MOBSF

ANDROID STATIC ANALYSIS REPORT

athenaOne (1.0.10)

File Name:	com.athenaone.prod_15.apk
Package Name:	com.athenaone.prod
Scan Date:	Aug. 29, 2025, 7:58 p.m.
App Security Score:	63/100 (LOW RISK)
Grade:	
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	12	4	3	1

FILE INFORMATION

File Name: com.athenaone.prod_15.apk
Size: 25.06MB
MD5: 0208d11f67e901aafa5d73b03c1623c3
SHA1: 52ee23ce3db1184073f6e2f69ccc9ca23e461831
SHA256: c0e823399fab5481422e60414dba6746bd4ca1183d1e55672fa435d25628fedb

APP INFORMATION

App Name: athenaOne
Package Name: com.athenaone.prod
Main Activity: com.athenaone.MainActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 1.0.10

Android Version Code: 15

APP COMPONENTS

Activities: 6
Services: 7
Receivers: 3
Providers: 6
Exported Activities: 1
Exported Services: 1
Exported Receivers: 1
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: 2024-03-20 07:43:44+00:00
Valid To: 2054-03-20 07:43:44+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x18810a756e31ed8023e9566c421047a52d03a19a
Hash Algorithm: sha256
md5: de54fb9e04642c22a935c6f7da809d80
sha1: cb2bff4351e390e70757b8998b95742f8ae0226f
sha256: b911c3a40b31ec4f95e225d50ec3d0b1fa0f065476f73ed3f8b1ac95d653ada2
sha512: 57e79053353c6a67e815fdc1751ae79615a963f2e9c451bbb738c44ead35751c6404aad0bf6ea023a507d177305241b4c505287004bc233f28cd4aff06493215
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 4e7d1c1245de4cef53999899292c41d17f4b14b3319462758eebdb419fb4bfc1
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.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
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.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
com.athenaone.prod.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
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
0208d11f67e901aafa5d73b03c1623c3.apk	FINDINGS: Anti-VM Code — DETAILS: possible VM check

FILE	DETAILS
classes.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.MANUFACTURER check possible Build.SERIAL 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>
classes2.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>

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

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
net.openid.appauth.RedirectUriReceiverActivity	Schemes: x-ama-app://,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 0 | WARNING: 4 | 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	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.
3	Activity (net.openid.appauth.RedirectUriReceiverActivity) 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.
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.

</> CODE ANALYSIS

HIGH: **0** | WARNING: **6** | INFO: **4** | SECURE: **2** | 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/emeraldsanto/encryptedstorage/RNEncryptedStorageModule.java com/fastrsa/FastRsaModule.java com/gantix/JailMonkey/AdbEnabled/AdbEnabled.java com/gantix/JailMonkey/MockLocation/MockLocationCheck.java com/github/barteksc/pdfviewer/PDFView.java com/github/barteksc/pdfviewer/RenderingHandler.java com/github/barteksc/pdfviewer/link/DefaultLinkHandler.java com/github/mikephil/charting/charts/BarChart.java com/github/mikephil/charting/charts/BarLineChartBase.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/charts/CombinedChart.java com/github/mikephil/charting/charts/HorizontalBarChart.java com/github/mikephil/charting/charts/PieRadarChartBase.java com/github/mikephil/charting/components/AxisBase.java com/github/mikephil/charting/data/ChartData.java com/github/mikephil/charting/data/CombinedData.java com/github/mikephil/charting/data/LineDat

NO	ISSUE	SEVERITY	STANDARDS	FILES
				aSet.java com/github/mikephil/charting/data/PieEntry.java com/github/mikephil/charting/listener/BarLineChartTouchListener.java com/github/mikephil/charting/renderer/CombinedChartRenderer.java com/github/mikephil/charting/renderer/ScatterChartRenderer.java com/github/mikephil/charting/utils/FileUtils.java com/github/mikephil/charting/utils/Utils.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/iterable/iterableapi/IterableActionRunner.java com/iterable/iterableapi/IterableLogger.java com/launchdarkly/sdk/android/LDAndroidLogging.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/RNInstallReferrerClient.java com/learnium/RNDeviceInfo/resolver/DeviceIdResolver.java com/lugg/RNCConfig/RNCConfigModule.java com/reactnativeavoidsoftinput/ReactNativeAvoidSoftInputLogger.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java
	The App logs information. Sensitive		CWE: CWE-532: Insertion of Sensitive	

