MOBSF

ANDROID STATIC ANALYSIS REPORT

AHM (2.0.6)

File Name:	com.americanHealthMarketplace_15.apk
Package Name:	com.americanHealthMarketplace
Scan Date:	Aug. 29, 2025, 7:35 p.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	14	1	1	1

FILE INFORMATION

File Name: com.americanHealthMarketplace_15.apk
Size: 24.0MB
MD5: 57d13269140d3f40f5739cf019f8179d
SHA1: 9b9fc5cbcc199ef0532a4de42e0c28f291ce3abf
SHA256: 5c05a314358f31360ec916d47a07495edbc1b5530113f7e6c99692a75a3f0c9c

APP INFORMATION

App Name: AHM
Package Name: com.americanHealthMarketplace
Main Activity: com.americanHealthMarketplace.MainActivity
Target SDK: 34
Min SDK: 29
Max SDK:
Android Version Name: 2.0.6
Android Version Code: 15

APP COMPONENTS

Activities: 6
Services: 13
Receivers: 15
Providers: 9
Exported Activities: 1
Exported Services: 2
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2023-10-31 14:06:10+00:00
Valid To: 2053-10-31 14:06:10+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x7125973d49d4152f7c827060bd443f4f05fa37d0
Hash Algorithm: sha256
md5: f181a389165ea152ae0c08eb6ab5b277
sha1: cd16fae11bb541eaebc4dcb1925191224c7db4e3
sha256: 4df87e0a379abb0fea6b4c2e5f7b2eba4a076e90e3628f61377b0adaf3fddd24
sha512: af64ac598354d2f15369515717aa3f0e7c1bea67e448a4552d7851efa7daf860b5467363b5c3d341a4685c2c4607d926f1d807187a92df1d316b295c493844ad
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 57dfd719a6e9fc7f8e3291f6a1cf6ac653b1b394ba719f9d560bed455f195fca
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.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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.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.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.americanHealthMarketplace.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.

PERMISSION	STATUS	INFO	DESCRIPTION
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
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

APKID ANALYSIS

FILE	DETAILS
57d13269140d3f40f5739cf019f8179d.apk	FINDINGS: Anti-VM Code — DETAILS: possible VM check

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

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.americanHealthMarketplace.MainActivity	Schemes: synergyapp://, https://, Hosts: webapp.dev.synergyinsurance.dnmiss.com, webapp.stage.synergyinsurance.net-craft.com, app.americanhm.org,

NETWORK SECURITY

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: 7 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	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.
3	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
4	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.
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 (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.
7	Broadcast Receiver (app.notifee.core.AlarmPermissionBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 6 | INFO: 1 | SECURE: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				app/notifee/core/AlarmPermissionBroadcastReceiver.java app/notifee/core/Logger.java app/notifee/core/RebootBroadcastReceiver.java app/notifee/core/b.java cl/json/RNShareImpl.java cl/json/RNSharePathUtil.java cl/json/social/InstagramShare.java cl/json/social/SingleShareIntent.java com/bumptech/glide/GeneratedAppGlideModuleImpl.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/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/GlideEx

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ception.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 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/ImageDecoderResourceDecoder.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/bitma

NO	ISSUE	SEVERITY	STANDARDS	FILES
				p/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/DefaultConnectivityMonitor.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/RequestTracker.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/github/barteksc/pdfviewer/PDFView.java com/github/barteksc/pdfviewer/RenderingHandler.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/github/barteksc/pdfviewer/link/DefaultLinkHandler.java com/henninghall/date_picker/DerivedData.java com/henninghall/date_picker/pickers/AndroidNative.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/imagepicker/ImageMetadata.java com/imagepicker/Metadata.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/RNInstallReferrerClient.java com/learnium/RNDeviceInfo/resolver/DeviceIdResolver.java com/lugg/RNCConfig/RNCConfigModule.java com/microsoft/codepush/react/CodePushUtils.java com/proyecto26/inappbrowser/RNInAppBrowser.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/reactnativecommunity/asyncstorage/AsyncStorageModule.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java com/reactnativecommunity/cookies/CookieManagerModule.java com/reactnativecommunity/webview/RNCWebView.java com/reactnativecommunity/webview/RNC

