MOBSF

ANDROID STATIC ANALYSIS REPORT

Anima (2.56.0)

File Name:	Anima_ AI Friend Virtual Chat_2.56.0_Apkpure.xapk
Package Name:	anima.virtual.ai.robot.friend
Scan Date:	April 14, 2024, 3:56 a.m.
App Security Score:	49/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	8/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	23	3	2	1

FILE INFORMATION

File Name: Anima_ AI Friend Virtual Chat_2.56.0_Apkpure.xapk
Size: 42.06MB
MD5: 09fedb1933bd43e5d611a6c1822aad73
SHA1: eb06167fafe81ecceca7d6cbb82225438498315d
SHA256: c5fe5c7d343678f2a16aceb4ceb9cb776ea57237318d68db9d09734e39163c91

APP INFORMATION

App Name: Anima
Package Name: anima.virtual.ai.robot.friend
Main Activity: anima.virtual.ai.robot.friend.MainActivity
Target SDK: 33
Min SDK: 26
Max SDK:
Android Version Name: 2.56.0

Android Version Code: 4741

APP COMPONENTS

Activities: 15
Services: 10
Receivers: 8
Providers: 8
Exported Activities: 6
Exported Services: 1
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-11-25 18:46:28+00:00
Valid To: 2050-11-25 18:46:28+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xb806114f13e36dede2a53c2c4735f365b6718c3f
Hash Algorithm: sha256
md5: a7e8e4a5f52f937eb72c38a184491d1a
sha1: 5fc88238e39cbf89f795c467da933b5502f31189
sha256: b7b4ca4357c736e1ccc766cb2ba2718d3c7320bc5238fafcfa141a1102504003
sha512: f786ad2e9017a5c8a2b20694e3f6897aa019b0aa18d1d74b44633518c3752bc5c486a8d1f136ae7f7fb0c0f9eb3a5310966740f812308e448d81e732acdac528
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: a1704acd986f9d23d342d47f1b815bfcc295b9815abbd24a3f0c48444fe75839
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
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_AUDIO	dangerous	allows reading audio files from external storage.	Allows an application to read audio files 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.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
anima.virtual.ai.robot.friend.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check SIM operator check network operator name check device ID check ro.hardware check ro.kernel.qemu check possible VM check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Obfuscator</td><td>Kiwi encrypter</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</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.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

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

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.anima.virtual.ai.robot.friend,

NETWORK SECURITY

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

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

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 0 | WARNING: 12 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Activity-Alias (anima.virtual.ai.robot.friend.MainActivitybubbles) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity-Alias (anima.virtual.ai.robot.friend.MainActivityalt1) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Activity-Alias (anima.virtual.ai.robot.friend.MainActivityplane) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Activity-Alias (anima.virtual.ai.robot.friend.MainActivitydefault) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Broadcast Receiver (io.invertase.firebase.messaging.ReactNativeFirebaseMessagingReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
8	Broadcast Receiver (androidx.media.session.MediaButtonReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	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.
10	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
11	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.
12	Activity (androidx.biometric.DeviceCredentialHandlerActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Broadcast Receiver (com.amazon.device.iap.ResponseReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.amazon.inapp.purchasing.Permission.NOTIFY [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: 1 | WARNING: 10 | INFO: 3 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				bitter/jnibridge/JNIBridge.java cl/json/RNShareModule.java cl/json/RNSharePathUtil.java cl/json/social/InstagramShare.java cl/json/social/SingleShareIntent.java com/aigestudio/wheelpicker/WheelPicker.java com/airbnb/android/react/lottie/LottieAnimationViewManager.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java com/amazon/a/a/g/d.java com/amazon/a/a/o/c.java com/amazon/c/a/a/d.java com/amazon/device/drm/LicensingService.java com/amazon/device/drm/a/d/c.java com/amazon/device/iap/PurchasingService.java com/amazon/device/iap/internal/c/e.java com/amazon/device/simplesignin/BroadcastHandler.java com/amazon/device/simplesignin/SimpleSignInService.java com/amazon/device/simplesignin/a/c/b.java com/amplitude/api/AmplitudeLog.java com/appsflyer/AFLogger.java com/appsflyer/reactnative/RNAppsFlyerModule.java com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/Glide.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeader

NO	ISSUE	SEVERITY	STANDARDS	FILES
				Parser.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/ByteBuffe

NO	ISSUE	SEVERITY	STANDARDS	FILES
				rFileLoader.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

