ANDROID STATIC ANALYSIS REPORT

🤖 REALTOR.ca (2.1.0)

File Name:	ca.crea.realtor.apk
Package Name:	ca.crea.realtor
Scan Date:	May 4, 2025, 7:50 p.m.
App Security Score:	**40/100 (MEDIUM RISK)**
Grade:	**B**
Trackers Detection:	9/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
5	13	1	1	1

FILE INFORMATION

File Name: ca.crea.realtor.apk
Size: 18.59MB
MD5: 5f842f40202fa048558b4503730de9c8
SHA1: ac1417d0cfa4ee5e5a00c2adbe0c8cccb9253b2b
SHA256: 28b2476693969105dd13942b7b3c969f56cbae9235f6ba054f98b716b0c89fef

APP INFORMATION

App Name: REALTOR.ca
Package Name: ca.crea.realtor
Main Activity: ca.crea.realtor.activities.LoadingActivity
Target SDK: 22
Min SDK: 15
Max SDK:
Android Version Name: 2.1.0

Android Version Code: 2051

◫ APP COMPONENTS

Activities: 24
Services: 0
Receivers: 0
Providers: 0
Exported Activities: 3
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

✸ CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: C=ca, ST=ontario, L=toronto, O=indusblue, OU=indusblue, CN=benjaminmoss
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-02-08 17:54:47+00:00
Valid To: 2039-06-26 17:54:47+00:00
Issuer: C=ca, ST=ontario, L=toronto, O=indusblue, OU=indusblue, CN=benjaminmoss
Serial Number: 0x4f32b6e7
Hash Algorithm: sha1
md5: 955fc5981a10a402b5003d62b0f75509
sha1: 5a8d63d8a63197b85c66802a7478ddf50e2c6266
sha256: 7eadc3a10e4fa5907d1a4fc6e90b98ddb23c3ff9061460ae8d90887364c80ff1
sha512: 149684a97e84ddcaed408f188db321bad614a46bb124b15e3f5b5a7e120c349d77cfbf74f8e09763bc7d3b1052193ab90f59e218514708968cace1fab579761f
Found 1 unique certificates

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.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.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.

🔍 APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><td>FINDINGS</td><td>DETAILS</td></tr><tr><td>Anti-VM Code</td><td>Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible Build.SERIAL check Build.TAGS check network operator name check possible VM check</td></tr><tr><td>Compiler</td><td>dx</td></tr></table>

FILE	DETAILS
classes2.dex	**FINDINGS** / **DETAILS** table below

FINDINGS	DETAILS
Anti-VM Code	Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check possible Build.SERIAL check
Compiler	dx

🔒 NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

📇 CERTIFICATE ANALYSIS

HIGH: **2** | WARNING: **0** | INFO: **1**

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

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	high	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.
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

🔍 MANIFEST ANALYSIS

HIGH: **1** | WARNING: **3** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 4.0.3-4.0.4, [minSdk=15]	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	Activity (com.foresee.sdk.tracker.app.SurveyInviteActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
3	Activity (com.foresee.sdk.tracker.app.OnExitSurveyInviteActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Activity (com.foresee.sdk.tracker.app.SurveyActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.