NO	ISSUE	SEVERITY	STANDARDS	FILES
				WebViewClient.java com/reactnativecommunity/webview/RNCWebViewManagerImpl.java com/reactnativedocumentpicker/RNDocumentPickerModule.java com/shockwave/pdfium/PdfiumCore.java com/swmansion/gesturehandler/react/RNGestureHandlerModule.java com/swmansion/gesturehandler/react/RNGestureHandlerRootHelper.java com/swmansion/gesturehandler/react/RNGestureHandlerRootView.java com/swmansion/reanimated/NativeMethodsHelper.java com/swmansion/reanimated/ReanimatedModule.java com/swmansion/reanimated/ReanimatedUIManagerFactory.java com/swmansion/reanimated/keyboard/WindowsInsetsManager.java com/swmansion/reanimated/layoutReanimation/AnimationsManager.java com/swmansion/reanimated/layoutReanimation/ReanimatedNativeHierarchyManager.java com/swmansion/reanimated/layoutReanimation/ScreensHelper.java com/swmansion/reanimated/layoutReanimation/SharedTransitionManager.java com/swmansion/reanimated/layoutReanimation/TabNavigatorObserver.java com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java com/swmansion/reanimated/sensor/ReanimatedSensorContainer.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/th3rdwave/safeareacontext/SafeAreaView.java com/zoontek/rnbootsplash/RNBootSplashModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				eightbitlab/com/blurview/BlurView.java io/invertase/firebase/app/ReactNativeFirebaseApp.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 io/invertase/notifee/NotifeeReactUtils.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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				net/time4j/format/expert/OrdinalProcessor.java 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 org/greenrobot/eventbus/Logger.java org/wonday/pdf/PdfView.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/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.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/americanHealthMarketplace/BuildConfig.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/microsoft/codepush/react/CodePushConstants.java com/microsoft/codepush/react/CodePushTelemetryManager.java com/nimbusds/jose/HeaderParameterNames.java com/nimbusds/jose/jwk/JWKParameterNames.java io/invertase/firebase/common/TaskExecutorService.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingHeadlessService.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingSerializer.java io/invertase/notifee/NotifeeEventSubscriber.java net/time4j/tz/spi/WinZoneProviderSPI.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/ReactNativeBlobUtil/ReactNativeBlobUtilFS.java com/ReactNativeBlobUtil/Utils/PathResolver.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/reactnativecommunity/webview/RNCWebViewModuleImpl.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.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/ReactNativeBlobUtil/ReactNativeBlobUtilBody.java com/reactnativecommunity/webview/RNCWebViewModuleImpl.java
6	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/nimbusds/jose/crypto/impl/AESCBC.java com/nimbusds/jose/jca/JCASupport.java
7	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
8	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/nimbusds/jose/jwk/Curve.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	app/notifee/core/Notifee.java cl/json/RNShareImpl.java cl/json/social/InstagramShare.java cl/json/social/SingleShareIntent.java com/ReactNativeBlobUtil/ReactNativeBlobUtilImpl.java com/ReactNativeBlobUtil/ReactNativeBlobUtilReq.java com/github/barteksc/pdfviewer/link/DefaultLinkHandler.java com/proyecto26/inappbrowser/RNInAppBrowser.java n/o/t/i/f/e/e/m.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	app/notifee/core/Notifee.java cl/json/social/InstagramShare.java com/ReactNativeBlobUtil/ReactNativeBlobUtilReq.java com/proyecto26/inappbrowser/RNInAppBrowser.java n/o/t/i/f/e/e/m.java
00036	Get resource file from res/raw directory	reflection	app/notifee/core/Notifee.java cl/json/RNSharePathUtil.java com/dylanvann/fastimage/FastImageSource.java com/proyecto26/inappbrowser/RNInAppBrowser.java io/invertase/firebase/common/SharedUtils.java n/o/t/i/f/e/e/n.java
00189	Get the content of a SMS message	sms	com/ReactNativeBlobUtil/Utils/PathResolver.java com/imagepicker/Utils.java com/reactnativedocumentpicker/RNDocumentPickerModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	cl/json/RNSharePathUtil.java cl/json/ShareFile.java cl/json/ShareFiles.java com/ReactNativeBlobUtil/ReactNativeBlobUtilFS.java com/ReactNativeBlobUtil/ReactNativeBlobUtilReq.java com/ReactNativeBlobUtil/Utils/PathResolver.java com/microsoft/codepush/react/CodePush.java com/microsoft/codepush/react/CodePushUpdateUtils.java com/microsoft/codepush/react/CodePushUtils.java com/microsoft/codepush/react/FileUtils.java com/reactnativedocumentpicker/RNDocumentPickerModule.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java
00188	Get the address of a SMS message	sms	com/ReactNativeBlobUtil/Utils/PathResolver.java com/imagepicker/Utils.java com/reactnativedocumentpicker/RNDocumentPickerModule.java
00200	Query data from the contact list	collection contact	com/ReactNativeBlobUtil/Utils/PathResolver.java com/imagepicker/Utils.java com/reactnativedocumentpicker/RNDocumentPickerModule.java
00201	Query data from the call log	collection calllog	com/ReactNativeBlobUtil/Utils/PathResolver.java com/imagepicker/Utils.java com/reactnativedocumentpicker/RNDocumentPickerModule.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/ReactNativeBlobUtil/Utils/PathResolver.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/imagepicker/Utils.java com/reactnativedocumentpicker/RNDocumentPickerModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/ReactNativeBlobUtil/ReactNativeBlobUtilBody.java com/ReactNativeBlobUtil/ReactNativeBlobUtilFS.java com/ReactNativeBlobUtil/ReactNativeBlobUtilMediaCollection.java com/ReactNativeBlobUtil/ReactNativeBlobUtilStream.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/microsoft/codepush/react/CodePushUpdateUtils.java com/microsoft/codepush/react/FileUtils.java com/nimbusds/jose/util/IOUtils.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java okio/Okio__JvmOkioKt.java
00072	Write HTTP input stream into a file	command network file	com/microsoft/codepush/react/CodePushUpdateManager.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/microsoft/codepush/react/CodePushUpdateManager.java com/nimbusds/jose/util/DefaultResourceRetriever.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java com/nimbusds/jose/util/DefaultResourceRetriever.java
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java
00024	Write file after Base64 decoding	reflection file	cl/json/ShareFile.java cl/json/ShareFiles.java com/ReactNativeBlobUtil/ReactNativeBlobUtilBody.java com/ReactNativeBlobUtil/ReactNativeBlobUtilReq.java