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	[redacted] information should never be logged.	info	Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/reactnativecommunity/asyncstorage/AsyncStorageModule.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java com/reactnativecommunity/webview/RNCWebView.java com/reactnativecommunity/webview/RNCWebViewClient.java com/reactnativecommunity/webview/RNCWebViewManagerImpl.java com/reactnativecommunity/webview/RNCWebViewModuleImpl.java com/rnappauth/utils/UnsafeConnectionBuilder.java com/scottyab/rootbeer/RootBeer.java com/scottyab/rootbeer/RootBeerNative.java com/scottyab/rootbeer/util/QLog.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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				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/SafeAreaView.java io/invertase/firebase/app/ReactNativeFirebaseApp.java io/invertase/firebase/app/ReactNativeFirebaseAppModule.java io/invertase/firebase/common/RCTConvertFirebase.java io/invertase/firebase/common/ReactNativeFirebaseEventEmitter.java io/invertase/firebase/common/SharedUtils.java io/invertase/firebase/crashlytics/ReactNativeFirebaseCrashlyticsInitProvider.java io/invertase/firebase/crashlytics/ReactNativeFirebaseCrashlyticsModule.java io/invertase/firebase/perf/ScreenTrace.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/legere/pdfiumandroid/DefaultLogger.java io/legere/pdfiumandroid/PdfiumCore.java net/openid/appauth/internal/Logger.java org/wonday/pdf/PdfView.java timber/log/Timber.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	com/gantix/JailMonkey/HookDetection/HookDetectionCheck.java com/scottyab/rootbeer/Const.java
3	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/iterable/iterableapi/IterableDatabaseManager.java com/iterable/iterableapi/IterableTaskStorage.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/launchdarkly/eventsource/EventSource.java com/rnappauth/utils/UnsafeConnectionBuilder.java
5	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/gantix/JailMonkey/Rooted/GreaterThan23.java com/gantix/JailMonkey/Rooted/LessThan23.java com/scottyab/rootbeer/RootBeer.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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/athenaone/BuildConfig.java com/iterable/iterableapi/IterableConstants.java com/iterable/iterableapi/IterableKeychain.java com/launchdarkly/sdk/LDContext.java com/launchdarkly/sdk/android/PersistentDataStoreWrapper.java com/reactnativeavoidsoftinput/AvoidSoftInputModuleImpl.java com/reactnativeavoidsoftinput/events/AvoidSoftInputAppliedOffsetChangedEvent.java com/reactnativeavoidsoftinput/events/BaseAvoidSoftInputEvent.java io/invertase/firebase/common/TaskExecutorService.java net/openid/appauth/TokenRequest.java
7	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/ReactNativeBlobUtil/ReactNativeBlobUtilFS.java com/ReactNativeBlobUtil/Utils/PathResolver.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/utils/FileUtils.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/reactnativecommunity/webview/RNCWebViewModuleImpl.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/ReactNativeBlobUtil/ReactNativeBlobUtilBody.java com/reactnativecommunity/webview/RNCWebViewModuleImpl.java
9	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/iterable/iterableapi/IterableKeychain.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/ReactNativeBlobUtil/ReactNativeBlobUtilUtils.java com/airbnb/lottie/network/NetworkCache.java
11	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	com/reactnativecommunity/clipboard/ClipboardModule.java
12	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/reactnativecommunity/clipboard/ClipboardModule.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/ReactNativeBlobUtil/ReactNativeBlobUtilBody.java com/ReactNativeBlobUtil/ReactNativeBlobUtilFS.java com/ReactNativeBlobUtil/ReactNativeBlobUtilMediaCollection.java com/ReactNativeBlobUtil/ReactNativeBlobUtilStream.java com/airbnb/android/react/lottie/LottieAnimationViewPropertyManager.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/iterable/iterableapi/IterableUtilImpl.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java okio/Okio__JvmOkioKt.java
00043	Calculate WiFi signal strength	collection wifi	com/reactnativecommunity/netinfo/ConnectivityReceiver.java
00123	Save the response to JSON after connecting to the remote server	network command	net/openid/appauth/AuthorizationServiceConfiguration.java
00091	Retrieve data from broadcast	collection	com/ReactNativeBlobUtil/ReactNativeBlobUtilReq.java com/iterable/iterableapi/IterableApi.java com/iterable/iterableapi/IterablePushNotificationUtil.java net/openid/appauth/AuthorizationManagementActivity.java
00022	Open a file from given absolute path of the file	file	com/ReactNativeBlobUtil/ReactNativeBlobUtilFS.java com/ReactNativeBlobUtil/ReactNativeBlobUtilReq.java com/ReactNativeBlobUtil/Utils/PathResolver.java com/airbnb/lottie/LottieCompositionFactory.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/github/mikephil/charting/charts/Chart.java com/launchdarkly/sdk/android/HttpFeatureFlagFetcher.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/ReactNativeBlobUtil/ReactNativeBlobUtilImpl.java com/ReactNativeBlobUtil/ReactNativeBlobUtilReq.java com/github/barteksc/pdfviewer/link/DefaultLinkHandler.java com/github/wumke/RNImmediatePhoneCall/RNImmediatePhoneCallModule.java com/iterable/iterableapi/IterableActionRunner.java com/iterable/iterableapi/IterableNotificationHelper.java com/rnappauth/RNAppAuthModule.java net/openid/appauth/AuthorizationException.java
00036	Get resource file from res/raw directory	reflection	com/iterable/iterableapi/IterableActionRunner.java com/iterable/iterableapi/IterableNotificationHelper.java io/invertase/firebase/common/SharedUtils.java
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/iterable/iterableapi/IterableRequestTask.java net/openid/appauth/AuthorizationService.java
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/github/wuxudong/rncharts/utils/DrawableUtils.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/ReactNativeBlobUtil/ReactNativeBlobUtilReq.java com/iterable/iterableapi/IterableActionRunner.java
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java
00024	Write file after Base64 decoding	reflection file	com/ReactNativeBlobUtil/ReactNativeBlobUtilBody.java com/ReactNativeBlobUtil/ReactNativeBlobUtilReq.java com/airbnb/lottie/LottieCompositionFactory.java
00189	Get the content of a SMS message	sms	com/ReactNativeBlobUtil/Utils/PathResolver.java

