ANDROID STATIC ANALYSIS REPORT

Dear Me (1.0.19)

File Name:	com.kompanion.habit.android_46.apk
Package Name:	com.kompanion.habit.android
Scan Date:	Aug. 30, 2025, 10:37 p.m.
App Security Score:	48/100 (MEDIUM RISK)

Grade:	B
Trackers Detection:	7/432

FINDINGS SEVERITY

HIGH	⚠ MEDIUM	INFO	✓ SECURE	HOTSPOT
2	19	4	1	1

FILE INFORMATION

File Name: com.kompanion.habit.android_46.apk
Size: 72.93MB
MD5: 70fc15e48f47d45e0e10806c5392be59
SHA1: b5c1fd3f27ad2e00b9336c1d101f178cc0265035
SHA256: 21ffccd17fb0adeb096e6891594b2e791477989446145f7decef507a0ff58555

APP INFORMATION

App Name: Dear Me
Package Name: com.kompanion.habit.android

Main Activity: com.kompanion.habit.android.MainActivity

Target SDK: 34

Min SDK: 24

Max SDK:

Android Version Name: 1.0.19

Android Version Code: 46

APP COMPONENTS

Activities: 14

Services: 16

Receivers: 20

Providers: 15

Exported Activities: 2

Exported Services: 2

Exported Receivers: 5

Exported Providers: 1

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: True
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: 2024-02-16 10:25:31+00:00
Valid To: 2054-02-16 10:25:31+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xf2289b3c2be444becd61c08b3c9391669ab1879
Hash Algorithm: sha256
md5: 7db32ac1f2e565c769d27c89268cfbbf
sha1: d8086a2dc34aa4b4b01669e3900c53aa4c079320
sha256: 0350cbed2c6831586436a5f4d977abbe5414d6588af712e77a7423c7f37be9ed
sha512: 8c5e4d975d0fd86d0cac0c188831665aaa296e93b68856ed330675c8b6670fad136d442ff09cda8e846b0cfac86d70bc9e19b958517ab49f689f223bef8ce89e
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 635a028000ec1780992d6dbfd0a74e5d1dc9183bff9ac79a9bcfee02ad77b64b
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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.

PERMISSION	STATUS	INFO	DESCRIPTION
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	unknown	Unknown permission	Unknown permission from android reference
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.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_MEDIA_AUDIO	dangerous	allows reading audio files from external storage.	Allows an application to read audio files from external storage.
com.kompanion.habit.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
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.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>70fc15e48f47d45e0e10806c5392be59.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
possible Build.SERIAL check
network operator name check
device ID check
ro.kernel.qemu check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
possible Build.SERIAL check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
network operator name check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.kompanion.habit.android.MainActivity	Schemes: kompanion.habit.test://, kompanion.habit://,

ACTIVITY	INTENT
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.kompanion.habit.android,

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: 1 | WARNING: 10 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Content Provider (com.facebook.FacebookContentProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
3	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.
4	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
5	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
6	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.
7	Activity (com.facebook.CustomTabActivity) 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.
8	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.
9	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
10	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.
11	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: **0** | WARNING: **7** | INFO: **4** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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/rnfs/RNFSManager.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java
2	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/amplitude/api/PinnedAmplitudeClient.java zendesk/core/ZendeskNetworkModule.java zendesk/support/SupportSdkModule.java
				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/airbnb/android/react/lottie/LottieAnimationViewPropertyManager.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/ammarahmed/mmkv/RNMMKVModule.java com/ammarahmed/mmkv/SecureKeystore.java com/amplitude/api/AmplitudeLog.java com/appsflyer/internal/AFa1aSDK.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1uSDK.java com/appsflyer/internal/AFc1vSDK.java com/appsflyer/internal/AFf1cSDK.java com/appsflyer/internal/AFf1dSDK.java com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1kSDK.java com/appsflyer/internal/AFf1lSDK.java com/appsflyer/internal/AFf1tSDK.java com/appsflyer/internal/AFg1hSDK.java com/appsflyer/internal/AFg1jSDK.java com/appsflyer/internal/AFg1nSDK.java com/appsflyer/reactnative/RNAppsFlyerModule.java com/appsflyer/share/CrossPromotionHelper.java com/appsflyer/share/LinkGenerator.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/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 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/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/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