</> CODE ANALYSIS

HIGH: **1** | WARNING: **9** | INFO: **1** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	ca/crea/realtor/activities/BaseActivity.java ca/crea/realtor/fragments/MortgageAmortizationFragment.java ch/qos/logback/core/android/CommonPathUtil.java com/afollestad/materialdialogs/folderselector/FileChooserDialog.java com/afollestad/materialdialogs/folderselector/FolderChooserDialog.java crittercism/android/bn.java net/hockeyapp/android/Constants.java net/hockeyapp/android/tasks/DownloadFileTask.java
				antistatic/spinnerwheel/WheelHorizontalView.java antistatic/spinnerwheel/adapters/AbstractWheelTextAdapter.java bolts/MeasurementEvent.java ca/crea/creaservice/core/Database/DatabaseUtils.java ca/crea/creaservice/core/analytics/BaseAnalyticsRequest.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ca/crea/creaservice/core/requests/BaseRequest.java
				ca/crea/realtor/activities/BaseActivity.java
				ca/crea/realtor/activities/DemographicsActivity.java
				ca/crea/realtor/activities/ListedPropertiesActivity.java
				ca/crea/realtor/activities/LoadingActivity.java
				ca/crea/realtor/activities/PreferencesDetailsActivity.java
				ca/crea/realtor/activities/PropertyTourActivity.java
				ca/crea/realtor/activities/SavedSearchActivity.java
				ca/crea/realtor/activities/SearchListingsActivity.java
				ca/crea/realtor/activities/SearchOfficesResultsActivity.java
				ca/crea/realtor/activities/SearchRealtorsActivity.java
				ca/crea/realtor/adapters/ListingAdapter.java
				ca/crea/realtor/fragments/AutoCompleteResultsFragment.java
				ca/crea/realtor/fragments/EmailFriendFragment.java
				ca/crea/realtor/fragments/EmailRealtorFragment.java
				ca/crea/realtor/fragments/HomeFragment.java
				ca/crea/realtor/fragments/OfficeDetailsFragment.java
				ca/crea/realtor/fragments/PlacesAutoCompleteFragment.java
				ca/crea/realtor/fragments/PreferencesSearchFilterFragment.java
				ca/crea/realtor/fragments/PropertyDetailsFragment.java
				ca/crea/realtor/fragments/SearchFilterFragment.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ca/crea/realtor/fragments/SearchListingResultsListFragment.java
				ca/crea/realtor/fragments/SearchMapFragment.java
				ca/crea/realtor/utils/CREAUtils.java
				ca/crea/realtor/views/MeasuredImageView.java
				ch/qos/logback/classic/android/LogcatAppender.java
				ch/qos/logback/classic/pattern/TargetLengthBasedClassNameAbbreviator.java
				ch/qos/logback/classic/spi/ThrowableProxy.java
				ch/qos/logback/core/joran/util/ConfigurationWatchListUtil.java
				ch/qos/logback/core/property/FileExistsPropertyDefiner.java
				ch/qos/logback/core/recovery/ResilientOutputStreamBase.java
				ch/qos/logback/core/sift/AppenderTrackerImpl.java
				ch/qos/logback/core/spi/ContextAwareBase.java
				ch/qos/logback/core/spi/ContextAwareImpl.java
				ch/qos/logback/core/subst/Node.java
				com/comscore/analytics/Core.java
				com/comscore/applications/KeepAlive.java
				com/comscore/measurement/MeasurementDispatcher.java
				com/comscore/metrics/Request.java
				com/comscore/streaming/StreamSense.java
				com/comscore/streaming/StreamSensePlaylist.java
				com/comscore/streaming/StreamSenseVideoView.java
				com/comscore/streaming/d.java
				com/comscore/streaming/m.java
				com/comscore/streaming/plugin/StreamSensePlugin.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/comscore/utils/CSLog.java com/comscore/utils/CacheFlusher.java com/comscore/utils/Connectivity.java com/comscore/utils/ConnectivityChangeReceiver.java com/comscore/utils/CustomExceptionHandler.java com/comscore/utils/DispatchQueue.java com/comscore/utils/FileUtils.java com/comscore/utils/InstallReferrerReceiver.java com/comscore/utils/OfflineMeasurementsCache.java com/comscore/utils/Utils.java com/comscore/utils/task/TaskExecutor.java com/comscore/utils/task/a.java com/echo/holographlibrary/BarGraph.java com/echo/holographlibrary/PieGraph.java com/foresee/mobileReplay/MobileReplayModule.java com/foresee/mobileReplay/data/BandwidthMonitorImpl.java com/foresee/mobileReplay/data/CapacityMonitorImpl.java com/foresee/mobileReplay/data/FileSystemHelper.java com/foresee/mobileReplay/data/SessionRepositoryImpl.java com/foresee/mobileReplay/http/AbstractRestServiceClient.java com/foresee/mobileReplay/http/AsyncHttpRequest.java com/foresee/mobileReplay/http/BlacklistCheck.java com/foresee/mobileReplay/http/FsServiceClientImpl.java com/foresee/mobileReplay/http/HttpPostClient.java com/foresee/mobileReplay/imageDiff/DefaultDiffingParamStrategy.java