RULE ID	BEHAVIOUR	LABEL	FILES
00192	Get messages in the SMS inbox	sms	com/ReactNativeBlobUtil/Utils/PathResolver.java
00188	Get the address of a SMS message	sms	com/ReactNativeBlobUtil/Utils/PathResolver.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/ReactNativeBlobUtil/Utils/PathResolver.java
00191	Get messages in the SMS inbox	sms	com/ReactNativeBlobUtil/ReactNativeBlobUtilReq.java com/ReactNativeBlobUtil/Utils/PathResolver.java
00200	Query data from the contact list	collection contact	com/ReactNativeBlobUtil/Utils/PathResolver.java
00201	Query data from the call log	collection calllog	com/ReactNativeBlobUtil/Utils/PathResolver.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/ReactNativeBlobUtil/Utils/PathResolver.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00078	Get the network operator name	collection telephony	com/learnium/RNDeviceInfo/RNDeviceModule.java
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

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	com/github/wuxudong/rncharts/utils/DrawableUtils.java com/iterable/iterableapi/IterableRequestTask.java net/openid/appauth/AuthorizationService.java
00109	Connect to a URL and get the response code	network command	com/iterable/iterableapi/IterableDeeplinkManager.java com/iterable/iterableapi/IterableRequestTask.java net/openid/appauth/AuthorizationService.java
00005	Get absolute path of file and put it to JSON object	file	com/airbnb/lottie/LottieCompositionFactory.java
00004	Get filename and put it to JSON object	file collection	com/airbnb/lottie/LottieCompositionFactory.java
00125	Check if the given file path exist	file	com/ReactNativeBlobUtil/ReactNativeBlobUtilReq.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/643766357236/namespaces/firebase:fetch?key=AIzaSyAGU3KfYbmrsFCe2zT53M_QKNnwWgRHfLI. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	3/44	android.permission.CALL_PHONE, 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

DOMAIN	STATUS	GEOLOCATION
athenaone.api.athena.io	ok	**IP:** 52.223.11.224 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api.iterable.com	ok	**IP:** 34.197.231.174 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
links.iterable.com	ok	**IP:** 52.71.110.1 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
mobile.launchdarkly.com	ok	**IP:** 18.214.35.222 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
success.athenahealth.com	ok	**IP:** 13.110.52.8 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.788464 **Longitude:** -122.394608 **View:** Google Map
athenaone.preview.api.athena.io	ok	**IP:** 34.225.179.172 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **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.eu.iterable.com	ok	**IP:** 52.31.143.172 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
clientsdk.launchdarkly.com	ok	**IP:** 151.101.1.55 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
athenaone.sandbox.api.athena.io	ok	**IP:** 54.83.190.37 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
athenaone.clienttrain.api.athena.io	ok	**IP:** 54.160.46.86 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
clientstream.launchdarkly.com	ok	**IP:** 13.248.151.210 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

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

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27

HARDCODED SECRETS

POSSIBLE SECRETS
"API_URL" : "https://athenaone.api.athena.io"
"CLEINTTRAIN_API_URL" : "https://athenaone.clienttrain.api.athena.io"
"DUMMY_TEST_USER_NAME" : "testuser"
"DUMMY_TEST_USER_PASSWORD" : "cn@123"