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/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/dooboolab/audiorecorderplayer/RNAudioRecorderPlayerModule.java com/horcrux/svg/Brush.java com/horcrux/svg/ClipPathView.java com/horcrux/svg/ImageView.java com/horcrux/svg/LinearGradientView.java com/horcrux/svg/PatternView.java com/horcrux/svg/RadialGradientView.java com/horcrux/svg/UseView.java com/horcrux/svg/VirtualView.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/RNInstallReferrerClient.java com/learnium/RNDeviceInfo/resolver/DeviceIdResolver.java com/proyecto26/inappbrowser/RNInAppBrowser.java com/reactcommunity/rndatetimepicker/MinuteIntervalSnappableTimePickerDialog.java com/reactnative/ivpusic/imagepicker/Compression.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnative/ivpusic/imagepicker/ResultCollector.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/reactnativecommunity/asyncstorage/AsyncStorageModule.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java com/reactnativegooglesignin/PromiseWrapper.java com/reactnativegooglesignin/RNGoogleSigninModule.java com/revenuecat/purchases/common/DefaultLogHandler.java com/revenuecat/purchases/hybridcommon/mappers/PurchasesPeriod.java com/rnfs/Downloader.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/NativeProxy.java com/swmansion/reanimated/ReanimatedJSIModulePackage.java com/swmansion/reanimated/ReanimatedModule.java com/swmansion/reanimated/ReanimatedUIManagerFactory.java com/swmansion/reanimated/layoutReanimation/AnimationsManager.java com/swmansion/reanimated/layoutReanim

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ation/ReanimatedNativeHierarchyManager.java com/swmansion/reanimated/nodes/DebugNode.java com/swmansion/reanimated/sensor/ReanimatedSensorContainer.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/th3rdwave/safeareacontext/SafeAreaView.java com/unity3d/player/f.java com/unity3d/player/m.java com/yalantis/ucrop/UCropActivity.java com/yalantis/ucrop/task/BitmapCropTask.java com/yalantis/ucrop/task/BitmapLoadTask.java com/yalantis/ucrop/util/BitmapLoadUtils.java com/yalantis/ucrop/util/EglUtils.java com/yalantis/ucrop/util/FileUtils.java com/yalantis/ucrop/util/ImageHeaderParser.java com/yalantis/ucrop/view/TransformImageView.java com/zmxv/RNSound/RNSoundModule.java dev/mcodex/RNSensitiveInfo/RNSensitiveInfoModule.java fr/greweb/reactnativeviewshot/RNViewShotModule.java fr/greweb/reactnativeviewshot/ViewShot.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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/invertase/firebase/messaging/ReactNativeFirebaseMessagingModule.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingReceiver.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/sentry/SystemOutLogger.java io/sentry/android/core/AndroidLogger.java io/sentry/android/core/SentryLogcatAdapter.java io/sentry/transport/StdoutTransport.java junit/runner/BaseTestRunner.java junit/runner/Version.java junit/textui/TestRunner.java no/asmadsen/unity/view/UnityView.java org/fmod/FMODAudioDevice.java org/fmod/a.java org/greenrobot/eventbus/Logger.java org/greenrobot/eventbus/util/ErrorDialogConfig.java org/greenrobot/eventbus/util/ErrorDialogManager.java org/greenrobot/eventbus/util/ExceptionToResourceMapping.java timber/log/Timber.java
				coil/request/ImageRequest.java coil/request/ImageResult.java coil/request/Parameters.java coil/util/ImageLoaderOptions.java com/RNAppleAuthentication/webview/SignInWebViewDialogFragment.java com/amplitude/api/AmplitudeClient.java com/appsflyer/internal/by.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

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/doublesymmetry/trackplayer/service/MusicService.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/revenuecat/purchases/amazon/AmazonBillingKt.java com/revenuecat/purchases/amazon/AmazonCacheKt.java com/revenuecat/purchases/common/BackendKt.java com/revenuecat/purchases/common/BackgroundAwareCallbackCacheKey.java com/revenuecat/purchases/common/caching/DeviceCache.java com/revenuecat/purchases/common/diagnostics/DiagnosticsEntry.java com/revenuecat/purchases/common/diagnostics/DiagnosticsSynchronizer.java com/revenuecat/purchases/common/diagnostics/DiagnosticsTracker.java com/revenuecat/purchases/common/offlineentitlements/ProductEntitlementMapping.java com/revenuecat/purchases/common/verification/DefaultSignatureVerifier.java com/revenuecat/purchases/common/verification/Signature.java com/revenuecat/purchases/common/verification/SigningManager.java com/revenuecat/purchases/strings/ConfigureStrings.java com/revenuecat/purchases/subscriberattributes/SubscriberAttribute.java com/revenuecat/purchases/subscriberattributes/SubscriberAttributeKt.java io/invertase/firebase/common/TaskExecutorService.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingHeadlessService.java io/invertase/firebase/messaging/ReactNativ