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/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/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/ijzerenhein/sharedelement/RNSharedElementNode.java com/imagepicker/ImageMetadata.java com/imagepicker/Metadata.java com/imagepicker/VideoMetadata.java com/jakewharton/disklrucache/DiskLruCache.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/RNInstallReferrerClient.java com/learnium/RNDeviceInfo/resolver/DeviceIdResolver.java com/lugg/ReactNativeConfig/ReactNativeConfigModule.java com/oblador/keychain/KeychainModule.java com/oblador/keychain/cipherStorage/CipherStorageBase.java com/oblador/keychain/cipherStorage/CipherStorageFacebookConceal.java com/oblador/keychain/cipherStorage/CipherStorageKeystoreAesCbc.java com/oblador/keychain/cipherStorage/CipherStorageKeystoreRsaEcb.java com/oblador/keychain/decryptionHandler/DecryptionResultHandlerInteractiveBiometric.java com/oblador/keychain/decryptionHandler/DecryptionResultHandlerInteractiveBiometricManualRetry.java com/reactnativecommunity/webview/RNCWebView.java com/reactnativecommunity/webview/RNCWebViewClient.java com/reactnativecommunity/webview/RNCWebViewManagerImpl.java com/reactnativegooglesignin/PromiseWrapper.java com/reactnativegooglesignin/RNGoogleSigninModule.java com/rnfs/Downloader.java com/sparkfabrikreactnativeidfaaaid/ReactNativeIdfaAaidModule.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/layoutReanimation/AnimationsManager.java com/swmansion/reanimated/layoutReanimation/ReanimatedNativeHierarchyManager.java com/swmansion/reanimated/layoutReanimation/SharedTransitionManager.java com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java com/swmansion/reanimated/sensor/ReanimatedSensorContainer.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/th3rdwave/safeareacontext/SafeAreaView.java com/wheelpicker/LoopRunnable.java com/wheelpicker/LoopTimerTask.java com/wheelpicker/LoopView.java com/wheelpicker/LoopViewGestureListener.java com/wheelpicker/MTimer.java com/wheelpicker/MessageHandler.java com/wheelpicker/WheelPickerManager.java com/zendesk/logger/Logger.java com/zoontek/rnbootsplash/RNBootSplashModuleImpl.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				dagger/android/AndroidInjection.java expo/modules/ExpoModulesPackage.java expo/modules/adapters/react/services/UIManagerModuleWrapper.java expo/modules/apploader/AppLoaderProvider.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 expo/modules/filesystem/FileSystemModule.java fr/greweb/reactnativeviewshot/RNViewShotModule.java fr/greweb/reactnativeviewshot/ViewShot.java 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/crashlytics/ReactNativeFirebaseCrashlyticsInitProvider.java io/invertase/firebase/crashlytics/ReactNativeFirebaseCrashlyticsModule.java io/invertase/firebase/installations/ReactNativeFirebaseInstallationsModule.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 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 zendesk/belvedere/BelvedereFileProvider.java zendesk/belvedere/L.java zendesk/belvedere/Storage.java zendesk/messaging/MessagingModel.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/RNAppleAuthentication/webview/SignInWebViewDialogFragment.java com/amplitude/api/AmplitudeClient.java com/appsflyer/reactnative/RNAppsFlyerConstants.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/kompanion/habit/android/BuildConfig.java com/oblador/keychain/KeychainModule.java expo/modules/adapters/react/NativeModulesProxy.java expo/modules/constants/ExponentInstallationId.java expo/modules/interfaces/permissions/PermissionsResponse.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 zendesk/core/Constants.java zendesk/core/LegacyIdentityMigrator.java zendesk/core/ZendeskCoreSettingsStorage.java zendesk/core/ZendeskIdentityStorage.java zendesk/core/ZendeskMachineIdStorage.java zendesk/core/ZendeskStorage.java zendesk/messaging/MessagingActivity.java zendesk/support/CreateRequest.java zendesk/support/LegacyRequestMigrator.java zendesk/support/ZendeskArticleVoteStorage.java zendesk/support/ZendeskHelpCenterSettingsProvider.java zendesk/support/ZendeskRequestStorage.java zendesk/support/ZendeskSupportSettingsProvider.java zendesk/support/requestlist/RequestListModel.java zendesk/support/requestlist/RequestListView.java
5	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	com/reactnativecommunity/clipboard/ClipboardModule.java
6	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/amplitude/eventexplorer/EventExplorerInfoActivity.java com/reactnativecommunity/clipboard/ClipboardModule.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/airbnb/lottie/network/NetworkCache.java expo/modules/filesystem/FileSystemModule.java
8	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	expo/modules/adapters/react/permissions/PermissionsService.java expo/modules/constants/ExponentInstallationId.java
9	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/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFb1gSDK.java com/appsflyer/internal/AFc1fSDK.java
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/amplitude/api/DatabaseHelper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	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 fr/greweb/reactnativeviewshot/RNViewShotModule.java
12	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/RNAppleAuthentication/webview/SignInWebViewDialogFragment.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00192	Get messages in the SMS inbox	sms	cl/json/RNSharePathUtil.java com/appsflyer/internal/AFb1jSDK.java com/rnfs/RNFSManager.java
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/airbnb/lottie/LottieCompositionFactory.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/appsflyer/internal/AFg1jSDK.java com/rnfs/RNFSManager.java expo/modules/filesystem/FileSystemModule.java fr/greweb/reactnativeviewshot/RNViewShotModule.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java zendesk/belvedere/BitmapUtils.java zendesk/belvedere/Storage.java zendesk/core/ZendeskSessionStorage.java zendesk/support/request/AttachmentUploadService.java zendesk/support/request/CellAttachmentLoadingUtil.java