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	com/foresee/mobileReplay/jobQueue/DeactivateRecordingJob.java com/foresee/mobileReplay/jobQueue/DeleteSessionJob.java com/foresee/mobileReplay/jobQueue/EndSessionJob.java com/foresee/mobileReplay/jobQueue/ImageDiffJob.java com/foresee/mobileReplay/jobQueue/ImageJob.java com/foresee/mobileReplay/jobQueue/JobQueueServiceImpl.java com/foresee/mobileReplay/jobQueue/SubmitSessionJob.java com/foresee/mobileReplay/perfLog/PerfDbContentProvider.java com/foresee/mobileReplay/perfLog/PerfLoggerLogCatImpl.java com/foresee/mobileReplay/perfLog/PerfLoggerSqliteImpl.java com/foresee/mobileReplay/receivers/ConnectivityChangeEventReceiver.java com/foresee/mobileReplay/recorder/FSWebViewClient.java com/foresee/mobileReplay/recorder/HierarchyWalker.java com/foresee/mobileReplay/recorder/LayoutAwareCaptureStrategy.java com/foresee/mobileReplay/recorder/Mask.java com/foresee/mobileReplay/recorder/ScheduledCaptureStrategy.java com/foresee/mobileReplay/recorder/ScheduledHandsOnCaptureStrategy.java com/foresee/mobileReplay/recorder/ScheduledTouchSensitiveCaptureStrategy.java com/foresee/mobileReplay/recorder/ScreenRecorder.java com/foresee/mobileReplay/recorder/ThreadSafeCaptureStateProxy.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/foresee/mobileReplay/recorder/ViewCaptureRunnable.java com/foresee/mobileReplay/recorder/WebViewMask.java com/foresee/mobileReplay/recorder/WebViewMaskingInterface.java com/foresee/mobileReplay/recorder/WebViewRegistryImpl.java com/foresee/mobileReplay/session/AbstractReplaySessionState.java com/foresee/mobileReplay/session/AwaitingBlacklistCheck.java com/foresee/mobileReplay/session/Paused.java com/foresee/mobileReplay/session/SessionManager.java com/foresee/mobileReplay/tasks/CaptureSubmissionTask.java com/foresee/mobileReplay/tasks/EventSubmissionTask.java com/foresee/mobileReplay/touchTracking/InterceptView.java com/foresee/mobileReplay/util/LogUtil.java com/foresee/sdk/ForeSee.java com/foresee/sdk/configuration/BaseConfigurationLoader.java com/foresee/sdk/configuration/Configuration.java com/foresee/sdk/events/EventSubscriberImpl.java com/foresee/sdk/internal/ForeSeeFacade.java com/foresee/sdk/stateTracking/StateManager.java com/foresee/sdk/tracker/PersistedState.java com/foresee/sdk/tracker/TrackingContext.java com/foresee/sdk/tracker/app/DefaultTrackerLogger.java com/foresee/sdk/tracker/app/OnExitSurveyI

