



ANDROID STATIC ANALYSIS REPORT



 AccessNow (2.5.1)

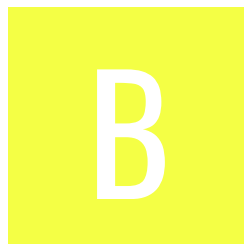
File Name: AccessNow.apk

Package Name: com.accessnow.app

Scan Date: Nov. 17, 2024, 11:34 p.m.






App Security Score: 49/100 (MEDIUM RISK)

Grade:



Trackers Detection: 6/432

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
3	15	3	2	1

FILE INFORMATION

File Name: AccessNow.apk

Size: 10.59MB

MD5: a7fc3cb21ab359a27a1bbc0c84419fc1

SHA1: 564df6295cc3e36fed919a5042e2f89b37511ce2

SHA256: 031258b3e32432dac71de8a7b421c02dcd72583a685be554b1123b1c8d88dfed

APP INFORMATION

App Name: AccessNow

Package Name: com.accessnow.app

Main Activity: com.accessnow.app.SplashActivity

Target SDK: 33

Min SDK: 23

Max SDK:

Android Version Name: 2.5.1

Android Version Code: 74

APP COMPONENTS

Activities: 10

Services: 14

Receivers: 13

Providers: 12

Exported Activities: 2

Exported Services: 2

Exported Receivers: 2

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: 2019-09-18 14:09:06+00:00

Valid To: 2049-09-18 14:09:06+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0x30bf8c0b8116d592f46f5189fc126e21b745ff04

Hash Algorithm: sha256

md5: 0ef20f2e00d2d3ca0436f5adc157610d

sha1: 16d71c60bf0c7d3b62a279f4fc74f8c1e7785a81

sha256: 61251234bc0e0739437c23e1240c8349d156b00c1a7ce41ca300d37f721ac464

sha512: f080abaf90217fdb7ee5c0274192604312fb68557b0b399325b82781a24c708d642bd9f6b7e843a0176bbd9c152c97134cfbd9887be206f7df0eae14b7fbf3d0

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 271ba6dd7e50cd9e87a412166a27f5d2e2e1a1c11dc85660973994644c4fed3b

Found 1 unique certificates

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY	unknown	Unknown permission	Unknown permission from android reference
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.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.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
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.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check possible Build.SERIAL check Build.TAGS check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8 without marker (suspicious)

FILE	DETAILS	
classes2.dex	FINDINGS	DETAILS
	Anti-VM Code	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
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8 without marker (suspicious)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.accessnow.app.MainActivity	Schemes: accessnow://, https://, Hosts: *, map.accessnow.com,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.accessnow.app,

NETWORK SECURITY

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

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

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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

TITLE	SEVERITY	DESCRIPTION
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.

Q MANIFEST ANALYSIS

HIGH: 1 | WARNING: 6 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched 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	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Activity (com.accessnow.app.MainActivity) 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	Broadcast Receiver (com.learnium.RNDeviceInfo.RNDeviceReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
5	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.
6	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.
7	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.

NO	ISSUE	SEVERITY	DESCRIPTION
8	<p>Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission: android.permission.DUMP [android:exported=true]</p>	warning	<p>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.</p>

</> CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	<p>App can write to App Directory. Sensitive Information should be encrypted.</p>	info	<p>CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14</p>	<p>expo/modules/adapters/react/permissions/PermissionsService.java expo/modules/constants/ExponentInstallatonId.java expo/modules/errorrecovery/ErrorRecoveryModule.java</p>
				<p>cl/json/RNShareModule.java cl/json/RNSharePathUtil.java cl/json/social/InstagramShare.java cl/json/social/SingleShareIntent.java com/brentvatne/react/ReactVideoView.java com/bumptechnology/glide/GeneratedAppGlideModuleImpl.java com/bumptechnology/glide/Glide.java</p>

