MOBSF

ANDROID STATIC ANALYSIS REPORT

Dribbleup (10.0.11)

File Name:	com.dribbleupmedball_1703092000.apk
Package Name:	com.dribbleupmedball
Scan Date:	Aug. 29, 2025, 9:54 p.m.
App Security Score:	49/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	22	2	2	1

FILE INFORMATION

File Name: com.dribbleupmedball_1703092000.apk
Size: 100.88MB
MD5: 4e6f6540cc155d36cb666076ec8aa20a
SHA1: 81e3891a0220b90aabb713797b2e64057a9aaef7
SHA256: c9a45bf01e2c552068568204e4a0c6f7dc89505d8d9fe41828b425317f668656

APP INFORMATION

App Name: Dribbleup
Package Name: com.dribbleupmedball
Main Activity: com.dribbleupapp.MainActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 10.0.11

Android Version Code: 1703092000

APP COMPONENTS

Activities: 9
Services: 15
Receivers: 16
Providers: 6
Exported Activities: 1
Exported Services: 3
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-04-22 23:43:12+00:00
Valid To: 2049-04-22 23:43:12+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xdc7e82ff5b3231806715181b74ef53de2f9e1e0d
Hash Algorithm: sha256
md5: e52da20d3eb7a6cc5ba254403f314f02
sha1: 6dabaeb1e9ad70d8ebe6c4c95139bd82234f9a1d
sha256: e0d5dbe4f838b3347042af8381182e0c96a9ead94ba1d67e269907f4697e35f0
sha512: 06407cca9230dee79601a5ad89afe3c6924386e4e178c87b3518a1a69d16a413a695bad185dc8142e614adaab6742d48bfd747135f5df8e616ec2df7bcca09ba
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 520859f2a44e53b230e009401378363f7dba94274ad7073379b7f4a0b919696e
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.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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".
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
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

PERMISSION	STATUS	INFO	DESCRIPTION
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.
com.dribbleupmedball.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.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>4e6f6540cc155d36cb666076ec8aa20a.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>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
possible Build.SERIAL check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes3.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check network operator name check possible VM check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

FILE	DETAILS
classes4.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check possible VM check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.dribbleupapp.MainActivity	Schemes: dribbleup://, Hosts: open,

NETWORK SECURITY

HIGH: 3 | WARNING: 1 | INFO: 0 | SECURE: 0

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	*	warning	Base config is configured to trust system certificates.
3	*	high	Base config is configured to trust user installed certificates.
4	du-matt.com localhost dribbleup.com	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: **9** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.

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

NO	ISSUE	SEVERITY	DESCRIPTION
6	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.
7	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.
8	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.

NO	ISSUE	SEVERITY	DESCRIPTION
9	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.
10	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: 9 | INFO: 1 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				app/notifee/core/AlarmPermissionBroadcastReceiver.java app/notifee/core/Logger.java app/notifee/core/RebootBroadcastReceiver.java app/notifee/core/b.java com/airbnb/android/react/lottie/LottieAnimationViewPropertyManager.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java com/aurelhubert/ahbottomnavigation/AHBottomNavigation.java com/brentvatne/react/ReactVideoView.java com/dooboolab/rniap/PlayUtils.java com/dooboolab/rniap/PromiseUtlisKt.java com/dooboolab/rniap/RNIapModule$getPurchaseHistoryByType$1.java com/dooboolab/rniap/RNIapModule.java com/dribbleupapp/bluetooth/Logger.java com/dribbleupapp/cameramodule/CameraPres

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/dribbleupapp/cameramodule/CameraProcessor.java com/dribbleupapp/cameramodule/CameraUtils.java com/dribbleupapp/cameramodule/MyCustomViewManager.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/MaskView.java com/horcrux/svg/PatternView.java com/horcrux/svg/RadialGradientView.java com/horcrux/svg/UseView.java com/horcrux/svg/VirtualView.java com/ibits/react_native_in_app_review/AppReviewModule.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/RNInstallReferrerClient.java com/learnium/RNDeviceInfo/resolver/DeviceIdResolver.java com/masteratul/exceptionhandler/DefaultErrorScreen.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/ResourceRe