NO	ISSUE	SEVERITY	STANDARDS	FILES FOLDER
				nviteActivity.java com/foresee/sdk/tracker/app/SurveyActivity.java com/foresee/sdk/tracker/layouts/InviteViewParams.java com/foresee/sdk/tracker/tasks/HttpGetAsyncTask.java com/h6ah4i/android/widget/advrecyclerview/animator/GeneralItemAnimator.java com/h6ah4i/android/widget/advrecyclerview/animator/impl/ItemAddAnimationManager.java com/h6ah4i/android/widget/advrecyclerview/animator/impl/ItemChangeAnimationManager.java com/h6ah4i/android/widget/advrecyclerview/animator/impl/ItemMoveAnimationManager.java com/h6ah4i/android/widget/advrecyclerview/animator/impl/ItemRemoveAnimationManager.java com/h6ah4i/android/widget/advrecyclerview/draggable/DraggableItemWrapperAdapter.java com/h6ah4i/android/widget/advrecyclerview/swipeable/ItemSlidingAnimator.java com/j256/ormlite/android/AndroidLog.java com/j256/ormlite/android/apptools/OrmLiteConfigUtil.java com/j256/ormlite/logger/LocalLog.java com/nineoldandroids/animation/PropertyValuesHolder.java com/plasticmobile/joomo/api/APIManager.java com/plasticmobile/joomo/api/APIRequest.java com/plasticmobile/joomo/location/LocationManager.java com/plasticmobile/joomo/location/LocationUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/plasticmobile/joomo/parser/JsonParser.java com/plasticmobile/joomo/parser/ModelParser.java com/plasticmobile/joomo/utils/LogUtility.java com/touchimageview/TouchImageView.java com/viewpagerindicator/CirclePageIndicator.java crittercism/android/Cdo.java crittercism/android/d.java crittercism/android/h.java me/zhanghai/android/materialprogressbar/MaterialProgressBar.java net/hockeyapp/android/Constants.java net/hockeyapp/android/CrashManager.java net/hockeyapp/android/ExceptionHandler.java net/hockeyapp/android/FeedbackActivity.java net/hockeyapp/android/FeedbackManager.java net/hockeyapp/android/PaintActivity.java net/hockeyapp/android/tasks/AttachmentDownloader.java net/hockeyapp/android/tasks/CheckUpdateTaskWithUI.java net/hockeyapp/android/views/PaintView.java net/sf/cglib/core/DebuggingClassWriter.java net/sf/cglib/reflect/FastMethod.java org/aopalliance/aop/AspectException.java org/slf4j/helpers/MessageFormatter.java org/slf4j/helpers/Util.java roboguice/util/Ln.java roboguice/util/SafeAsyncTask.java uk/co/senab/photoview/PhotoViewAttacher.java uk/co/senab/photoview/log/LoggerDefault.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	bolts/MeasurementEvent.java ch/qos/logback/classic/ClassicConstants.java ch/qos/logback/classic/joran/action/ConfigurationAction.java ch/qos/logback/classic/sift/ContextBasedDiscriminator.java ch/qos/logback/core/CoreConstants.java ch/qos/logback/core/rolling/helper/DateTokenConverter.java ch/qos/logback/core/rolling/helper/IntegerTokenConverter.java com/comscore/streaming/Constants.java com/comscore/utils/Constants.java com/comscore/utils/InstallReferrerReceiver.java com/comscore/utils/Storage.java com/foresee/mobileReplay/Keys.java com/foresee/mobileReplay/data/BandwidthMonitorImpl.java com/foresee/mobileReplay/domain/SessionGroup.java com/foresee/sdk/tracker/QueryStringKeys.java com/foresee/sdk/tracker/URLConstructor.java com/foresee/sdk/tracker/app/TrackerLoader.java com/foresee/sdk/tracker/util/FsrSettings.java net/hockeyapp/android/CrashManager.java net/hockeyapp/android/LoginManager.java net/hockeyapp/android/Tracking.java net/hockeyapp/android/utils/VersionCache.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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/foresee/mobileReplay/perfLog/PerfDb.java com/j256/ormlite/android/AndroidCompiledStatement.java com/j256/ormlite/android/AndroidDatabaseConnection.java com/j256/ormlite/android/compat/ApiCompatibility.java com/j256/ormlite/android/compat/BasicApiCompatibility.java com/j256/ormlite/android/compat/JellyBeanApiCompatibility.java
5	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	net/sf/cglib/transform/AbstractTransformTask.java
6	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/foresee/sdk/tracker/services/ExitSurveyServiceClientImpl.java net/hockeyapp/android/utils/SimpleMultipartEntity.java
7	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/comscore/android/id/IdHelperAndroid.java com/comscore/utils/Utils.java net/hockeyapp/android/LoginActivity.java roboguice/util/Strings.java
8	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/comscore/applications/AppStartMeasurement.java com/comscore/utils/RootDetector.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	bolts/WebViewAppLinkResolver.java ca/crea/realtor/utils/LandTransferTaxUtils.java com/foresee/mobileReplay/recorder/WebViewRegistryImpl.java com/foresee/sdk/tracker/app/SurveyActivity.java
10	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	ca/crea/realtor/fragments/MyStuffFragment.java com/plasticmobile/joomo/security/Signature.java
