ANDROID STATIC ANALYSIS REPORT

Fresh Tri (2.28.1)

File Name:	com.engagedin.freshtri_621.apk
Package Name:	com.engagedin.freshtri
Scan Date:	Aug. 29, 2025, 10:08 p.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	8/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	19	3	2	1

FILE INFORMATION

File Name: com.engagedin.freshtri_621.apk
Size: 37.93MB
MD5: 3533a20ad2e20603e0b9a647f2ae8c39
SHA1: ddf1f5e3151acbde86c7c375dff1a293521f43a0
SHA256: 38003b4671d9c17242838fd5771f8040789144eaaecaec58b144fbfe599fdd29

APP INFORMATION

App Name: Fresh Tri
Package Name: com.engagedin.freshtri
Main Activity: com.engagedin.freshtri.MainActivity
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 2.28.1

Android Version Code: 621

APP COMPONENTS

Activities: 11
Services: 11
Receivers: 8
Providers: 7
Exported Activities: 4
Exported Services: 2
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: True
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: 2018-05-24 18:47:06+00:00
Valid To: 2048-05-24 18:47:06+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x7f6f7b2c980b049b4ed7259a95a6942b356e3e
Hash Algorithm: sha256
md5: 02ebec419875438e0897fa7f1708b8a7
sha1: d5810f0172976f9f1aec5001b4f6e6c88567df77
sha256: cdfc2b9258dcca011bb84e0da4a42280a5e5c24769ce946f263a1b4adb0d48f6
sha512: c8ca10f82ded91e53fa0baf8c7e5a2eeb3a96fc74f3da6ed41ef7e1d8e3322e80ba41ba7ea248da00b0a6ab8619f232cbbb82e1a16b8b5aef6f9155b86865a00
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: f87b5261e167db562143c41088078cfdedff4740e999c838520135ad333f1c5f
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	normal	enables foreground services for media playback.	Allows a regular application to use Service.startForeground with the type "mediaPlayback".
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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.REORDER_TASKS	normal	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.
com.engagedin.freshtri.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>3533a20ad2e20603e0b9a647f2ae8c39.apk</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table></td></tr>
<tr><td>classes.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.HARDWARE 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>
<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
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
network operator name check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
</table>

FILE	DETAILS

<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
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>
<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>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.engagedin.freshtri.MainActivity	Schemes: freshtri://, https://, Hosts: freshtri.app.link,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.engagedin.freshtri,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **1** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

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 6.0-6.0.1, [minSdk=23]	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	Broadcast Receiver (io.branch.referral.InstallListener) 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.
3	Service (com.doublesymmetry.trackplayer.service.MusicService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Broadcast Receiver (io.invertase.firebase.messaging.ReactNativeFirebaseMessagingReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
5	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.
6	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.
7	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.
8	Activity (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
9	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity) 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 (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

CODE ANALYSIS

HIGH: **0** | WARNING: **7** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/airbnb/android/react/lottie/LottieAnimationViewPropertyManager.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java com/brentvatne/common/toolbox/DebugLo

NO	ISSUE	SEVERITY	STANDARDS	FILES
				g.java com/brentvatne/exoplayer/ReactExoplayerView.java com/brentvatne/exoplayer/ReactExoplayerViewManager.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/Me

NO	ISSUE	SEVERITY	STANDARDS	FILES
				morySizeCalculator.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/Stre