NO	ISSUE	SEVERITY	STANDARDS	FILES
				<div>com/bumptech/glide/disklru/DiskLruCache.java</div> <div>com/bumptech/glide/gifdecoder/GifHeaderParser.java</div> <div>com/bumptech/glide/gifdecoder/StandardGifDecoder.java</div> <div>com/bumptech/glide/load/data/AssetPathFetcher.java</div> <div>com/bumptech/glide/load/data/HttpUrlFetcher.java</div> <div>com/bumptech/glide/load/data/LocalUriFetcher.java</div> <div>com/bumptech/glide/load/data/mediastore/ThumbFetcher.java</div> <div>com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java</div> <div>com/bumptech/glide/load/engine/DecodeJob.java</div> <div>com/bumptech/glide/load/engine/DecodePath.java</div> <div>com/bumptech/glide/load/engine/Engine.java</div> <div>com/bumptech/glide/load/engine/GlideException.java</div> <div>com/bumptech/glide/load/engine/SourceGenerator.java</div> <div>com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java</div> <div>com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java</div> <div>com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java</div> <div>com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java</div> <div>com/bumptech/glide/load/engine/executor/GlideExecutor.java</div> <div>com/bumptech/glide/load/engine/executor/RuntimeCompat.java</div> <div>com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java</div>

NO	ISSUE	SEVERITY	STANDARDS	FILES
				<div>com/bumptech/glide/load/model/ByteBufferLoader.java</div> <div>com/bumptech/glide/load/model/ByteBufferLoader.java</div> <div>com/bumptech/glide/load/model/FileLoader.java</div> <div>com/bumptech/glide/load/model/FileLoader.java</div> <div>com/bumptech/glide/load/model/ResourceLoader.java</div> <div>com/bumptech/glide/load/model/ResourceLoader.java</div> <div>com/bumptech/glide/load/model/StreamEncoder.java</div> <div>com/bumptech/glide/load/model/StreamEncoder.java</div> <div>com/bumptech/glide/load/resource/ImageDecoderResourceDecoder.java</div> <div>com/bumptech/glide/load/resource/ImageDecoderResourceDecoder.java</div> <div>com/bumptech/glide/load/resource/Bitmap/BitmapEncoder.java</div> <div>com/bumptech/glide/load/resource/Bitmap/BitmapEncoder.java</div> <div>com/bumptech/glide/load/resource/Bitmap/BitmapImageDecoderResourceDecoder.java</div> <div>com/bumptech/glide/load/resource/Bitmap/BitmapImageDecoderResourceDecoder.java</div> <div>com/bumptech/glide/load/resource/Bitmap/DefaultImageHeaderParser.java</div> <div>com/bumptech/glide/load/resource/Bitmap/DefaultImageHeaderParser.java</div> <div>com/bumptech/glide/load/resource/Bitmap/Downsampler.java</div> <div>com/bumptech/glide/load/resource/Bitmap/Downsampler.java</div> <div>com/bumptech/glide/load/resource/Bitmap/DrawableToBitmapConverter.java</div> <div>com/bumptech/glide/load/resource/Bitmap/DrawableToBitmapConverter.java</div> <div>com/bumptech/glide/load/resource/Bitmap/HardwareConfigState.java</div> <div>com/bumptech/glide/load/resource/Bitmap/HardwareConfigState.java</div> <div>com/bumptech/glide/load/resource/Bitmap/TransformationUtils.java</div> <div>com/bumptech/glide/load/resource/Bitmap/TransformationUtils.java</div> <div>com/bumptech/glide/load/resource/Bitmap/VideoDecoder.java</div> <div>com/bumptech/glide/load/resource/Bitmap/VideoDecoder.java</div> <div>com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java</div> <div>com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java</div> <div>com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java</div> <div>com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java</div> <div>com/bumptech/glide/load/resource/gif/StreamGifDecoder.java</div> <div>com/bumptech/glide/load/resource/gif/StreamGifDecoder.java</div> <div>com/bumptech/glide/manager/DefaultConnectivityMonitor.java</div> <div>com/bumptech/glide/manager/DefaultConnectivityMonitor.java</div> <div>com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java</div> <div>com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java</div> <div>com/bumptech/glide/manager/RequestManager.java</div> <div>com/bumptech/glide/manager/RequestManager.java</div>