RULE ID	BEHAVIOUR	LABEL	FILES
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/ammarahmed/mmkv/Storage.java com/appsflyer/internal/AFb1iSDK.java com/appsflyer/internal/AFg1jSDK.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/imagepicker/VideoMetadata.java com/jakewharton/disklrucache/DiskLruCache.java com/rnfs/RNFSManager.java com/rnfs/Uploader.java expo/modules/core/logging/PersistentFileLog.java expo/modules/filesystem/FileSystemModule.java okio/Okio__JvmOkioKt.java
00028	Read file from assets directory	file	com/rnfs/RNFSManager.java
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/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1bSDK.java com/appsflyer/internal/AFc1vSDK.java com/appsflyer/internal/AFf1vSDK.java expo/modules/adapters/react/permissions/PermissionsService.java expo/modules/filesystem/FileSystemModule.java n/o/t/i/f/e/e/m.java zendesk/messaging/ui/UtilsAttachment.java zendesk/support/guide/ViewArticleActivity.java zendesk/support/request/ComponentInputForm.java zendesk/support/requestlist/RequestListView.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 expo/modules/adapters/react/permissions/PermissionsService.java n/o/t/i/f/e/e/m.java zendesk/messaging/ui/UtilsAttachment.java zendesk/support/guide/ViewArticleActivity.java
00089	Connect to a URL and receive input stream from the server	command network	com/amplitude/api/ConfigManager.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/rnfs/Downloader.java
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/rnfs/Downloader.java
00109	Connect to a URL and get the response code	network command	com/amplitude/api/ConfigManager.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java com/appsflyer/internal/AFf1jSDK.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/rnfs/Downloader.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFi1bSDK.java com/appsflyer/internal/AFi1iSDK.java com/appsflyer/internal/AFi1jSDK.java
00043	Calculate WiFi signal strength	collection wifi	com/reactnativecommunity/netinfo/ConnectivityReceiver.java
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java
00014	Read file into a stream and put it into a JSON object	file	com/appsflyer/internal/AFg1jSDK.java
00005	Get absolute path of file and put it to JSON object	file	com/airbnb/lottie/LottieCompositionFactory.java com/appsflyer/internal/AFg1jSDK.java
00091	Retrieve data from broadcast	collection	com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1vSDK.java
00036	Get resource file from res/raw directory	reflection	app/notifee/core/Notifee.java cl/json/RNSharePathUtil.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFf1qSDK.java com/appsflyer/internal/AFi1iSDK.java com/appsflyer/internal/AFi1nSDK.java com/dylanvann/fastimage/FastImageSource.java expo/modules/adapters/react/permissions/PermissionsService.java expo/modules/filesystem/FileSystemModule.java io/invertase/firebase/common/SharedUtils.java n/o/t/i/f/e/e/n.java
00024	Write file after Base64 decoding	reflection file	cl/json/ShareFile.java cl/json/ShareFiles.java com/airbnb/lottie/LottieCompositionFactory.java expo/modules/filesystem/FileSystemModule.java
00121	Create a directory	file command	expo/modules/filesystem/FileSystemModule.java
00125	Check if the given file path exist	file	expo/modules/filesystem/FileSystemModule.java
00104	Check if the given path is directory	file	expo/modules/filesystem/FileSystemModule.java
00016	Get location info of the device and put it to JSON object	location collection	com/amplitude/api/AmplitudeClient.java
00189	Get the content of a SMS message	sms	zendesk/belvedere/Storage.java
00188	Get the address of a SMS message	sms	zendesk/belvedere/Storage.java
00200	Query data from the contact list	collection contact	zendesk/belvedere/Storage.java
00201	Query data from the call log	collection calllog	zendesk/belvedere/Storage.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java zendesk/belvedere/Storage.java