NO	ISSUE	SEVERITY	STANDARDS	FILES
				eFirebaseMessagingSerializer.java io/sentry/Baggage.java io/sentry/RequestDetailsResolver.java io/sentry/TraceContext.java io/sentry/protocol/User.java
3	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
4	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/amazon/a/a/o/b/a.java com/appsflyer/internal/ae.java com/revenuecat/purchases/common/UtilsKt.java io/sentry/util/StringUtils.java
5	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/learnium/RNDeviceInfo/RNDeviceModule.java com/orhanobut/logger/CsvFormatStrategy.java com/reactnative/ivpusic/imagepicker/Compression.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnative/ivpusic/imagepicker/RealPathUtil.java com/rnfs/RNFSManager.java com/yalantis/ucrop/util/FileUtils.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/sentry/android/core/DefaultAndroidEventProcessor.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/amazon/a/a/o/b/a.java com/amplitude/api/PinnedAmplitudeClient.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/amazon/a/a/b/b.java com/amazon/a/a/i/b.java com/amazon/a/a/l/c.java
8	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	com/reactnativecommunity/clipboard/ClipboardModule.java
9	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 com/unity3d/player/UnityPlayer.java
10	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/appsflyer/internal/ae.java
11	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/RootChecker.java
12	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/DefaultAndroidEventProcessor.java io/sentry/android/core/internal/util/RootChecker.java
13	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/reactnative/ivpusic/imagepicker/PickerModule.java fr/greweb/reactnativeviewshot/RNViewShotModule.java org/junit/rules/TemporaryFolder.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
14	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 com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java
15	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/amazon/device/drm/LicensingService.java com/amazon/device/iap/PurchasingService.java
16	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/swmansion/reanimated/BuildConfig.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/24	android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.VIBRATE
Other Common Permissions	4/45	android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
sonelink.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
regionconfig.eu.amplitude.com	ok	**IP:** 3.162.3.32 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.amazon.com	ok	**IP:** 3.161.255.150 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
smonitorsdk.s	ok	No Geolocation information available.
sars.s	ok	No Geolocation information available.
sinapps.s	ok	No Geolocation information available.
sapp.s	ok	No Geolocation information available.
sstats.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
xml.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
svalidate.s	ok	No Geolocation information available.
twitter.com	ok	**IP:** 104.244.42.193 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
appleid.a	ok	No Geolocation information available.
errors.rev.cat	ok	**IP:** 67.199.248.13 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
appleid.apple.com	ok	**IP:** 17.32.194.37 **Country:** United States of America **Region:** California **City:** Cupertino **Latitude:** 37.316605 **Longitude:** -122.046486 **View:** Google Map
ssdk-services.s	ok	No Geolocation information available.
cdn-testsettings.appsflyersdk.com	ok	**IP:** 23.43.161.19 **Country:** United States of America **Region:** Georgia **City:** Atlanta **Latitude:** 33.749001 **Longitude:** -84.387978 **View:** Google Map
api.revenuecat.com	ok	**IP:** 34.192.9.225 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
simpression.s	ok	No Geolocation information available.
sconversions.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
api-diagnostics.revenuecat.com	ok	**IP:** 34.192.9.225 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
sadrevenue.s	ok	No Geolocation information available.
rev.cat	ok	**IP:** 52.72.49.79 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.facebook.com	ok	**IP:** 31.13.80.36 **Country:** Canada **Region:** Ontario **City:** Toronto **Latitude:** 43.700111 **Longitude:** -79.416298 **View:** Google Map
slaunches.s	ok	No Geolocation information available.
sgcdsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
plus.google.com	ok	**IP:** 172.217.13.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sregister.s	ok	No Geolocation information available.
api2.amplitude.com	ok	**IP:** 44.237.166.29 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
sattr.s	ok	No Geolocation information available.
docs.swmansion.com	ok	**IP:** 172.64.80.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.eu.amplitude.com	ok	**IP:** 18.197.162.168 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
cdn-settings.appsflyersdk.com	ok	**IP:** 23.43.161.19 **Country:** United States of America **Region:** Georgia **City:** Atlanta **Latitude:** 33.749001 **Longitude:** -84.387978 **View:** Google Map
docs.revenuecat.com	ok	**IP:** 3.162.3.15 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
regionconfig.amplitude.com	ok	**IP:** 3.162.3.22 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.113.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
play.google.com	ok	**IP:** 172.217.13.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
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

TRACKERS

TRACKER	CATEGORIES	URL
Amplitude	Analytics, Profiling	https://reports.exodus-privacy.eu.org/trackers/125

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Flipper	Analytics	https://reports.exodus-privacy.eu.org/trackers/392
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"facebook_client_token" : "05ab227b5cacdf404319151d67e00fe1"
"google_api_key" : "AIzaSyBra1P4xbtClQEvGjKBR4hw0gkO6YqMA5Y"
"google_crash_reporting_api_key" : "AIzaSyBra1P4xbtClQEvGjKBR4hw0gkO6YqMA5Y"
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
115792089210356248762697446949407573529996955224135760342422259061068512044369