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	agerFragment.java com/bumptechnology/glide/manager/RequestManagerRetriever.java com/bumptechnology/glide/manager/RequestTracker.java com/bumptechnology/glide/manager/SupportRequestManagerFragment.java com/bumptechnology/glide/module/ManifestParser.java com/bumptechnology/glide/request/SingleRequest.java com/bumptechnology/glide/request/target/CustomViewTarget.java com/bumptechnology/glide/request/target/ViewTarget.java com/bumptechnology/glide/signature/ApplicationVersionSignature.java com/bumptechnology/glide/util/pool/FactoryPools.java com/imagepicker/ImageMetadata.java com/imagepicker/Metadata.java com/imagepicker/VideoMetadata.java com/learnium/RNDeviceInfo/RNDeviceInfoModule.java com/learnium/RNDeviceInfo/RNInstallReferrerClient.java com/learnium/RNDeviceInfo/resolver/DeviceIdResolver.java com/proyecto26/inappbrowser/RNInAppBrowser.java com/reactnative/ivpusic/imagepicker/Compression.java com/reactnative/ivpusic/imagepicker/ResultCollector.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/reactnativecommunity/asyncstorage/AsyncStorageModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				<div>com/reactnativecommunity/asyncstorage/R</div> <div>com/reactnativecommunity/DatabaseSupplier.java</div> <div>com/rnmaps/maps/FileUtil.java</div> <div>com/rnmaps/maps/MapGradientPolyline.java</div> <div>com/rnmaps/maps/MapModule.java</div> <div>com/rnmaps/maps/MapTileProvider.java</div> <div>com/rnmaps/maps/MapTileWorker.java</div> <div>com/rnmaps/maps/MapUrlTile.java</div> <div>com/swmansion/gesturehandler/react/RNGestureHandlerRootHelper.java</div> <div>com/swmansion/gesturehandler/react/RNGestureHandlerRootView.java</div> <div>com/swmansion/reanimated/NativeMethodHelper.java</div> <div>com/swmansion/reanimated/NativeProxy.java</div> <div>com/swmansion/reanimated/ReanimatedJSIModulePackage.java</div> <div>com/swmansion/reanimated/ReanimatedModule.java</div> <div>com/swmansion/reanimated/layoutReanimation/ReanimatedNativeHierarchyManager.java</div> <div>com/swmansion/reanimated/nodes/DebugNode.java</div> <div>com/swmansion/reanimated/sensor/ReanimatedSensorContainer.java</div> <div>com/th3rdwave/safeareacontext/SafeAreaView.java</div> <div>com/yalantis/ucrop/UCropActivity.java</div> <div>com/yalantis/ucrop/task/BitmapCropTask.java</div> <div>com/yalantis/ucrop/task/BitmapLoadTask.java</div> <div>com/yalantis/ucrop/util/BitmapLoadUtils.java</div> <div>com/yalantis/ucrop/util/EglUtils.java</div> <div>com/yalantis/ucrop/util/ImageHeaderParser.java</div>