RULE ID	BEHAVIOUR	LABEL	FILES
00078	Get the network operator name	collection telephony	com/amplitude/api/DeviceInfo.java com/appsflyer/internal/AFi1xSDK.java com/learnium/RNDeviceInfo/RNDeviceModule.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00130	Get the current WIFI information	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00134	Get the current WiFi IP address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00082	Get the current WiFi MAC address	collection wifi	com/learnium/RNDeviceInfo/RNDeviceModule.java
00009	Put data in cursor to JSON object	file	com/amplitude/api/DatabaseHelper.java
00094	Connect to a URL and read data from it	command network	net/time4j/tz/spi/TimezoneRepositoryProviderSPI.java
00012	Read data and put it into a buffer stream	file	com/rnfs/Uploader.java
00004	Get filename and put it to JSON object	file collection	com/airbnb/lottie/LottieCompositionFactory.java
00137	Get last known location of the device	location collection	com/amplitude/api/DeviceInfo.java
00115	Get last known location of the device	collection location	com/amplitude/api/DeviceInfo.java
00132	Query The ISO country code	telephony collection	com/amplitude/api/DeviceInfo.java
00072	Write HTTP input stream into a file	command network file	com/rnfs/Downloader.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/101330198578/namespaces/firebase:fetch?key=AIzaSyDIZuCTlD7jNWFdPC6enPwsaF-L6GGSyyY is enabled. Ensure that the configurations are not sensitiv referrerScreen=BANNER","image":{"ar":"https://dsgmc6umf6chc.cloudfront.net/habit/banner-images/ar/Discount%20Banner_fall_ar.png","de":"https://dsgmc6umf6chc.cloudfront.net/habit/banner-images/de/Discount%20Banner_fall_de.png"," images/id/Discount%20Banner_fall_id.png","it":"https://dsgmc6umf6chc.cloudfront.net/habit/banner-images/it/Discount%20Banner_fall_it.png","ja":"https://dsgmc6umf6chc.cloudfront.net/habit/banner-images/ja/Discount%20Banner_fall_ja.pn '{"calendarScreenInitialTabConfigId":"default","initialTab":"CALENDAR"}', 'cycle_period_popup_config': '{"cyclePeriodPopupConfigId":"default","enabled":true,"subscriberOnly":false,"deepLink":"https://apps.apple.com/redeem?ctx=offercodes&id= '{"configId":"default","availableAuthenticators":["Apple","Google","Facebook"]}', 'external_paywall_config': '{"paywallConfigId":"default","packages":["kompanion.habit.plus.monthly.direct","kompanion.habit.plus.yearly.direct","kompanion.habit.p ["kompanion.habit.plus.monthly.direct","kompanion.habit.plus.yearly.lto","kompanion.habit.plus.3months.direct"],"bestValuePackageId":"kompanion.habit.plus.yearly.direct","popularPackageId":"kompanion.habit.plus.3months.direct","default 'habit_streaks_config': '{"habitStreaksConfigId":"in-app-default","enabled":true}', 'iap_sheet_config': '{"iapSheetConfigId":"default","isEnabled":false}', 'insights_config': '{"insightsConfigId":"default","isCloseButtonVisible":true,"availableLanguages": ["kompanion.habit.plus.monthly.direct","kompanion.habit.plus.yearly.lto","kompanion.habit.plus.3months.direct"],"bestValuePackageId":"kompanion.habit.plus.yearly.direct","popularPackageId":"kompanion.habit.plus.3months.direct","default '{"limitedTimeOfferConfigId":"lto_default","enabled":true,"highPricePackageId":"kompanion.habit.plus.yearly.direct","lowPricePackageId":"kompanion.habit.plus.yearly.lto.y","priceDisplayFormat":"original","countdownSeconds":300,"introAnimat 1)","backgroundImage":"https://dsgmc6umf6chc.cloudfront.net/LTO/habit/LTO-NEWYEAR-BadgeBg.jpg","backgroundColor":"rgba(248, 253, 255, 1)"}}}}', 'local_notification_config': '{"localNotificationConfigId":"default","enabled":true,"android13N 'localizations_config': '{"ar":{"banner_button_title":"نضم الان","onboarding_rate_us_screen_button_text":"أعطنا ٥ نجوم","rateUsModal_rateUsButton_text":"أعطنا ٥ نجوم","cycleSync_popUp_membershipForAYear_text":"عضوية لمدة 3 أشهر","cycleSync_ stars","cycleSync_popUp_membershipForAYear_text":"membership for 3 months","cycleSync_popUp_startFreeYear_button_text":"Start free membership"},"es":{"banner_button_title":"Únete ahora","onboarding_rate_us_screen_button_text":"Re mois","cycleSync_popUp_startFreeYear_button_text":"Commencer l\'adhésion gratuite"},"he":{"banner_button_title":"הצטרף עכשיו","onboarding_rate_us_screen_button_text":"נשמח לקבל 5 כוכבים","rateUsModal_rateUsButton_text":"קבל 5 כוכבים □","rateUsModal_rateUsButton_text":"5□□□□□□□□□□□","cycleSync_popUp_membershipForAYear_text":"3□□□□","cycleSync_popUp_startFreeYear_button_text":"□□□□□□□□□□□□","paywallScreen_bottomSheet_unlockHabits_text":"24□□□7□□□□□□"} членство","cycleSync_popUp_startFreeYear_button_text":"Начать