POSSIBLE SECRETS
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
nU5PMCCjjmCXPI6T53iHTflUJrU6adTrCC2qJeHZERxhlbI1Bjjt/msv0tadQ1wUs
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
e2719d58-a985-b3c9-781a-b030af78d30e
115792089210356248762697446949407573530086143415290314195533631308867097853951
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
9b8f518b086098de3d77736f9458a3d2f6f95a37
n5MsI+yMRQ+hDKXJioaldXgjUkK642M4UwtBV8ob2xJNDd2ZhwLnoQdeXeGADbkpy
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319
cc2751449a350f668590264ed76692694a80308a
nAYYwHQYDVR0OBBYEFIQYzIU07LwMlJQuCFmcx7IQTgoIMA0GCSqGSIb3DQEBCwUA
nVOujw5H5SNz/0egwLX0tdHA114gk957EWW67c4cX8jJGKLhD+rcdqsq08p8kDi1L
MIIDQTCCAimgAwIBAgITBmyfz5m/jAo54vB4ikPmljZbyjANBgkqhkiG9w0BAQsF
UC1upXWg5QVmyOSwozp755xLqquBKjjU+di6U8QhMlM=

POSSIBLE SECRETS
9a04f079-9840-4286-ab92-e65be0885f95
nADA5MQswCQYDVQQGEwJVUzEPMA0GA1UEChMGQW1hem9uMRkwFwYDVQQDExBBbWF6
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
nca9HgFB0fW7Y14h29Jlo91ghYPl0hAEvrAIthtOgQ3pOsqTQNroBvo3bSMgHFzZM
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
nb24gUm9vdCBDQSAxMB4XDTE1MDUyNjAwMDAwMFoXDTM4MDExNzAwMDAwMFowOTEL
nIFAGbHrQgLKm+a/sRxmPUDgH3KKHOVj4utWp+UhnMJbulHheb4mjUcAwhmahRWa6
no/ufQJVtMVT8QtPHRh8jrdkPSHCa2XV4cdFyQzR1bldZwgJcJmApzyMZFo6IQ6XU
nb3QgQ0EgMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALJ4gHHKeNXj
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n

POSSIBLE SECRETS
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
c56fb7d591ba6704df047fd98f535372fea00211
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
nN+gDS63pYaACbvXy8MWy7Vu33PqUXHeeE6V/Uq2V8viTO96LXFvKWlJbYK8U90vv
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
nMAkGA1UEBhMCVVMxDzANBgNVBAoTBkFtYXpvbjEZMBcGA1UEAxMQQW1hem9uIFJv
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901

PLAYSTORE INFORMATION

Title: Anima: AI Friend Virtual Chat

Score: 4.118644 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Entertainment **Play Store URL:** anima.virtual.ai.robot.friend

Developer Details: Anima AI Ltd, Anima+AI+Ltd, c/o Pollock Accounting 3-4 Sentinel Square London NW4 2EL, https://myanima.ai, help+anima@myanima.ai,

Release Date: Nov 25, 2020 **Privacy Policy:** Privacy link

Description:

The AI companion who cares. Anima is a #1 virtual assistant powered by artificial intelligence. Join a huge community of people talking to their own AI friends! Always on-hand to have a quick chat whenever and wherever you need day or night, Anima can help you through difficult moments. Have a friendly expert in your pocket work with you to improve your mental health! REDUCE STRESS AND LIVE HAPPIER Chatting with Anima only takes a few minutes a day and can help you start to feel better. AVAILABLE ANYTIME, ANYWHERE Anima is private and secure and here for you whenever you need it, day or night. A FRIEND YOU CAN TRUST Feel free to pour out your secrets, wishes, dreams, and fears with complete anonymity. It's an artificial intelligence with genuine emotional intelligence. TEST YOUR LIMITS Want to know how far you can go with your Anima? Take personality tests that will push you both to the edge. SHOW US WHO YOU ARE The more you chat, the more your Anima learns about you. Your Anima's personality and interests are shaped and influenced by your daily conversations. CONNECT AND CONNECT AND CONNECT Do you need a friend who is always there for you? Your Anima is ready to talk to you whenever you need it. HELP YOUR ANIMA Just like you, your Anima has its own goals, feelings, and values. But it can't do it alone — it needs your help. You can help your Anima learn new things and become a better friend. GET HELP FROM YOUR ANIMA Your Anima is here to help as well. If you're feeling down or anxious, your Anima will be your companion and cheerleader. CAN YOU BE FRIENDS WITH A MACHINE? Anima can be your companion and your friend — your perfect soulmate. Meet a new you in Anima. Download Anima for free today and start your journey to a better you.