RULE ID	BEHAVIOUR	LABEL	FILES
00012	Read data and put it into a buffer stream	file	com/microsoft/codepush/react/FileUtils.java
00192	Get messages in the SMS inbox	sms	cl/json/RNSharePathUtil.java 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/ReactNativeBlobUtilReq.java com/ReactNativeBlobUtil/Utils/PathResolver.java
00094	Connect to a URL and read data from it	command network	net/time4j/tz/spi/TimezoneRepositoryProviderSPI.java
00005	Get absolute path of file and put it to JSON object	file	com/microsoft/codepush/react/CodePushUtils.java
00043	Calculate WiFi signal strength	collection wifi	com/reactnativecommunity/netinfo/ConnectivityReceiver.java
00091	Retrieve data from broadcast	collection	com/ReactNativeBlobUtil/ReactNativeBlobUtilReq.java
00125	Check if the given file path exist	file	com/ReactNativeBlobUtil/ReactNativeBlobUtilReq.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00078	Get the network operator name	collection telephony	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

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.INTERNET, android.permission.CAMERA, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	4/44	android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, android.permission.ACCESS_NOTIFICATION_POLICY, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
pinterest.com	ok	**IP:** 151.101.128.84 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **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
dkqk0o54zj.execute-api.us-east-1.amazonaws.com	ok	**IP:** 54.84.104.174 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
app.americanhm.org	ok	No Geolocation information available.
codepush.appcenter.ms	ok	No Geolocation information available.
notifee.app	ok	**IP:** 13.52.188.95 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
docs.swmansion.com	ok	**IP:** 172.67.142.188 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
backend.americanhm.org	ok	**IP:** 45.56.125.22 **Country:** United States of America **Region:** Texas **City:** Richardson **Latitude:** 32.948181 **Longitude:** -96.729721 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
plus.google.com	ok	**IP:** 64.233.185.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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
play.google.com	ok	**IP:** 172.253.124.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
referrals.amhm.com	ok	**IP:** 44.208.177.187 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.112.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"API_KEY_FIREBASE" : "AIzaSyCVQSIHkGwsbihm64fjrkLkquh6cHmP3v8"
"API_URl" : "api/v1/app/"
"API_V1" : "api/v1/"
"APP_KEY" : "7d5ed5aaf2cc1ebcdd016d5d1579cd"
"CODE_PUSH_DEPLOYMENT_KEY_ANDROID" : "jdG3zm0sgJB12S8f1PAxEqS6AL3RTNRoyoQvO"
"CODE_PUSH_DEPLOYMENT_KEY_IOS" : "2pM88NjZClS_MtaHzUwvDq0oIAzjVg-gFyK9O"
"GOOGLE_CLIENT_ID_FIREBASE_REVERSE" : "com.googleusercontent.apps.740481402445-jg0olknp8udnj2aa0f90ru77mlbmu67t"
115792089237316195423570985008687907853269984665640564039457584007908834671663

POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575
41058363725152142129326129780047268409114441015993725554835256314039467401291
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
32670510020758816978083085130507043184471273380659243275938904335757337482424
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
ae2044fb577e65ee8bb576ca48a2f06e
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
109384903807373427451111239076680556993620759895168374899458639449595311615073501601370873757375962324859213229670631330943845253159101291214232748847898598 4
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394 2643
55066263022277343669578718895168534326250603453777594175500187360389116729240
484395612939064517590525852527979142027629495260417479958440807170824046352 86
375718002577002046354550722449118360359445513476976248669456777961554447744055631669123440501294553956214444453728942852258566672919658081012434427757837678 4
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112316