бесплатное членство"},"tr":{"banner_button_title":"Şimdi katıl","onboarding_rate_us_screen_button_text":"Bize 5 yıldız ver","rateUsModal_rateUsButton_text":"Bize 5 yıldız ver", ["TODAY","DISCOVER"],"howManyTextWillDisplayEachDay":3,"themeImageData":[{"id":"DreamyImage","tinyImage":"https://dsgmc6umf6chc.cloudfront.net/habit/motivation-banner-images/Free/Dreamy.jpg","image":"https://dsgmc6umf6chc.clo images/Free/Ice+blur.jpg","isLockedForFreeUser":false},{"id":"AffirmationsImage","tinyImage":"https://dsgmc6umf6chc.cloudfront.net/habit/motivation-banner-images/Free/Affirmations.jpg","image":"https://dsgmc6umf6chc.cloudfront.net/habi images/Locked/Leopheart+blur.jpg","isLockedForFreeUser":true},{"id":"NotepadImage","tinyImage":"https://dsgmc6umf6chc.cloudfront.net/habit/motivation-banner-images/Free/Notepad.jpg","image":"https://dsgmc6umf6chc.cloudfront.net/ha images/Locked/Pink+Panther+blur.jpg","isLockedForFreeUser":true},{"id":"SilkImage","tinyImage":"https://dsgmc6umf6chc.cloudfront.net/habit/motivation-banner-images/Locked/Silk.jpg","image":"https://dsgmc6umf6chc.cloudfront.net/habit/ images/Free/Crescent+blur.jpg","isLockedForFreeUser":false},{"id":"LoveFreeImage","tinyImage":"https://dsgmc6umf6chc.cloudfront.net/habit/motivation-banner-images/Free/Love.jpg","image":"https://dsgmc6umf6chc.cloudfront.net/habit/mo {"id":"Disco1Image","tinyImage":"https://dsgmc6umf6chc.cloudfront.net/habit/motivation-banner-images/Locked/Disco-1.jpg","image":"https://dsgmc6umf6chc.cloudfront.net/habit/motivation-banner-images/Locked/Disco+Background-1.jpg"," {"id":"CityImage","tinyImage":"https://dsgmc6umf6chc.cloudfront.net/habit/motivation-banner-images/Free/City.jpg","image":"https://dsgmc6umf6chc.cloudfront.net/habit/motivation-banner-images/Free/City+Background.jpg","blurImage":"htt {"id":"ConfidanceImage","tinyImage":"https://dsgmc6umf6chc.cloudfront.net/habit/motivation-banner-images/Free/Confidance.jpg","image":"https://dsgmc6umf6chc.cloudfront.net/habit/motivation-banner-images/Free/Confidance+Backgroun {"id":"HorizonImage","tinyImage":"https://dsgmc6umf6chc.cloudfront.net/habit/motivation-banner-images/Locked/Horizon.jpg","image":"https://dsgmc6umf6chc.cloudfront.net/habit/motivation-banner-images/Locked/Horizon+Background.jpg {"id":"SparklingImage","tinyImage":"https://dsgmc6umf6chc.cloudfront.net/habit/motivation-banner-images/Free/Sparkling.jpg","image":"https://dsgmc6umf6chc.cloudfront.net/habit/motivation-banner-images/Free/Sparkling+Background.jpg", {"id":"PixelImage","tinyImage":"https://dsgmc6umf6chc.cloudfront.net/habit/motivation-banner-images/Locked/Pixel.jpg","image":"https://dsgmc6umf6chc.cloudfront.net/habit/motivation-banner-images/Locked/Pixel+Background.jpg","blurIma [{"id":"JUSTIFICATION_SECRET"},{"id":"JUSTIFICATION_EFFORTS"},{"id":"JUSTIFICATION_SCIENCE"},{"id":"VALUE_TODAY"},{"id":"VALUE_DISCOVER"},{"id":"VALUE_JOURNAL"},{"id":"CHAR_INTRO"},{"id":"AGE"},{"id":"GENDER"},{"id":"SLEEP_DURATION {"id":"PERSONAL_SUMMARY"},{"id":"BETTER_YOU_JUSTIFICATION"},{"id":"STATEMENT_ROUTINES"},{"id":"STATEMENT_PRODUCTIVE"},{"id":"STATEMENT_DEDICATION"},{"id":"FIRST_HABIT_INTRODUCTION"},{"id":"FIRST_HABIT_START"},{"id":"FIRST carousel/en/2.png","tr":"https://dsgmc6umf6chc.cloudfront.net/habit/paywall-carousel/tr/2.png","es":"https://dsgmc6umf6chc.cloudfront.net/habit/paywall-carousel/es/2.png","fr":"https://dsgmc6umf6chc.cloudfront.net/habit/paywall-carousel/ carousel/it/2.png","ar":"https://dsgmc6umf6chc.cloudfront.net/habit/paywall-carousel/ar/2.png"}},{"titleKey":"paywallScreen_bestRoutine_title_text","descriptionKey":"paywallScreen_bestRoutine_description_text","images":{"en":"https://dsgmc6 carousel/he/4.png","ja":"https://dsgmc6umf6chc.cloudfront.net/habit/paywall-carousel/ja/4.png","de":"https://dsgmc6umf6chc.cloudfront.net/habit/paywall-carousel/de/4.png","id":"https://dsgmc6umf6chc.cloudfront.net/habit/paywall-carouse carousel/es/1.png","fr":"https://dsgmc6umf6chc.cloudfront.net/habit/paywall-carousel/fr/1.png","pt":"https://dsgmc6umf6chc.cloudfront.net/habit/paywall-carousel/pt/1.png","ru":"https://dsgmc6umf6chc.cloudfront.net/habit/paywall-carousel/ {"titleKey":"paywallScreen_planSmart_title_text","descriptionKey":"paywallScreen_planSmart_description_text","images":{"en":"https://dsgmc6umf6chc.cloudfront.net/habit/paywall-carousel/en/3_1.png","tr":"https://dsgmc6umf6chc.cloudfront.n carousel/ja/3_1.png","de":"https://dsgmc6umf6chc.cloudfront.net/habit/paywall-carousel/de/3_1.png","id":"https://dsgmc6umf6chc.cloudfront.net/habit/paywall-carousel/id/3_1.png","it":"https://dsgmc6umf6chc.cloudfront.net/habit/paywall-ca