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ader.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/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/asyncstorage/AsyncStorageModule.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java com/reactnativemmkv/MmkvModule.java com/reactnativenavigation/react/DevPermissionRequest.java com/reactnativenavigation/react/events/EventEmitter.java com/reactnativenavigation/utils/LogKt.java com/reactnativenavigation/utils/Time.java com/reactnativenavigation/utils/WindowInsetsUtils.java com/reactnativenavigation/viewcontrollers/stack/topbar/button/IconResolver.java com/reactnativenavigation/views/sidemenu/SideMenu.java com/sudoplz/rninappupdates/SpReactNativeInAppUpdatesModule.java com/swmansion/gesturehandler/react/RNGestu

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	reHandlerModule.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/swmansion/rnscreens/ScreensModule.java com/swmansion/rnscreens/SearchBarManager.java com/swmansion/rnscreens/utils/ScreenDummyLayoutHelper.java com/th3rdwave/safeareacontext/SafeAreaView.java com/wix/reactnativenotifications/RNNotificationsModule.java com/wix/reactnativenotifications/core/notification/PushNotification.java com/zmxv/RNSound/RNSoundModule.java com/zoontek/rnpermissions/RNPermissionsModule.java eightbitlab/com/blurview/BlurView.java im/shimo/react/prompt/RNPromptModule.java io/grpc/android/AndroidChannelBuilder.java io/grpc/okhttp/internal/Platform.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/invertase/firebase/app/ReactNativeFirebaseApp.java io/invertase/firebase/app/ReactNativeFirebaseAppModule.java io/invertase/firebase/common/RCTConvertFirebase.java io/invertase/firebase/common/ReactNativeFirebaseEventEmitter.java io/invertase/firebase/common/SharedUtils.java io/invertase/firebase/firestore/ReactNativeFirebaseFirestoreSerialize.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/invertase/notifee/NotifeeReactUtils.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 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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				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 org/tensorflow/lite/NativeInterpreterWrapper.java org/wonday/orientation/OrientationActivityLifecycle.java org/wonday/orientation/OrientationModule.java
2	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/mixpanel/android/mpmetrics/MPDbAdapter.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	coil/memory/MemoryCache.java coil/memory/MemoryCacheService.java coil/request/Parameters.java com/oblador/keychain/KeychainModule.java com/reactnativenavigation/options/params/ThemeColourKt.java com/reactnativenavigation/react/Constants.java com/sudoplz/rninappupdates/SpReactNativeInAppUpdatesModule.java io/grpc/PersistentHashArrayMappedTrie.java io/grpc/internal/DnsNameResolver.java io/grpc/internal/PickFirstLoadBalancerProvider.java io/grpc/internal/TransportFrameUtil.java io/invertase/firebase/common/TaskExecutorService.java io/invertase/notifee/NotifeeEventSubscriber.java io/sentry/Baggage.java io/sentry/RequestDetailsResolver.java io/sentry/SpanDataConvention.java io/sentry/TraceContext.java io/sentry/protocol/User.java net/time4j/tz/spi/WinZoneProviderSPI.java
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	io/grpc/okhttp/OkHttpClientTransport.java io/grpc/okhttp/OkHttpServerTransport.java
5	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	io/grpc/internal/DnsNameResolver.java io/grpc/internal/ExponentialBackoffPolicy.java io/grpc/internal/PickFirstLoadBalancer.java io/grpc/internal/RetriableStream.java io/grpc/okhttp/OkHttpClientTransport.java io/grpc/util/OutlierDetectionLoadBalancer.java io/grpc/util/RoundRobinLoadBalancer.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	io/grpc/okhttp/OkHttpChannelBuilder.java io/grpc/okhttp/OkHttpServerBuilder.java io/grpc/util/AdvancedTlsX509TrustManager.java
7	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
8	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
9	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 io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/sentry/android/core/DeviceInfoUtil.java
10	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 io/sentry/react/RNSentryModuleImpl.java
11	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