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/yalantis/ucrop/view/TransformImageView.java expo/modules/ExpoModulesPackage.java expo/modules/adapters/react/views/ViewManagerAdapterUtils.java expo/modules/application/ApplicationModule.java expo/modules/constants/ConstantsService.java expo/modules/constants/ExponentInstallationId.java expo/modules/filesystem/FileSystemModule.java expo/modules/location/LocationHelpers.java expo/modules/location/LocationModule.java expo/modules/location/services/LocationTaskService.java expo/modules/location/taskConsumers/LocationTaskConsumer.java fr/bamlab/rnimageresizer/ImageResizer.java fr/bamlab/rnimageresizer/ImageResizerModule.java io/invertase/firebase/app/ReactNativeFirebaseApp.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/Utils/ReactNativeFirebaseUtilsModule.java io/nlopez/smartlocation/Utils/LoggerFactory.java io/sentry/android/core/AndroidLogger.java io/sentry/core/SystemOutLogger.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	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/reactnative/ivpusic/imagepicker/PickerModule.java expo/modules/adapters/react/NativeModulesProxy.java
4	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/sentry/core/SentryClient.java
5	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/util/RootChecker.java
6	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/DefaultAndroidEventProcessor.java io/sentry/android/core/util/RootChecker.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/learnium/RNDeviceInfo/RNDeviceModule.java com/reactnative/ivpusic/imagepicker/Compression.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnative/ivpusic/imagepicker/RealPathUtil.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/sentry/android/core/DefaultAndroidEventProcessor.java
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/reactnative/ivpusic/imagepicker/PickerModule.java com/rnmaps/maps/FileUtil.java com/rnmaps/maps/MapModule.java
9	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/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.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	expo/modules/filesystem/FileSystemModule.java

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	cl/json/RNShareModule.java cl/json/social/InstagramShare.java cl/json/social/SingleShareIntent.java com/proyecto26/inappbrowser/RNInAppBrowser.java com/reactnative/ivpusic/imagepicker/PickerModule.java expo/modules/adapters/react/permissions/PermissionsService.java expo/modules/filesystem/FileSystemModule.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	cl/json/social/InstagramShare.java com/proyecto26/inappbrowser/RNInAppBrowser.java expo/modules/adapters/react/permissions/PermissionsService.java
00036	Get resource file from res/raw directory	reflection	cl/json/RNSharePathUtil.java com/dylanvann/fastimage/FastImageSource.java com/proyecto26/inappbrowser/RNInAppBrowser.java com/rnmaps/maps/ImageReader.java com/rnmaps/maps/MapMarker.java expo/modules/adapters/react/permissions/PermissionsService.java expo/modules/filesystem/FileSystemModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/bumptech/glide/disklru/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/imagepicker/VideoMetadata.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/rnmaps/maps/FileUtil.java com/rnmaps/maps/MapLocalTile.java com/rnmaps/maps/MapTileProvider.java com/yalantis/ucrop/util/FileUtils.java expo/modules/filesystem/FileSystemModule.java io/sentry/core/EnvelopeSender.java io/sentry/core/SendCachedEvent.java io/sentry/core/cache/DiskCache.java io/sentry/core/cache/SessionCache.java okio/Okio.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	cl/json/RNSharePathUtil.java cl/json/ShareFile.java cl/json/ShareFiles.java com/oblador/vectoricons/VectorIconsModule.java com/reactnative/ivpusic/imagepicker/Compression.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnative/ivpusic/imagepicker/RealPathUtil.java expo/modules/filesystem/FileSystemModule.java fr/bamlab/rnimagepicker/ImageResizer.java fr/bamlab/rnimagepicker/ImageResizerModule.java io/invertase/firebase/Utils/ReactNativeFirebaseUtilsModule.java io/sentry/android/core/AndroidOptionsInitializer.java io/sentry/android/core/DefaultAndroidEventProcessor.java io/sentry/core/DirectoryProcessor.java io/sentry/core/EnvelopeSender.java io/sentry/core/SendCachedEvent.java io/sentry/core/cache/DiskCache.java io/sentry/core/cache/SessionCache.java
00024	Write file after Base64 decoding	reflection file	cl/json/ShareFile.java cl/json/ShareFiles.java expo/modules/filesystem/FileSystemModule.java fr/bamlab/rnimagepicker/ImageResizer.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java
00012	Read data and put it into a buffer stream	file	expo/modules/filesystem/FileSystemModule.java io/sentry/core/EnvelopeSender.java io/sentry/core/cache/SessionCache.java
00091	Retrieve data from broadcast	collection	expo/modules/location/services/LocationTaskService.java