11	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/afollestad/materialdialogs/BuildConfig.java com/afollestad/materialdialogs/commons/BuildConfig.java
12	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/plasticmobile/joomo/security/AES256Encrypt.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00054	Install other APKs from file	reflection	net/hockeyapp/android/tasks/DownloadFileTask.java net/hockeyapp/android/views/AttachmentView.java
00022	Open a file from given absolute path of the file	file	ch/qos/logback/core/FileAppender.java ch/qos/logback/core/property/FileExistsPropertyDefiner.java ch/qos/logback/core/rolling/helper/Compressor.java ch/qos/logback/core/rolling/helper/RenameUtil.java com/afollestad/materialdialogs/folderselector/FileChooserDialog.java com/afollestad/materialdialogs/folderselector/FolderChooserDialog.java com/crittercism/app/CrittercismNDK.java com/j256/ormlite/android/apptools/OrmLiteConfigUtil.java crittercism/android/bi.java crittercism/android/cy.java crittercism/android/dr.java crittercism/android/ec.java crittercism/android/i.java net/hockeyapp/android/Constants.java net/hockeyapp/android/FeedbackManager.java net/hockeyapp/android/tasks/DownloadFileTask.java net/hockeyapp/android/utils/ImageUtils.java net/sf/cglib/transform/AbstractProcessTask.java net/sf/cglib/transform/AbstractTransformTask.java
00072	Write HTTP input stream into a file	command network file	net/hockeyapp/android/tasks/AttachmentDownloader.java net/hockeyapp/android/tasks/DownloadFileTask.java
00089	Connect to a URL and receive input stream from the server	command network	bolts/WebViewAppLinkResolver.java net/hockeyapp/android/tasks/AttachmentDownloader.java net/hockeyapp/android/tasks/DownloadFileTask.java
00030	Connect to the remote server through the given URL	network	bolts/WebViewAppLinkResolver.java net/hockeyapp/android/tasks/AttachmentDownloader.java net/hockeyapp/android/tasks/DownloadFileTask.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	bolts/WebViewAppLinkResolver.java com/comscore/metrics/Request.java crittercism/android/h.java net/hockeyapp/android/tasks/DownloadFileTask.java
00094	Connect to a URL and read data from it	command network	bolts/WebViewAppLinkResolver.java ch/qos/logback/core/util/FileUtil.java net/hockeyapp/android/tasks/AttachmentDownloader.java net/hockeyapp/android/tasks/DownloadFileTask.java
00108	Read the input stream from given URL	network command	bolts/WebViewAppLinkResolver.java crittercism/android/db.java net/hockeyapp/android/tasks/AttachmentDownloader.java net/hockeyapp/android/tasks/DownloadFileTask.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	bolts/AppLinkNavigation.java bolts/AppLinks.java bolts/MeasurementEvent.java ca/crea/realtor/activities/BaseActivity.java ca/crea/realtor/activities/PropertyTourActivity.java ca/crea/realtor/fragments/RealtorDetailsFragment.java ca/crea/realtor/utils/CREAUtils.java ca/crea/realtor/utils/DialogRateApp.java ca/crea/realtor/utils/DialogSharingAppOptions.java ca/crea/realtor/views/OfficeDetailsHeaderView.java ca/crea/realtor/views/RowRealtorView.java com/foresee/sdk/tracker/app/SurveyActivity.java com/plasticmobile/joomo/utils/Utils.java crittercism/android/ap.java net/hockeyapp/android/FeedbackActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	bolts/AppLinkNavigation.java bolts/MeasurementEvent.java ca/crea/realtor/utils/CREAUtils.java ca/crea/realtor/utils/DialogRateApp.java com/plasticmobile/joomo/utils/Utils.java crittercism/android/ap.java
00091	Retrieve data from broadcast	collection	ca/crea/realtor/activities/ListedPropertiesActivity.java net/hockeyapp/android/FeedbackActivity.java net/hockeyapp/android/LoginActivity.java net/hockeyapp/android/PaintActivity.java
00013	Read file and put it into a stream	file	ch/qos/logback/core/joran/GenericConfigurator.java ch/qos/logback/core/joran/action/PropertyAction.java ch/qos/logback/core/rolling/helper/Compressor.java ch/qos/logback/core/rolling/helper/RenameUtil.java com/foresee/mobileReplay/data/CapacityMonitorImpl.java com/foresee/mobileReplay/data/SessionRepositoryImpl.java com/j256/ormlite/android/apptools/OrmLiteSqliteOpenHelper.java crittercism/android/bt.java crittercism/android/dr.java net/hockeyapp/android/utils/ImageUtils.java net/hockeyapp/android/utils/SimpleMultipartEntity.java net/sf/cglib/transform/AbstractTransformTask.java org/simpleframework/xml/core/Persister.java
00012	Read data and put it into a buffer stream	file	ch/qos/logback/core/rolling/helper/Compressor.java ch/qos/logback/core/rolling/helper/RenameUtil.java net/sf/cglib/transform/AbstractTransformTask.java
00014	Read file into a stream and put it into a JSON object	file	crittercism/android/bt.java