POSSIBLE SECRETS
"PREVIEW_API_URL" : "https://athenaone.preview.api.athena.io"
"SANDBOX_API_URL" : "https://athenaone.sandbox.api.athena.io"
"com.google.firebase.crashlytics.mapping_file_id" : "47c407e050a447fb8bb338248467f077"
"google_api_key" : "AIzaSyAGU3KfYbmrsFCe2zT53M_QKNnwWgRHfLI"
"google_crash_reporting_api_key" : "AIzaSyAGU3KfYbmrsFCe2zT53M_QKNnwWgRHfLI"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
23456789abcdefghjkmnpqrstvwxyz
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
7fmduHKTdHHrlMvldlEqAllSfii1tl35bxj1OXN5Ve8c4lU6URVu4xtSHc3BVZxS6WWJnxMDhIfQN0N0K2NDJg==
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
ABi2fbt8vkzj7SJ8aD5jc4xJFTDFntdkMrYXL3itsvqY1Qlw
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43

POSSIBLE SECRETS
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
dZozdop5rgKNxjbrQAd5nntAGpgh9w84O1Xgg==
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
115792089210356248762697446949407573530086143415290314195533631308867097853951
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: athenaOne

Score: 2.7317073 **Installs:** 10,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.athenaone.prod

Developer Details: athenahealth, athenahealth, None, None, vbadave@athenahealth.com,

Release Date: Apr 2, 2024 **Privacy Policy:** Privacy link

Description:

athenaOne Mobile for Android Designed with doctors and healthcare providers in mind, the athenaOne mobile app for Android is a secure extension of athenaClinicals on desktop. The app supports clinicians in delivering high quality care to patients and completing key clinical tasks, even when they're away from their desk. The app syncs in real time, so you have access to the most up to date information, on the go. What you can do: See what's coming Access your daily schedule and upcoming appointments for yourself and/or those you support. Stay connected View inbox categories such as Open encounters, Labs & Imaging, and Patient Cases. Identify and contact patients Look up patient information like contact details, care team, insurance, pharmacies and more. Review patient information View sections of the patient chart like Allergies, Problems, Vaccines, Medications, and Labs & Imaging.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 19:58:22	Generating Hashes	OK
2025-08-29 19:58:22	Extracting APK	OK
2025-08-29 19:58:22	Unzipping	OK
2025-08-29 19:58:22	Parsing APK with androguard	OK
2025-08-29 19:58:22	Extracting APK features using aapt/aapt2	OK

2025-08-29 19:58:22	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 19:58:24	Parsing AndroidManifest.xml	OK
2025-08-29 19:58:24	Extracting Manifest Data	OK
2025-08-29 19:58:24	Manifest Analysis Started	OK
2025-08-29 19:58:24	Performing Static Analysis on: athenaOne (com.athenaone.prod)	OK
2025-08-29 19:58:24	Fetching Details from Play Store: com.athenaone.prod	OK
2025-08-29 19:58:25	Checking for Malware Permissions	OK
2025-08-29 19:58:25	Fetching icon path	OK
2025-08-29 19:58:25	Library Binary Analysis Started	OK
2025-08-29 19:58:25	Reading Code Signing Certificate	OK
2025-08-29 19:58:25	Running APKiD 2.1.5	OK

2025-08-29 19:58:27	Detecting Trackers	OK
2025-08-29 19:58:30	Decompiling APK to Java with JADX	OK
2025-08-29 19:58:46	Converting DEX to Smali	OK
2025-08-29 19:58:46	Code Analysis Started on - java_source	OK
2025-08-29 19:58:48	Android SBOM Analysis Completed	OK
2025-08-29 19:58:53	Android SAST Completed	OK
2025-08-29 19:58:53	Android API Analysis Started	OK
2025-08-29 19:58:56	Android API Analysis Completed	OK
2025-08-29 19:58:57	Android Permission Mapping Started	OK
2025-08-29 19:59:00	Android Permission Mapping Completed	OK
2025-08-29 19:59:01	Android Behaviour Analysis Started	OK

2025-08-29 19:59:05	Android Behaviour Analysis Completed	OK
2025-08-29 19:59:05	Extracting Emails and URLs from Source Code	OK
2025-08-29 19:59:06	Email and URL Extraction Completed	OK
2025-08-29 19:59:06	Extracting String data from APK	OK
2025-08-29 19:59:06	Extracting String data from Code	OK
2025-08-29 19:59:06	Extracting String values and entropies from Code	OK
2025-08-29 19:59:09	Performing Malware check on extracted domains	OK
2025-08-29 19:59:11	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.