RULE ID	BEHAVIOUR	LABEL	FILES
00072	Write HTTP input stream into a file	command network file	fr/bamlab/rnimageresizer/ImageResizer.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java fr/bamlab/rnimageresizer/ImageResizer.java io/sentry/core/transport/HttpTransport.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java fr/bamlab/rnimageresizer/ImageResizer.java io/sentry/core/transport/HttpTransport.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/rnmaps/maps/MapTileProvider.java fr/bamlab/rnimageresizer/ImageResizer.java
00094	Connect to a URL and read data from it	command network	fr/bamlab/rnimageresizer/ImageResizer.java
00108	Read the input stream from given URL	network command	fr/bamlab/rnimageresizer/ImageResizer.java
00192	Get messages in the SMS inbox	sms	cl/json/RNSharePathUtil.java com/reactnative/ivpusic/imagepicker/RealPathUtil.java
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java
00121	Create a directory	file command	expo/modules/filesystem/FileSystemModule.java
00125	Check if the given file path exist	file	expo/modules/filesystem/FileSystemModule.java
00104	Check if the given path is directory	file	expo/modules/filesystem/FileSystemModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/UrlFetcher.java io/sentry/core/transport/HttpTransport.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceInfoModule.java
00078	Get the network operator name	collection telephony	com/learnium/RNDeviceInfo/RNDeviceInfoModule.java
00038	Query the phone number	collection	com/learnium/RNDeviceInfo/RNDeviceInfoModule.java
00130	Get the current WIFI information	wifi collection	com/learnium/RNDeviceInfo/RNDeviceInfoModule.java
00134	Get the current WiFi IP address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceInfoModule.java
00082	Get the current WiFi MAC address	collection wifi	com/learnium/RNDeviceInfo/RNDeviceInfoModule.java
00191	Get messages in the SMS inbox	sms	com/reactnative/ivpusic/imagepicker/RealPathUtil.java
00147	Get the time of current location	collection location	expo/modules/location/LocationHelpers.java
00043	Calculate WiFi signal strength	collection wifi	com/reactnativecommunity/netinfo/ConnectivityReceiver.java
00096	Connect to a URL and set request method	command network	io/sentry/core/transport/HttpTransport.java

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://accessnow-api-app.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/578029664899/namespaces/firebase:fetch?key=AlzaSyDFpdSXhSDu5Idb4QHJGhqSUIWX629ZpBw. This is indicated by the response: {'state': 'NO_TEMPLATE'}

🔗 ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	10/25	android.permission.INTERNET, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	6/44	android.permission.CALL_PHONE, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.ACTIVITY_RECOGNITION

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
github.com	ok	IP: 140.82.112.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
play.google.com	ok	IP: 142.251.32.78 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
accessnow-api-app.firebaseio.com	ok	IP: 34.120.206.254 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map

DOMAIN	STATUS	GEOLOCATION
map.accessnow.com	ok	IP: 99.83.220.108 Country: United States of America Region: Washington City: Seattle Latitude: 47.606209 Longitude: -122.332069 View: Google Map
pinterest.com	ok	IP: 151.101.192.84 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
twitter.com	ok	IP: 104.244.42.65 Country: United States of America Region: California City: San Francisco Latitude: 37.773968 Longitude: -122.410446 View: Google Map
www.facebook.com	ok	IP: 31.13.80.36 Country: Canada Region: Ontario City: Toronto Latitude: 43.700111 Longitude: -79.416298 View: Google Map

DOMAIN	STATUS	GEOLOCATION
plus.google.com	ok	IP: 142.251.33.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

HARDCODED SECRETS

POSSIBLE SECRETS
"facebook_client_token" : "8addb3f71abc594f46c632a57edc3e29"
"firebase_database_url" : "https://accessnow-api-app.firebaseio.com"
"google_api_key" : "AlzaSyDFpdSXhSDu5Idb4QHJGhqSUIWX629ZpBw"
"google_crash_reporting_api_key" : "AlzaSyDFpdSXhSDu5Idb4QHJGhqSUIWX629ZpBw"
"google_maps_api_key" : "AlzaSyArt-NPlihVuq161xOIM0CJSEOCB78__z8"
9b8f518b086098de3d77736f9458a3d2f6f95a37
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
258EAF5-E914-47DA-95CA-C5AB0DC85B11
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
c103703e120ae8cc73c9248622f3cd1e
cc2751449a350f668590264ed76692694a80308a
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
01360240043788015936020505
c56fb7d591ba6704df047fd98f535372fea00211
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc

POSSIBLE SECRETS
470fa2b4ae81cd56ecbcdca9735803434cec591fa
49f946663a8deb7054212b8adda248c6

PLAYSTORE INFORMATION

Title: AccessNow

Score: 3.5 **Installs:** 5,000+ **Price:** 0 **Android Version Support:** **Category:** Maps & Navigation **Play Store URL:** [com.accessnow.app](https://play.google.com/store/apps/details?id=com.accessnow.app)

Developer Details: AccessNow, AccessNow, None, <http://accessnow.ca>, hello@accessnow.me,

Release Date: Sep 23, 2019 **Privacy Policy:** [Privacy link](#)

Description:

AccessNow is sharing accessibility information about places around the world. Search for specific places like a restaurant, hotel or store, or browse the map to see what is nearby with the accessibility features you require. If info isn't already on our map, you can add it yourself and contribute to our worldwide community. Filter the map by category and tags and find the access that you need now.

SCAN LOGS

Timestamp	Event	Error
2024-11-17 23:34:11	Generating Hashes	OK
2024-11-17 23:34:11	Extracting APK	OK

2024-11-17 23:34:11	Unzipping	OK
2024-11-17 23:34:11	Getting Hardcoded Certificates/Keystores	OK
2024-11-17 23:34:11	Parsing APK with androguard	OK
2024-11-17 23:34:13	Parsing AndroidManifest.xml	OK
2024-11-17 23:34:13	Extracting Manifest Data	OK
2024-11-17 23:34:13	Performing Static Analysis on: AccessNow (com.accessnow.app)	OK
2024-11-17 23:34:13	Fetching Details from Play Store: com.accessnow.app	OK
2024-11-17 23:34:14	Manifest Analysis Started	OK
2024-11-17 23:34:14	Reading Network Security config from network_security_config.xml	OK
2024-11-17 23:34:14	Parsing Network Security config	OK
2024-11-17 23:34:14	Checking for Malware Permissions	OK

2024-11-17 23:34:14	Fetching icon path	OK
2024-11-17 23:34:14	Library Binary Analysis Started	OK
2024-11-17 23:34:14	Reading Code Signing Certificate	OK
2024-11-17 23:34:15	Running APKID 2.1.5	OK
2024-11-17 23:34:20	Updating Trackers Database....	OK
2024-11-17 23:34:20	Detecting Trackers	OK
2024-11-17 23:34:23	Decompiling APK to Java with JADX	OK
2024-11-17 23:34:38	Converting DEX to Smali	OK
2024-11-17 23:34:38	Code Analysis Started on - java_source	OK
2024-11-17 23:34:42	Android SAST Completed	OK
2024-11-17 23:34:42	Android API Analysis Started	OK

2024-11-17 23:34:44	Android API Analysis Completed	OK
2024-11-17 23:34:44	Android Permission Mapping Started	OK
2024-11-17 23:34:49	Android Permission Mapping Completed	OK
2024-11-17 23:34:50	Email and URL Extraction Completed	OK
2024-11-17 23:34:50	Android Behaviour Analysis Started	OK
2024-11-17 23:34:52	Android Behaviour Analysis Completed	OK
2024-11-17 23:34:52	Extracting String data from APK	OK
2024-11-17 23:34:52	Extracting String data from Code	OK
2024-11-17 23:34:52	Extracting String values and entropies from Code	OK
2024-11-17 23:34:54	Performing Malware check on extracted domains	OK
2024-11-17 23:34:56	Saving to Database	OK

Report Generated by - MobSF v4.1.9

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.

© 2024 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).