RULE ID	BEHAVIOUR	LABEL	FILES
00004	Get filename and put it to JSON object	file collection	crittercism/android/bt.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	bolts/AppLinkNavigation.java ca/crea/realtor/fragments/RealtorDetailsFragment.java ca/crea/realtor/utils/CREAUtils.java ca/crea/realtor/views/OfficeDetailsHeaderView.java com/plasticmobile/joomo/utils/Utils.java crittercism/android/ap.java
00147	Get the time of current location	collection location	com/plasticmobile/joomo/location/LocationUtils.java
00189	Get the content of a SMS message	sms	ca/crea/realtor/utils/CREAUtils.java
00188	Get the address of a SMS message	sms	ca/crea/realtor/utils/CREAUtils.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	ca/crea/realtor/utils/CREAUtils.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	ca/crea/realtor/utils/CREAUtils.java
00191	Get messages in the SMS inbox	sms	ca/crea/realtor/utils/CREAUtils.java
00200	Query data from the contact list	collection contact	ca/crea/realtor/utils/CREAUtils.java
00187	Query a URI and check the result	collection sms calllog calendar	ca/crea/realtor/utils/CREAUtils.java
00112	Get the date of the calendar event	collection calendar	ca/crea/realtor/utils/CREAUtils.java
00201	Query data from the call log	collection calllog	ca/crea/realtor/utils/CREAUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	ca/crea/realtor/utils/CREAUtils.java
00202	Make a phone call	control	ca/crea/realtor/fragments/RealtorDetailsFragment.java ca/crea/realtor/views/OfficeDetailsHeaderView.java
00203	Put a phone number into an intent	control	ca/crea/realtor/fragments/RealtorDetailsFragment.java ca/crea/realtor/views/OfficeDetailsHeaderView.java
00029	Initialize class object dynamically	reflection	net/sf/cglib/core/ReflectUtils.java net/sf/cglib/reflect/FastClass.java
00157	Instantiate new object using reflection, possibly used for dexClassLoader	reflection dexClassLoader	net/sf/cglib/core/ReflectUtils.java net/sf/cglib/reflect/FastClass.java
00046	Method reflection	reflection	net/sf/cglib/core/ReflectUtils.java
00125	Check if the given file path exist	file	ca/crea/realtor/activities/LoadingActivity.java net/hockeyapp/android/FeedbackManager.java net/hockeyapp/android/PaintActivity.java
00078	Get the network operator name	collection telephony	crittercism/android/bn.java
00123	Save the response to JSON after connecting to the remote server	network command	bolts/WebViewAppLinkResolver.java
00128	Query user account information	collection account	ca/crea/realtor/utils/DialogSharingAppOptions.java
00130	Get the current WIFI information	wifi collection	com/comscore/utils/Connectivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	crittercism/android/cu.java crittercism/android/h.java
00104	Check if the given path is directory	file	com/afollestad/materialdialogs/folderselector/FolderChooserDialog.java
00121	Create a directory	file command	net/hockeyapp/android/Constants.java

