URL:** com.humana.pharmacy

Developer Details: Humana Inc., 8169543994509222984, None, http://www.centerwellpharmacy.com, MobileDevelopers@centerwell.com,

Release Date: Apr 28, 2016 **Privacy Policy:** [Privacy link](#)

Description:

The new CenterWell Pharmacy™ mobile app makes it easier to keep track of your prescriptions. The new app has the same easy-to-use features, plus upcoming features focused on you. 1. Simplified refill ordering 2. Easy prescription transfers 3. Check your order's status at a glance ✔ COMPLETE MEDICATION LIST Stay organized with a full list of all your prescriptions filled at CenterWell Pharmacy, including those you no longer need and medication for your dependents. ✔ QUICK REFILLS Easily refill your prescriptions as soon as you sign in, straight from your home screen. ✔ PRESCRIPTION DETAILS View important details about your prescriptions, such as available refill dates, doctor information, images of your meds, and related educational videos. ✔ ORDER STATUS Know where your order is once it's processed with color-coded order status messages. ✔ SHIPMENT TRACKING Track shipments once they're shipped to estimate when your medication will arrive. ✔ SNAP-TO-FILL Submit a photo of your current prescription label to easily fill your prescription at CenterWell Pharmacy. ✔ TRANSFERS Quickly transfer your current prescriptions to CenterWell Pharmacy by viewing your prescription drug claims information from Humana. ✔ SPECIALTY MEDICATIONS Request a refill of an existing CenterWell Specialty Pharmacy™ prescription and order it at the same time as all your other medication. ✔ AUTO-REFILLS Automatically receive your next set of refills so you're sure to have your medication on time. NOTE: auto-refills are not available for Medicare customers. ✔ PAYMENT OPTIONS Change or update your credit card information and make payments securely from the app. ✔ PREFERENCES Set or update your preferences, such as how you want to be communicated (by phone, email or text) or if you'd like to receive an alert when your total charge is over your price limit. ✔ SHOP PRODUCTS Shop over-the-counter (OTC) products with the Health and Wellness credit that may be part of your Humana member benefit. NOTE: available to Medicare customers only. Download the CenterWell Pharmacy mobile app now to manage all your mail-delivery medications with ease! Note: The CenterWell Pharmacy mobile app is available only to Humana members. For issues with this app, please email cwpmobilefeedback@humana.com.

☰ SCAN LOGS

Timestamp	Event	Error
2025-08-30 22:05:02	Generating Hashes	OK
2025-08-30 22:05:02	Extracting APK	OK
2025-08-30 22:05:02	Unzipping	OK
2025-08-30 22:05:04	Parsing APK with androguard	OK

2025-08-30 22:05:04	Extracting APK features using aapt/aapt2	OK
2025-08-30 22:05:04	Getting Hardcoded Certificates/Keystores	OK
2025-08-30 22:05:06	Parsing AndroidManifest.xml	OK
2025-08-30 22:05:06	Extracting Manifest Data	OK
2025-08-30 22:05:06	Manifest Analysis Started	OK
2025-08-30 22:05:06	Performing Static Analysis on: CenterWell Pharmacy (com.humana.pharmacy)	OK
2025-08-30 22:05:07	Fetching Details from Play Store: com.humana.pharmacy	OK
2025-08-30 22:05:07	Checking for Malware Permissions	OK
2025-08-30 22:05:07	Fetching icon path	OK
2025-08-30 22:05:07	Library Binary Analysis Started	OK
2025-08-30 22:05:07	Reading Code Signing Certificate	OK

2025-08-30 22:05:08	Running APKiD 2.1.5	OK
2025-08-30 22:05:14	Detecting Trackers	OK
2025-08-30 22:05:19	Decompiling APK to Java with JADX	OK
2025-08-30 22:05:43	Converting DEX to Smali	OK
2025-08-30 22:05:43	Code Analysis Started on - java_source	OK
2025-08-30 22:05:49	Android SBOM Analysis Completed	OK
2025-08-30 22:06:02	Android SAST Completed	OK
2025-08-30 22:06:02	Android API Analysis Started	OK
2025-08-30 22:06:14	Android API Analysis Completed	OK
2025-08-30 22:06:14	Android Permission Mapping Started	OK
2025-08-30 22:06:26	Android Permission Mapping Completed	OK

2025-08-30 22:06:27	Android Behaviour Analysis Started	OK
2025-08-30 22:06:41	Android Behaviour Analysis Completed	OK
2025-08-30 22:06:41	Extracting Emails and URLs from Source Code	OK
2025-08-30 22:06:44	Email and URL Extraction Completed	OK
2025-08-30 22:06:44	Extracting String data from APK	OK
2025-08-30 22:06:44	Extracting String data from Code	OK
2025-08-30 22:06:44	Extracting String values and entropies from Code	OK
2025-08-30 22:06:49	Performing Malware check on extracted domains	OK
2025-08-30 22:06:52	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.