NO	ISSUE	SEVERITY	STANDARDS	FILES
12	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

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00175	Get notification manager and cancel notifications	notification	com/wix/reactnativenotifications/core/notificationdrawer/PushNotificationsDrawer.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
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java io/sentry/transport/HttpConnection.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	app/notifee/core/Notifee.java coil/map/ResourceIntMapper.java com/wix/reactnativenotifications/core/notification/NotificationChannel.java io/invertase/firebase/common/SharedUtils.java n/o/t/i/f/e/e/n.java
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 org/tensorflow/lite/Interpreter.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/dribbleupapp/objectdetection/TFLiteObjectDetectionAPIModel.java io/grpc/TlsChannelCredentials.java io/grpc/TlsServerCredentials.java io/grpc/util/AdvancedTlsX509KeyManager.java io/grpc/util/AdvancedTlsX509TrustManager.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 okio/Okio__JvmOkioKt.java
00091	Retrieve data from broadcast	collection	com/masteratul/exceptionhandler/DefaultErrorScreen.java com/wix/reactnativenotifications/core/NotificationIntentAdapter.java
00078	Get the network operator name	collection telephony	com/learnium/RNDeviceInfo/RNDeviceModule.java com/mixpanel/android/mpmetrics/SystemInformation.java
00056	Modify voice volume	control	com/zmxv/RNSound/RNSoundModule.java
00162	Create InetSocketAddress object and connecting to it	socket	io/grpc/android/UdsSocketFactory.java io/grpc/okhttp/internal/Platform.java

RULE ID	BEHAVIOUR	LABEL	FILES
00163	Create new Socket and connecting to it	socket	io/grpc/android/UdsSocket.java io/grpc/android/UdsSocketFactory.java io/grpc/okhttp/internal/Platform.java
00089	Connect to a URL and receive input stream from the server	command network	com/mixpanel/android/util/HttpService.java io/sentry/transport/HttpConnection.java
00109	Connect to a URL and get the response code	network command	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 net/time4j/tz/spi/TimezoneRepositoryProviderSPI.java
00108	Read the input stream from given URL	network command	com/mixpanel/android/util/HttpService.java
00043	Calculate WiFi signal strength	collection wifi	com/reactnativecommunity/netinfo/ConnectivityReceiver.java
00183	Get current camera parameters and change the setting.	camera	com/dribbleupapp/cameramodule/CameraProcessor.java com/dribbleupapp/cameramodule/CameraUtils.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	app/notifee/core/Notifee.java n/o/t/i/f/e/e/m.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	app/notifee/core/Notifee.java n/o/t/i/f/e/e/m.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00038	Query the phone number	collection	com/learnium/RNDeviceInfo/RNDeviceModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
00130	Get the current WIFI information	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00134	Get the current WiFi IP address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00082	Get the current WiFi MAC address	collection wifi	com/learnium/RNDeviceInfo/RNDeviceModule.java
00009	Put data in cursor to JSON object	file	com/mixpanel/android/mpmetrics/MPDbAdapter.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.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
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

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://du-medball-app.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/21097858504/namespaces/firebase:fetch?key=AIzaSyC0vQKGuLx6EwpmuOVqPQb5XzgBu4h5ZNo is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'app_store_review': 'false', 'deviceSetup__tableOffset': '0.75', 'deviceSetup__tableOffset_tablet': '0.75', 'maintenance_window': '{"startDate":0,"endDate":0}', 'onboard_v2_status_interval_ms': '1000', 'replay_sample_rate': '0.00', 'use_onboard_v2': 'true'}, 'state': 'UPDATE', 'templateVersion': '91'}