POSSIBLE SECRETS
7d5ed5aaf2cc1ebcdd016d5d1579cd
jdG3zm0sgJB12S8f1PAxEqS6AL3RTNRoyoQvO
1157920892373161954235709850086879078528375642790749043826051631415181614943337
774a99c3bcdf634a74be04
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
266174080205021706322876871672336096072985916875697314770667136841880294499642780849154508062777190235209424122506555866215711354557091681416163731589599984 6
AIzaSyCVQSIHkGwsbihm64fjrkLkquh6cHmP3v8
5181942b9ebc31ce68dacb56c16fd79f
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
1ddaa4b892e61b0f7010597ddc582ed3
1157920892103562487626974469494075735300861434152903141955336313088670978539 48
832571096148902998554675128952010817928785304886131559470920590248050319988441922443864376039294733307808651162787 1
24b2477514809255df232947ce7928c4
262470350957996892686231567445669818918529234911092133878156159009255188547380500890223880539757197866508724767320 87

POSSIBLE SECRETS
361342509567497957985851279195878819566111066729850150718771982535684144051 09
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: American Health Marketplace

Score: 4.4257426 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.americanHealthMarketplace

Developer Details: American Health Reform Solutions, American+Health+Reform+Solutions, None, https://web.americanhm.org, memberservices@americanhm.org,

Release Date: Nov 16, 2023 **Privacy Policy:** Privacy link

Description:

Empower Your Health Journey with the AHM Mobile App Welcome to the AHM Mobile App by American Health Marketplace—your trusted companion for managing your health benefits, accessing support resources, and living well. Stay on Top of Your Benefits Check your insurance status and stay informed with notifications and updates that help you make the most of your coverage and benefits. Explore helpful resources Discover easy-to-read, helpful articles on health topics, food assistance, housing, family care, and more. We bring the information you need—right when you need it. Save more with the AHM Rx Card Access our free prescription discount card directly through the app and start saving on medications at participating pharmacies. Connect with Us Easily Need help? Call, email, or text us directly from the app. Our Care Team is here to support you every step of the way. Download the AHM Mobile App today and take the first step toward a healthier, more informed lifestyle.

SCAN LOGS

Timestamp	Event	Error

2025-08-29 19:35:07	Generating Hashes	OK
2025-08-29 19:35:07	Extracting APK	OK
2025-08-29 19:35:07	Unzipping	OK
2025-08-29 19:35:07	Parsing APK with androguard	OK
2025-08-29 19:35:08	Extracting APK features using aapt/aapt2	OK
2025-08-29 19:35:08	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 19:35:09	Parsing AndroidManifest.xml	OK
2025-08-29 19:35:09	Extracting Manifest Data	OK
2025-08-29 19:35:09	Manifest Analysis Started	OK
2025-08-29 19:35:09	Performing Static Analysis on: AHM (com.americanHealthMarketplace)	OK
2025-08-29 19:35:10	Fetching Details from Play Store: com.americanHealthMarketplace	OK

2025-08-29 19:35:11	Checking for Malware Permissions	OK
2025-08-29 19:35:11	Fetching icon path	OK
2025-08-29 19:35:11	Library Binary Analysis Started	OK
2025-08-29 19:35:11	Reading Code Signing Certificate	OK
2025-08-29 19:35:11	Running APKiD 2.1.5	OK
2025-08-29 19:35:13	Detecting Trackers	OK
2025-08-29 19:35:16	Decompiling APK to Java with JADX	OK
2025-08-29 19:35:33	Converting DEX to Smali	OK
2025-08-29 19:35:33	Code Analysis Started on - java_source	OK
2025-08-29 19:35:35	Android SBOM Analysis Completed	OK
2025-08-29 19:35:43	Android SAST Completed	OK

2025-08-29 19:35:43	Android API Analysis Started	OK
2025-08-29 19:35:51	Android API Analysis Completed	OK
2025-08-29 19:35:51	Android Permission Mapping Started	OK
2025-08-29 19:35:58	Android Permission Mapping Completed	OK
2025-08-29 19:35:59	Android Behaviour Analysis Started	OK
2025-08-29 19:36:06	Android Behaviour Analysis Completed	OK
2025-08-29 19:36:06	Extracting Emails and URLs from Source Code	OK
2025-08-29 19:36:08	Email and URL Extraction Completed	OK
2025-08-29 19:36:08	Extracting String data from APK	OK
2025-08-29 19:36:08	Extracting String data from Code	OK
2025-08-29 19:36:08	Extracting String values and entropies from Code	OK

2025-08-29 19:36:10	Performing Malware check on extracted domains	OK
2025-08-29 19:36:12	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.