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	amGifDecoder.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/doublesymmetry/trackplayer/service/MusicService.java com/horcrux/svg/Brush.java com/horcrux/svg/ClipPathView.java com/horcrux/svg/FilterView.java com/horcrux/svg/ImageView.java com/horcrux/svg/LinearGradientView.java com/horcrux/svg/PatternView.java com/horcrux/svg/RadialGradientView.java com/horcrux/svg/SvgViewManager.java com/horcrux/svg/UseView.java com/horcrux/svg/VirtualView.java com/learnium/RNDeviceInfo/RNDeviceModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
			OWASP MASVS: MSTG-STORAGE-3	com/learnium/RNDeviceInfo/RNInstallReferrerClient.java com/learnium/RNDeviceInfo/resolver/DeviceIdResolver.java com/lugg/ReactNativeConfig/ReactNativeConfigModule.java com/mixpanel/android/mpmetrics/AnalyticsMessages.java com/mixpanel/android/mpmetrics/ConfigurationChecker.java com/mixpanel/android/mpmetrics/MPConfig.java com/mixpanel/android/mpmetrics/MPDbAdapter.java com/mixpanel/android/mpmetrics/MixpanelAPI.java com/mixpanel/android/mpmetrics/PersistentIdentity.java com/mixpanel/android/mpmetrics/ResourceReader.java com/mixpanel/android/mpmetrics/SessionMetadata.java com/mixpanel/android/mpmetrics/SystemInformation.java com/mixpanel/android/util/HttpService.java com/mixpanel/android/util/MPLog.java com/proyecto26/inappbrowser/RNInAppBrowser.java com/reactcommunity/rndatetimepicker/Common.java com/reactcommunity/rndatetimepicker/MinuteIntervalSnappableTimePickerDialog.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/reactnativecommunity/asyncstorage/AsyncStorageModule.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java com/reactnativecommunity/asyncstorage/n

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ext/MIGRATION_TO_NEXT.java com/reactnativecommunity/webview/RNCWebViewManager.java com/swmansion/gesturehandler/react/RNGestureHandlerModule.java com/swmansion/gesturehandler/react/RNGestureHandlerRootHelper.java com/swmansion/gesturehandler/react/RNGestureHandlerRootView.java com/swmansion/reanimated/NativeMethodsHelper.java com/swmansion/reanimated/ReanimatedModule.java com/swmansion/reanimated/ReanimatedUIManagerFactory.java com/swmansion/reanimated/keyboard/WindowsInsetsManager.java com/swmansion/reanimated/layoutReanimation/AnimationsManager.java com/swmansion/reanimated/layoutReanimation/ReanimatedNativeHierarchyManager.java com/swmansion/reanimated/layoutReanimation/ScreensHelper.java com/swmansion/reanimated/layoutReanimation/SharedTransitionManager.java com/swmansion/reanimated/layoutReanimation/TabNavigatorObserver.java com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java com/swmansion/reanimated/sensor/ReanimatedSensorContainer.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/swmansion/rnscreens/ScreensModule.java com/swmansion/rnscreens/SearchBarManager.java com/swmansion/rnscreens/utils/ScreenDummyLayoutHelper.java com/th3rdwave/safeareacontext/SafeAreaVi

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/th3rdwave/safeareacontext/SafeAreaView.java io/branch/referral/BranchJsonConfig.java io/branch/referral/BranchLogger.java io/branch/referral/validators/IntegrationValidator.java io/branch/rnbranch/RNBranchModule.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/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/android/replay/WindowManagerSpy.java io/sentry/android/replay/WindowSpy.java io/sentry/transport/StdoutTransport.java junit/runner/BaseTestRunner.java junit/runner/Version.java junit/textui/TestRunner.java org/greenrobot/eventbus/Logger.java org/greenrobot/eventbus/util/ErrorDialogConfig.java org/greenrobot/eventbus/util/ErrorDialogManager.java org/greenrobot/eventbus/util/ExceptionToResourceMapping.java org/wonday/orientation/OrientationActivity