⠿ ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/25	android.permission.GET_ACCOUNTS, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.READ_CONTACTS, android.permission.ACCESS_WIFI_STATE
Other Common Permissions	2/44	android.permission.CALL_PHONE, android.permission.WRITE_CONTACTS

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
replaycontroller.4seeresults.com	ok	**IP:** 18.64.141.32 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.slf4j.org	ok	**IP:** 195.15.222.169 **Country:** Switzerland **Region:** Basel-Stadt **City:** Basel **Latitude:** 47.558399 **Longitude:** 7.573270 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xml.org	ok	**IP:** 104.239.142.8 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
logback.qos.ch	ok	**IP:** 159.100.250.151 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map
www.crea.ca	ok	**IP:** 146.190.244.100 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.530769 **Longitude:** -122.684448 **View:** Google Map
mindprod.com	ok	**IP:** 65.110.21.43 **Country:** Canada **Region:** British Columbia **City:** Vancouver **Latitude:** 49.281139 **Longitude:** -123.125877 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sb.scorecardresearch.com	ok	**IP:** 18.64.141.39 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
maps.google.com	ok	**IP:** 216.58.209.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
realtor.ca	ok	**IP:** 45.223.28.18 **Country:** United States of America **Region:** Colorado **City:** Greenwood Village **Latitude:** 39.617210 **Longitude:** -104.950813 **View:** Google Map
developers.facebook.com	ok	**IP:** 157.240.227.1 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
survey.foreseeresults.com	ok	**IP:** 3.161.104.47 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
events.foreseeresults.com	ok	**IP:** 3.161.104.102 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
maps.googleapis.com	ok	**IP:** 172.217.169.234 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
cdn.konfigapps.com	ok	No Geolocation information available.
sdk.hockeyapp.net	ok	**IP:** 40.70.164.17 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
udm.scorecardresearch.com	ok	**IP:** 3.161.104.2 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.amazon.com	ok	**IP:** 18.64.139.19 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.howrealtorshelp.ca	ok	**IP:** 40.123.47.58 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
1sapi.realtor.ca	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
b.scorecardresearch.com	ok	**IP:** 18.64.141.107 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
play.google.com	ok	**IP:** 142.250.201.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.walkscore.com	ok	**IP:** 142.250.181.179 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
twitter.com	ok	**IP:** 162.159.140.229 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

✉ EMAILS

EMAIL	FILE
support@crittercism.com	crittercism/android/ap.java
support@crittercism.com	com/crittercism/app/Crittercism.java
omar@plasticmobile.com or@plasticmobile.com	ca/crea/realtor/activities/BaseActivity.java
info@crea.ca	Android String Resource

🕵 TRACKERS

TRACKER	CATEGORIES	URL
Apteligent by VMWare (formerly Crittercism)		https://reports.exodus-privacy.eu.org/trackers/155
ComScore	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/56
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
Foresee	Analytics	https://reports.exodus-privacy.eu.org/trackers/149

TRACKER	CATEGORIES	URL
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105
HockeyApp	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/26

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"api_url" : "https://%1$sapi.realtor.ca/"
"api_url_http" : "http://%1$sapi.realtor.ca/"
"map_key" : "AIzaSyBQtE-zY1IoGtnyRyI56OVlwGuysBgJjkA"
"walk_score_key" : "ccab95c6ff1a1e101a1b9415d6e9f21e"
"youtube_player_key" : "AIzaSyABpjxIPxroiXlldnP0RbhMjpgch-Vv7Is"
0po0eytBzXme4duX0wiNX/MVxDGsOqAJA730GSsf2qU=
TKBnk6LsB/ztAHRKvOeqGVGHZcMq6c3VMIHqT+CIUCi3sat+eOhprUGEP43nGUti
1d30e2ca9adf559cba0d4af978655e95
5e8f16062ea3cd2c4a0d547876baa6f38cabf625