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	5/44	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, android.permission.ACCESS_NOTIFICATION_POLICY

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:** 151.101.192.84 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
achievementapi.kompanionapp.com	ok	**IP:** 104.21.112.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
kompanion.zendesk.com	ok	**IP:** 216.198.54.6 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
appleid.apple.com	ok	**IP:** 17.23.96.16 **Country:** United States of America **Region:** California **City:** Cupertino **Latitude:** 37.316605 **Longitude:** -122.046486 **View:** Google Map
sinapps.s	ok	No Geolocation information available.
www.zendesk.com	ok	**IP:** 104.18.34.51 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.eu.amplitude.com	ok	**IP:** 3.127.160.87 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
plus.google.com	ok	**IP:** 172.217.12.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 142.250.188.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.
github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
twitter.com	ok	**IP:** 162.159.140.229 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sconversions.s	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.
insights.kompanionapp.com	ok	**IP:** 104.21.16.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sgcdsdk.s	ok	No Geolocation information available.
sattr.s	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:** 104.21.27.136 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
ssdk-services.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
sars.s	ok	No Geolocation information available.
identity.kompanionapp.com	ok	**IP:** 104.21.16.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sregister.s	ok	No Geolocation information available.
scdn-ssettings.s	ok	No Geolocation information available.
scdn-stestsettings.s	ok	No Geolocation information available.
dearme-quiz.kompanionapp.com	ok	**IP:** 18.238.96.104 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api2.amplitude.com	ok	**IP:** 44.231.47.42 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
aps-webhandler.appsflyer.com	ok	**IP:** 18.238.109.70 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
appleid.a	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
svalidate-and-log.s	ok	No Geolocation information available.
sapp.s	ok	No Geolocation information available.
sviap.s	ok	No Geolocation information available.
tools.android.com	ok	**IP:** 142.250.189.19 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
regionconfig.eu.amplitude.com	ok	**IP:** 18.238.96.4 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
regionconfig.amplitude.com	ok	**IP:** 18.155.173.77 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
svalidate.s	ok	No Geolocation information available.
habitapi.kompanionapp.com	ok	**IP:** 104.21.80.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Amplitude	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/125
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"AMPLITUDE_API_KEY" : "6dba9686d141d9bbfb7e99db0e8bab4e"
"APPSFLYER_DEV_KEY" : "saSk33o7FZjSjeoZGHz5i7"
"GOOGLE_OAUTH_WEB_CLIENT_ID" : "101330198578-9uqfmc591vpavn8eijama8ttg3885res.apps.googleusercontent.com"
"KOMPANION_ACHIEVEMENT_API_HOST" : "https://achievementapi.kompanionapp.com"