ABUSED PERMISSIONS

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

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
du-medball-app.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
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
notifee.app	ok	**IP:** 63.176.8.218 **Country:** United States of America **Region:** Virginia **City:** Reston **Latitude:** 38.925961 **Longitude:** -77.397331 **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
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
shopify.github.io	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.112.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
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
"firebase_database_url" : "https://du-medball-app.firebaseio.com"
"google_api_key" : "AIzaSyC0vQKGuLx6EwpmuOVqPQb5XzgBu4h5ZNo"
"google_crash_reporting_api_key" : "AIzaSyC0vQKGuLx6EwpmuOVqPQb5XzgBu4h5ZNo"

POSSIBLE SECRETS
5181942b9ebc31ce68dacb56c16fd79f
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
85053bf24bba75239b16a601d9387e17
1ddaa4b892e61b0f7010597ddc582ed3
ae2044fb577e65ee8bb576ca48a2f06e
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
24b2477514809255df232947ce7928c4

PLAYSTORE INFORMATION

Title: DribbleUp - Sports & Fitness

Score: 4.5877194 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.dribbleupmedball

Developer Details: DribbleUp Inc, DribbleUp+Inc, None, http://dribbleup.com, hello@dribbleup.com,

Release Date: Apr 23, 2019 **Privacy Policy:** Privacy link

Description:

The Official DribbleUp Sports & Fitness App New live and on-demand workouts every day with all your DribbleUp smart equipment. Medicine Ball, Boxing Gloves, Soccer, and Basketball! Using state-of-the-art technology, DribbleUp tracks your equipment to guide you through live and on-demand workouts. Take classes directly on your Android device or cast to a different compatible screen such as a smart television.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 21:54:13	Generating Hashes	OK
2025-08-29 21:54:14	Extracting APK	OK
2025-08-29 21:54:14	Unzipping	OK
2025-08-29 21:54:14	Parsing APK with androguard	OK
2025-08-29 21:54:14	Extracting APK features using aapt/aapt2	OK
2025-08-29 21:54:14	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 21:54:17	Parsing AndroidManifest.xml	OK
2025-08-29 21:54:17	Extracting Manifest Data	OK
2025-08-29 21:54:17	Manifest Analysis Started	OK

2025-08-29 21:54:17	Reading Network Security config from network_security_config.xml	OK
2025-08-29 21:54:17	Parsing Network Security config	OK
2025-08-29 21:54:17	Performing Static Analysis on: Dribbleup (com.dribbleupmedball)	OK
2025-08-29 21:54:18	Fetching Details from Play Store: com.dribbleupmedball	OK
2025-08-29 21:54:18	Checking for Malware Permissions	OK
2025-08-29 21:54:18	Fetching icon path	OK
2025-08-29 21:54:18	Library Binary Analysis Started	OK
2025-08-29 21:54:18	Reading Code Signing Certificate	OK
2025-08-29 21:54:19	Running APKiD 2.1.5	OK
2025-08-29 21:54:23	Detecting Trackers	OK
2025-08-29 21:54:27	Decompiling APK to Java with JADX	OK

2025-08-29 21:54:47	Converting DEX to Smali	OK
2025-08-29 21:54:47	Code Analysis Started on - java_source	OK
2025-08-29 21:54:51	Android SBOM Analysis Completed	OK
2025-08-29 21:54:58	Android SAST Completed	OK
2025-08-29 21:54:58	Android API Analysis Started	OK
2025-08-29 21:55:04	Android API Analysis Completed	OK
2025-08-29 21:55:04	Android Permission Mapping Started	OK
2025-08-29 21:55:09	Android Permission Mapping Completed	OK
2025-08-29 21:55:10	Android Behaviour Analysis Started	OK
2025-08-29 21:55:16	Android Behaviour Analysis Completed	OK
2025-08-29 21:55:16	Extracting Emails and URLs from Source Code	OK

2025-08-29 21:55:20	Email and URL Extraction Completed	OK
2025-08-29 21:55:20	Extracting String data from APK	OK
2025-08-29 21:55:20	Extracting String data from Code	OK
2025-08-29 21:55:20	Extracting String values and entropies from Code	OK
2025-08-29 21:55:24	Performing Malware check on extracted domains	OK
2025-08-29 21:55:25	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.