POSSIBLE SECRETS

SCirxCsFnDuwhNtITKQnfRWkNU6Q48eYcFxC37zR/rFFt2Tk535ut0aEwjgfj82K

5bVOp06Hzzf1wRchGC7JFKwDQFmKZBAMg9MmSmriiHc=

n2rmeKncQljdfBWnzypfsBgBVyre25Oaf6mn3QuNt5cQq7Xuaz3ZLuwmSTWxVzSQ

UlNrSUzyNQumjidHbyZmRamtp5eoPFvIeOwCo75MZksEyM6MMFg9gB6StAom9i00

6WjNkzIcCej8zG38Dh8uDdR8qxTeSY+F1EiowOLK0wqRSLiB7V6ZBEIW+z9XZ42z

NesWObNQJNwKtKC/NJD4K2vucrUuBYYlSiEnsLynoAw=

M3kRYlbLM9AydEhjx8lHSiSaDFH5NR8G6REmAWXbKM4=

hgCk8A4GQuleIlan21Er1535C3f4u3krghh5apIgsmw=

zXEwIzFN2SQaspV7iUirgyM8TI24BPO4ou3gjDg/chwmfbGE7kNKw8hZdBYzOnei

0136024004378801593602050

cjnl/tiDXvXrtfGWc6LdSVteaLdg9l49I4W5cfDIAhk=

SWJLGN5L6BF17klOXqOOpLP1xZAAM7Ng4jaTvXX9WY6PxRvldWXn1ENx7nHyTu84

4Yvi2n8BAkvE7VNBUElC3KZ0iuxbd5Z1l2yzQlO6iwr52KJ2qUcHr9aFTvQu+1Bz

P9Jrh/MxY+mhIP2GCt+FgNMwXo7cFnfTZwH6N5TxOR0=

3i2ndDfv2rTHiSisAbouNdArYfORhtTPEefj3q2f

POSSIBLE SECRETS

EaedvdYjGg60ZzpcKZqlpv9uw+zeAITd9onB2Q+u/DrbDRBeDmCL+IWET7OkGK9k

dWxlbXXBia4+kOf2ZonlBC9dp9hsDGLu+zzk8Y1C7Nc=

a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc

UfnmQ+YR85XZtQcjqL0gfNNqtZZWbeI/ADuaO9S0mxc=

5rpjrNDZLB7091vQKnpPAsEnQ56LZqAytHXDmTZuN8s=

8a3c4b262d721acd49a4bf97d5213199c86fa2b9

3VC4GsgbeokcqH9dWJc7GlTz7GbPB4R6Jvt33jUYc+U=

F2cmMww6lSTtMiqkoX/Czfb090kW53GPnMxNR6fKBurckyDBc8rt+tixGr7EJ0aF

:☰ SCAN LOGS

Timestamp	Event	Error
2025-05-04 19:50:11	Generating Hashes	OK
2025-05-04 19:50:11	Extracting APK	OK

2025-05-04 19:50:11	Unzipping	OK
2025-05-04 19:50:11	Parsing APK with androguard	OK
2025-05-04 19:50:11	Extracting APK features using aapt/aapt2	OK
2025-05-04 19:50:11	Getting Hardcoded Certificates/Keystores	OK
2025-05-04 19:50:17	Parsing AndroidManifest.xml	OK
2025-05-04 19:50:17	Extracting Manifest Data	OK
2025-05-04 19:50:17	Manifest Analysis Started	OK
2025-05-04 19:50:17	Performing Static Analysis on: REALTOR.ca (ca.crea.realtor)	OK
2025-05-04 19:50:17	Fetching Details from Play Store: ca.crea.realtor	OK
2025-05-04 19:50:18	Checking for Malware Permissions	OK
2025-05-04 19:50:18	Fetching icon path	OK

2025-05-04 19:50:18	Library Binary Analysis Started	OK
2025-05-04 19:50:18	Reading Code Signing Certificate	OK
2025-05-04 19:50:19	Running APKiD 2.1.5	OK
2025-05-04 19:50:24	Detecting Trackers	OK
2025-05-04 19:50:26	Decompiling APK to Java with JADX	OK
2025-05-04 19:51:15	Converting DEX to Smali	OK
2025-05-04 19:51:15	Code Analysis Started on - java_source	OK
2025-05-04 19:51:19	Android SBOM Analysis Completed	OK
2025-05-04 19:51:30	Android SAST Completed	OK
2025-05-04 19:51:30	Android API Analysis Started	OK
2025-05-04 19:51:38	Android API Analysis Completed	OK

2025-05-04 19:51:39	Android Permission Mapping Started	OK
2025-05-04 19:51:42	Android Permission Mapping Completed	OK
2025-05-04 19:51:43	Android Behaviour Analysis Started	OK
2025-05-04 19:51:49	Android Behaviour Analysis Completed	OK
2025-05-04 19:51:49	Extracting Emails and URLs from Source Code	OK
2025-05-04 19:51:51	Email and URL Extraction Completed	OK
2025-05-04 19:51:51	Extracting String data from APK	OK
2025-05-04 19:51:51	Extracting String data from Code	OK
2025-05-04 19:51:51	Extracting String values and entropies from Code	OK
2025-05-04 19:51:53	Performing Malware check on extracted domains	OK
2025-05-04 19:52:02	Saving to Database	OK

Report Generated by - MobSF v4.3.2

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.