POSSIBLE SECRETS
"KOMPANION_APP_API_HOST" : "https://habitapi.kompanionapp.com"
"KOMPANION_IDENTITY_API_HOST" : "https://identity.kompanionapp.com"
"KOMPANION_IDENTITY_KEYCHAIN_CREDENTIALS_KEY" : "KmpCredentials"
"KOMPANION_INSIGHT_API_HOST" : "https://insights.kompanionapp.com"
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"facebook_client_token" : "5de1e472b441aed86f78782fd88b24ef"
"google_api_key" : "AIzaSyDIZuCTlD7jNWFdPC6enPwsaF-L6GGSyyY"
"google_crash_reporting_api_key" : "AIzaSyDIZuCTlD7jNWFdPC6enPwsaF-L6GGSyyY"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
nb24gUm9vdCBDQSAxMB4XDTE1MDUyNjAwMDAwMFoXDTM4MDExNzAwMDAwMFowOTEL
nVOujw5H5SNz/0egwLX0tdHA114gk957EWW67c4cX8jJGKLhD+rcdqsq08p8kDi1L
nb3QgQ0EgMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALJ4gHHKeNXj
nU5PMCCjjmCXPI6T53iHTfIUJrU6adTrCC2qJeHZERxhlbI1Bjjt/msv0tadQ1wUs
cc5cf9c2705fe1910097692dc1e735785c1d96cec3078b9e
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
n5MsI+yMRQ+hDKXJioaldXgjUkK642M4UwtBV8ob2xJNDd2ZhwLnoQdeXeGADbkpy
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa
MIIDQTCCAimgAwIBAgITBmyfz5m/jAo54vB4ikPmljZbyjANBgkqhkiG9w0BAQsF
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
e4b001df9a082298dd090bb7455c45d92fbd5dda
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
ae2044fb577e65ee8bb576ca48a2f06e

POSSIBLE SECRETS
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
c56fb7d591ba6704df047fd98f535372fea00211
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
nIFAGbHrQgLKm+a/sRxmPUDgH3KKHOVj4utWp+UhnMJbulHheb4mjUcAwhmahRWa6
nca9HgFB0fW7Y14h29Jlo91ghYPl0hAEvrAIthtOgQ3pOsqTQNroBvo3bSMgHFzZM
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
9b8f518b086098de3d77736f9458a3d2f6f95a37
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
1ebcdd8dad6e5edcf276
no/ufQJVtMVT8QtPHRh8jrdkPSHCa2XV4cdFyQzR1bldZwgJcJmApzyMZFo6IQ6XU
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
0136024004378801593602050 5
115792089210356248762697446949407573530086143415290314195533631308867097853951
nMAkGA1UEBhMCVVMxDzANBgNVBAoTBkFtYXpvbjEZMBcGA1UEAxMQQW1hem9uIFJv
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
cc2751449a350f668590264ed76692694a80308a
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
5181942b9ebc31ce68dacb56c16fd79f
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
1ddaa4b892e61b0f7010597ddc582ed3

POSSIBLE SECRETS
nN+gDS63pYaACbvXy8MWy7Vu33PqUXHeeE6V/Uq2V8viTO96LXFvKWlJbYK8U90vv
nAYYwHQYDVR0OBBYEFIQYzIU07LwMlJQuCFmcx7IQTgoIMA0GCSqGSIb3DQEBCwUA
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
24b2477514809255df232947ce7928c4
115792089210356248762697446949407573529996955224135760342422259061068512044369
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
nADA5MQswCQYDVQQGEwJVUzEPMA0GA1UEChMGQW1hem9uMRkwFwYDVQQDExBBbWF6
6dba9686d141d9bbfb7e99db0e8bab4e

PLAYSTORE INFORMATION

Title: Dear Me: Daily Routine Tracker

Score: 4.6309524 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.kompanion.habit.android

Developer Details: Fitself, Fitself, None, https://fitself.com/, hi@appdearme.com,

Release Date: Aug 15, 2024 **Privacy Policy:** Privacy link

Description:

Introducing Dear Me: Daily Routine Tracker, designed to track your daily routine, habits, rituals and tasks to organize your days efficiently with useful to do lists and fun tips. Dear Me: Daily Routine Tracker isn't just a digital journal; it's your comprehensive organizer, a life-enriching checklist, and a schedule planner finely tuned to your unique needs, offering useful support. More importantly, it allows you to become a better version of yourself and elevate your life to extraordinary heights with its self care rituals. As a result, self-love sprouts in no time. Benefits of Dear Me: Daily Routine Tracker: •Start your mornings with a reminder towards rituals that set a foundation for a day full of achievements and self care. •Get the perfect routine ideas, involving essentials like meditation, exercise, self care, reading, cleaning, and even pet care. •Tailor your tasks, lists, and schedules to resonate with your ambitions, transforming each day into a stepping stone towards the person you desire to become. •Track your progress with useful to do lists. Let Dear Me: Daily Routine Tracker serve as your motivational organizer that boosts your self improvement, ensuring your to-do list doesn't just stay managed but inspires action. Whether it's completing your daily tasks, keeping tabs on your agenda, or embedding self care practices into your schedule, "Dear Me" guarantees that no detail is overlooked. For those navigating the complexities of ADHD, “Dear Me: Daily Routine Tracker” proves to be a sanctuary. It simplifies tasks into manageable segments, punctuated with reminders, helping in sustaining focus and organization. This planner respects your rhythm, molds to your lifestyle, and provides the subtle encouragement needed without overwhelming you. Get “Dear Me: Daily Routine Tracker” and unlock the transformative power of tracking, all within arm's reach. Nurture your habits and rituals that sculpt the finest version of you.

SCAN LOGS

Timestamp	Event	Error
2025-08-30 22:37:57	Generating Hashes	OK
2025-08-30 22:37:58	Extracting APK	OK
2025-08-30 22:37:58	Unzipping	OK

2025-08-30 22:37:58	Parsing APK with androguard	OK
2025-08-30 22:37:59	Extracting APK features using aapt/aapt2	OK
2025-08-30 22:37:59	Getting Hardcoded Certificates/Keystores	OK
2025-08-30 22:38:01	Parsing AndroidManifest.xml	OK
2025-08-30 22:38:01	Extracting Manifest Data	OK
2025-08-30 22:38:01	Manifest Analysis Started	OK
2025-08-30 22:38:01	Performing Static Analysis on: Dear Me (com.kompanion.habit.android)	OK
2025-08-30 22:38:03	Fetching Details from Play Store: com.kompanion.habit.android	OK
2025-08-30 22:38:06	Checking for Malware Permissions	OK
2025-08-30 22:38:06	Fetching icon path	OK
2025-08-30 22:38:06	Library Binary Analysis Started	OK
2025-08-30 22:38:06	Reading Code Signing Certificate	OK
2025-08-30 22:38:07	Running APKiD 2.1.5	OK
2025-08-30 22:38:15	Detecting Trackers	OK
2025-08-30 22:38:20	Decompiling APK to Java with JADX	OK
2025-08-30 22:44:39	Decompiling with JADX failed, attempting on all DEX files	OK
2025-08-30 22:44:39	Decompiling classes2.dex with JADX	OK

2025-08-30 22:44:50	Decompiling classes4.dex with JADX	OK
2025-08-30 22:45:02	Decompiling classes.dex with JADX	OK
2025-08-30 22:45:13	Decompiling classes3.dex with JADX	OK
2025-08-30 22:45:24	Decompiling classes2.dex with JADX	OK
2025-08-30 22:45:34	Decompiling classes4.dex with JADX	OK
2025-08-30 22:45:45	Decompiling classes.dex with JADX	OK
2025-08-30 22:45:57	Decompiling classes3.dex with JADX	OK
2025-08-30 22:46:07	Converting DEX to Smali	OK
2025-08-30 22:46:07	Code Analysis Started on - java_source	OK
2025-08-30 22:46:11	Android SBOM Analysis Completed	OK
2025-08-30 22:46:22	Android SAST Completed	OK
2025-08-30 22:46:22	Android API Analysis Started	OK
2025-08-30 22:46:31	Android API Analysis Completed	OK
2025-08-30 22:46:31	Android Permission Mapping Started	OK
2025-08-30 22:46:39	Android Permission Mapping Completed	OK
2025-08-30 22:46:39	Android Behaviour Analysis Started	OK
2025-08-30 22:46:49	Android Behaviour Analysis Completed	OK

2025-08-30 22:46:49	Extracting Emails and URLs from Source Code	OK
2025-08-30 22:46:53	Email and URL Extraction Completed	OK
2025-08-30 22:46:53	Extracting String data from APK	OK
2025-08-30 22:46:53	Extracting String data from Code	OK
2025-08-30 22:46:53	Extracting String values and entropies from Code	OK
2025-08-30 22:47:01	Performing Malware check on extracted domains	OK
2025-08-30 23:15:10	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.