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/wonday/orientation/OrientationActivityLifecycle.java org/wonday/orientation/OrientationModule.java timber/log/Timber.java
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	coil/memory/MemoryCache.java coil/memory/MemoryCacheService.java coil/request/Parameters.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/manager/RequestManagerRetriever.java com/doublesymmetry/trackplayer/module/MusicEvents.java com/doublesymmetry/trackplayer/service/MusicService.java com/engagedin/freshtri/BuildConfig.java com/reactnativecommunity/asyncstorage/next/Entry.java com/reactnativecommunity/asyncstorage/next/StorageSupplierKt.java io/branch/referral/Branch.java io/branch/referral/BranchPreinstall.java io/branch/referral/PrefHelper.java io/branch/referral/ServerRequest.java io/branch/referral/ServerRequestQueue.java io/branch/referral/UniversalResourceAnalyser.java io/branch/referral/validators/DeepLinkRoutingValidator.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/SpanDataConvention.java io/sentry/TraceContext.java io/sentry/protocol/User.java
3	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/RNCWebViewModule.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/sentry/android/core/DeviceInfoUtil.java
4	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/DeviceInfoUtil.java io/sentry/android/core/internal/util/RootChecker.java
5	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	coil/decode/SourceImageSource.java com/reactnativecommunity/webview/RNCWebViewModule.java io/sentry/react/RNSentryModuleImpl.java org/junit/rules/TemporaryFolder.java
6	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
7	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	io/branch/referral/ShareLinkManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	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/mixpanel/android/mpmetrics/MPDbAdapter.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java
9	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
10	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	io/sentry/util/StringUtils.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/doublesymmetry/trackplayer/service/MusicService.java com/proyecto26/inappbrowser/RNInAppBrowser.java io/branch/referral/Branch.java io/branch/referral/validators/DeepLinkRoutingValidator.java io/branch/rnbranch/RNBranchModule.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/doublesymmetry/trackplayer/service/MusicService.java com/proyecto26/inappbrowser/RNInAppBrowser.java io/branch/referral/Branch.java io/branch/rnbranch/RNBranchModule.java
00078	Get the network operator name	collection telephony	com/learnium/RNDeviceInfo/RNDeviceModule.java com/mixpanel/android/mpmetrics/SystemInformation.java io/branch/referral/SystemObserver.java
00036	Get resource file from res/raw directory	reflection	coil/map/ResourceIntMapper.java com/brentvatne/exoplayer/ReactExoplayerViewManager.java com/doublesymmetry/trackplayer/utils/BundleUtils.java com/dylanvann/fastimage/FastImageSource.java com/proyecto26/inappbrowser/RNInAppBrowser.java io/branch/referral/Branch.java io/invertase/firebase/common/SharedUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	coil/fetch/ContentUriFetcher.java com/airbnb/android/react/lottie/LottieAnimationViewPropertyManager.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/PreviousSessionFinalizer.java io/sentry/android/core/SentryPerformanceProvider.java io/sentry/android/replay/ReplayCache.java io/sentry/cache/CacheStrategy.java io/sentry/cache/CacheUtils.java io/sentry/cache/EnvelopeCache.java io/sentry/config/FilesystemPropertiesLoader.java io/sentry/instrumentation/file/FileInputStreamInitData.java io/sentry/instrumentation/file/SentryFileInputStream.java io/sentry/util/FileUtils.java junit/runner/BaseTestRunner.java okio/Okio__JvmOkioKt.java org/junit/experimental/max/MaxHistory.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	coil/disk/DiskCache.java com/airbnb/lottie/LottieCompositionFactory.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/sentry/DirectoryProcessor.java io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/PreviousSessionFinalizer.java io/sentry/SentryOptions.java io/sentry/android/core/AndroidOptionsInitializer.java io/sentry/android/core/DeviceInfoUtil.java io/sentry/android/core/cache/AndroidEnvelopeCache.java io/sentry/android/replay/ReplayCache.java io/sentry/android/replay/capture/BufferCaptureStrategy.java io/sentry/cache/CacheStrategy.java io/sentry/cache/CacheUtils.java io/sentry/cache/EnvelopeCache.java io/sentry/instrumentation/file/FileIOSpanManager.java io/sentry/react/RNSentryModuleImpl.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/mixpanel/android/util/HttpService.java io/sentry/transport/HttpConnection.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 io/sentry/transport/HttpConnection.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java com/mixpanel/android/util/HttpService.java io/sentry/transport/HttpConnection.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	io/branch/coroutines/InstallReferrersKt.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00038	Query the phone number	collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
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
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java
00092	Send broadcast	command	io/branch/rnbranch/RNBranchModule.java
00012	Read data and put it into a buffer stream	file	io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/cache/CacheStrategy.java io/sentry/cache/EnvelopeCache.java io/sentry/config/FilesystemPropertiesLoader.java io/sentry/util/FileUtils.java
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/mixpanel/android/util/HttpService.java io/sentry/transport/HttpConnection.java
00094	Connect to a URL and read data from it	command network	com/mixpanel/android/util/HttpService.java

RULE ID	BEHAVIOUR	LABEL	FILES
00108	Read the input stream from given URL	network command	com/mixpanel/android/util/HttpService.java
00009	Put data in cursor to JSON object	file	com/mixpanel/android/mpmetrics/MPDbAdapter.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java
00091	Retrieve data from broadcast	collection	io/branch/referral/Branch.java
00003	Put the compressed bitmap data into JSON object	camera	io/branch/referral/network/BranchRemoteInterfaceUrlConnection.java
00005	Get absolute path of file and put it to JSON object	file	com/airbnb/lottie/LottieCompositionFactory.java
00024	Write file after Base64 decoding	reflection file	com/airbnb/lottie/LottieCompositionFactory.java
00004	Get filename and put it to JSON object	file collection	com/airbnb/lottie/LottieCompositionFactory.java com/mixpanel/android/mpmetrics/MPDbAdapter.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://fresh-tri-v2.firebaseio.com

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/695634764133/namespaces/firebase:fetch?key=AIzaSyB0T2LovYBI9yCmyI50i8QgREH-yyCK9Jg. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

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

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
help.branch.io	ok	**IP:** 104.18.21.218 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api3-eu.branch.io	ok	**IP:** 18.155.173.118 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.branch.io	ok	**IP:** 18.238.109.24 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
o475345.ingest.sentry.io	ok	**IP:** 34.120.195.249 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
cdn01.freshtri.com	ok	**IP:** 172.64.145.29 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
bnc.lt	ok	**IP:** 18.238.109.60 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
docs.swmansion.com	ok	**IP:** 104.21.27.136 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.cloudinary.com	ok	**IP:** 44.199.104.91 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
api.mixpanel.com	ok	**IP:** 130.211.34.183 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
cdn.branch.io	ok	**IP:** 18.238.109.61 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api2.branch.io	ok	**IP:** 18.238.109.69 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
shopify.github.io	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
branch.app.link	ok	**IP:** 18.238.109.69 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
fresh-tri-v2.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.114.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

✉ EMAILS

EMAIL	FILE
4a68a21dc65ed7e31768@o475345.ingest	com/engagedin/freshtri/BuildConfig.java
4a68a21dc65ed7e31768@o475345.ingest	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67

TRACKER	CATEGORIES	URL
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
MixPanel	Analytics	https://reports.exodus-privacy.eu.org/trackers/118
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"cloudinaryApiKey" : "536145677462815"
"facebook_client_token" : "0e8e00bd1e06cb61d3d0095ed498ad13"
"firebase_database_url" : "https://fresh-tri-v2.firebaseio.com"
"google_api_key" : "AIzaSyB0T2LovYBI9yCmyI50i8QgREH-yyCK9Jg"
"google_crash_reporting_api_key" : "AIzaSyB0T2LovYBI9yCmyI50i8QgREH-yyCK9Jg"
"mixpanelToken" : "0f03199f7fc331357b394421634cff9c"
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a

POSSIBLE SECRETS
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
85053bf24bba75239b16a601d9387e17
c56fb7d591ba6704df047fd98f535372fea00211
0f03199f7fc331357b394421634cff9c
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
e973d14c97f1c647a41b0aff5c0c1a26
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
9a04f079-9840-4286-ab92-e65be0885f95
fb65702c07554a68a21dc65ed7e31768
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
e2719d58-a985-b3c9-781a-b030af78d30e
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
9b8f518b086098de3d77736f9458a3d2f6f95a37
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc

POSSIBLE SECRETS
cc2751449a350f668590264ed76692694a80308a
b956059a88e9dfb420dc5fb101fd3156

PLAYSTORE INFORMATION

Title: Fresh Tri: Habits & Mindset

Score: 4.459649 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.engagedin.freshtri

Developer Details: Fresh Tri, LLC, Fresh+Tri,+LLC, None, https://freshtri.com/, support@freshtri.com,

Release Date: May 27, 2018 **Privacy Policy:** Privacy link

Description:

- No tracking, measuring, or weighing. No guilt, shame, or failure. - Achieve the natural, sustainable, healthy lifestyle you've always wanted. - Learn the Iterative Mindset Method to become unstoppable! - Choose habits that fit you, and practice them until they become your natural way of life. Fresh Tri is a mindset and habit-building app that helps you eat healthy, manage stress, move more and think positively using brain science. Remove the frustration, shame, and failure of traditional tactics. Current weight loss and habit tracking apps are designed for fast results, not lasting results. With Fresh Tri, you'll gradually learn and use the Iterative Mindset Method™ — a science-based, practice-and-iteration approach that keeps you going, no matter the obstacle. Iteration just means that you figure out what works for you right now, by adjusting and tweaking your way toward the lifestyle you love and can easily maintain. How To Use The Fresh Tri App Follow 4 Easy Steps to achieve the sustainable, healthy lifestyle you've always wanted. (1) Create your Tri, a simple habit to practice. Then, you will: (2) Check-In daily. If things are going well, say so! And if not, that's totally OK. Why: When you Check-In, you'll get tips and ideas for practicing your habit or changing it up. Either way, you're iterating your way to success! Fresh Tri believes that relapse and setbacks are a normal and necessary part of a lasting habit-building process. (3) Share with the community! Set your daily intention and gratitude within the Fresh “Tri(be)” feed. Why: Intentions encourage self-honesty and accountability, while gratitude has been scientifically proven to improve emotional and physical health. By sharing with others (anonymously, if you wish), you can inspire — and be inspired by — others in the community. (4) Train your mindset. Visit the Train section to build your new and more powerful Iterative Mindset! Why: Learn how to apply the Iterative Mindset to your daily practice with nationally recognized health and wellness trainers, including MDs, PhDs, RDNs, and Clinical Health Coaches. Explore over 720 Mindset training sessions developed to power your wellness journey.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 22:08:11	Generating Hashes	OK
2025-08-29 22:08:11	Extracting APK	OK
2025-08-29 22:08:11	Unzipping	OK
2025-08-29 22:08:11	Parsing APK with androguard	OK
2025-08-29 22:08:11	Extracting APK features using aapt/aapt2	OK
2025-08-29 22:08:11	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 22:08:13	Parsing AndroidManifest.xml	OK
2025-08-29 22:08:13	Extracting Manifest Data	OK
2025-08-29 22:08:13	Manifest Analysis Started	OK
2025-08-29 22:08:13	Performing Static Analysis on: Fresh Tri (com.engagedin.freshtri)	OK

2025-08-29 22:08:14	Fetching Details from Play Store: com.engagedin.freshtri	OK
2025-08-29 22:08:15	Checking for Malware Permissions	OK
2025-08-29 22:08:15	Fetching icon path	OK
2025-08-29 22:08:15	Library Binary Analysis Started	OK
2025-08-29 22:08:15	Reading Code Signing Certificate	OK
2025-08-29 22:08:16	Running APKiD 2.1.5	OK
2025-08-29 22:08:21	Detecting Trackers	OK
2025-08-29 22:08:25	Decompiling APK to Java with JADX	OK
2025-08-29 22:08:46	Converting DEX to Smali	OK
2025-08-29 22:08:46	Code Analysis Started on - java_source	OK
2025-08-29 22:08:49	Android SBOM Analysis Completed	OK

2025-08-29 22:08:58	Android SAST Completed	OK
2025-08-29 22:08:58	Android API Analysis Started	OK
2025-08-29 22:09:05	Android API Analysis Completed	OK
2025-08-29 22:09:06	Android Permission Mapping Started	OK
2025-08-29 22:09:13	Android Permission Mapping Completed	OK
2025-08-29 22:09:14	Android Behaviour Analysis Started	OK
2025-08-29 22:09:23	Android Behaviour Analysis Completed	OK
2025-08-29 22:09:23	Extracting Emails and URLs from Source Code	OK
2025-08-29 22:09:25	Email and URL Extraction Completed	OK
2025-08-29 22:09:25	Extracting String data from APK	OK
2025-08-29 22:09:25	Extracting String data from Code	OK

2025-08-29 22:09:25	Extracting String values and entropies from Code	OK
2025-08-29 22:09:29	Performing Malware check on extracted domains	OK
2025-08-29 22:09:36	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.