MOBSF

ANDROID STATIC ANALYSIS REPORT

Kare (1.5.42)

File Name:	com.kareheroes_172.apk
Package Name:	com.kareheroes
Scan Date:	Aug. 30, 2025, 10:34 p.m.
App Security Score:	48/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	28	2	2	2

FILE INFORMATION

File Name: com.kareheroes_172.apk
Size: 9.29MB
MD5: 0d2b32420a978af83fad66217a7b37ec
SHA1: 19a4d68bc842964acf70d520c62204fa91a59568
SHA256: 66decafc9926005c348588353c65ba4303c8105354b880da26e720151babdcdc

APP INFORMATION

App Name: Kare
Package Name: com.kareheroes
Main Activity: com.kareheroes.MainActivity
Target SDK: 34
Min SDK: 21
Max SDK:
Android Version Name: 1.5.42

Android Version Code: 172

APP COMPONENTS

Activities: 13
Services: 17
Receivers: 20
Providers: 6
Exported Activities: 5
Exported Services: 3
Exported Receivers: 9
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=□□, ST=□□□, L=□□□, O=□□□□, OU=□□□□□, CN=□□
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-06-14 11:00:59+00:00
Valid To: 2046-10-30 11:00:59+00:00
Issuer: C=□□, ST=□□□, L=□□□, O=□□□□, OU=□□□□□, CN=□□
Serial Number: 0x94f820e
Hash Algorithm: sha256
md5: 691452720df0eba93067a3de9ace6594
sha1: 9363176add2ba3ba1992eab43e53c5c580660464
sha256: 3045f42ec6755af8cb94706a7029ae778c69d8a953e618dfab2fc9c6d9e848da
sha512: b2e0bd094026d6f64be7efc8b760247aaf2cc58ce94df8581ef8e336314040f88a4128514ad4258603391cfc37eb2c1b75ed49a19e34a89490fabc84ce0dbfda
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: b9ea878d2d7bef0be2dda662435655f49922411d952d6d5f998a198b25a5a710
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from 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.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
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
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
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
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.kareheroes.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	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

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
SIM operator check
network operator name 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
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.com.kareheroes,

ACTIVITY	INTENT
com.kareheroes.MainActivity	Schemes: http://, https://, Hosts: kareapp.page.link,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 2 | WARNING: 18 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.0-5.0.2, [minSdk=21]	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	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	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.
4	Service (com.kareheroes.location.CCLocationService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Broadcast Receiver (com.kareheroes.location.AlarmReceiver) 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.
6	Activity (com.onesignal.NotificationOpenedActivityHMS) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Broadcast Receiver (com.onesignal.BootUpReceiver) 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.
8	Broadcast Receiver (com.onesignal.UpgradeReceiver) 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.
9	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.
10	Activity (com.google.android.gms.appinvite.PreviewActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Broadcast Receiver (com.onesignal.FCMBroadcastReceiver) 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.
12	Broadcast Receiver (com.onesignal.NotificationDismissReceiver) 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
13	Activity (com.onesignal.NotificationOpenedReceiver) 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.
14	Activity (com.onesignal.NotificationOpenedReceiverAndroid22AndOlder) 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.
15	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.
16	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.

NO	ISSUE	SEVERITY	DESCRIPTION
17	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [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.
18	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.
19	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
20	High Intent Priority (999) - {1} Hit(s) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				b/a/k/a/a.java b/a/o/g.java b/f/e/c.java b/f/e/e.java b/f/e/f.java b/f/e/g.java b/f/e/j.java b/f/e/k.java b/f/h/b.java b/f/j/a.java b/f/k/a0.java b/f/k/b.java b/f/k/f0.java b/f/k/g.java b/f/k/g0/b.java b/f/k/i.java b/f/k/x.java b/f/k/y.java b/h/b/a.java b/k/a/a.java b/l/a/b.java b/l/b/c.java b/m/a/a.java b/n/a/c.java b/o/a/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				b/p/a.java b/q/a/a/i.java b/r/a/b.java co/apptailor/googlesignin/RNGoogleSigninModule.java co/apptailor/googlesignin/b.java com/geektime/rnonesignalandroid/RNOneSignal.java com/kareheroes/MainActivity.java com/kareheroes/location/AlarmReceiver.java com/kareheroes/location/CCLocationService.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/c.java com/learnium/RNDeviceInfo/d/a.java com/onesignal/JobIntentService.java com/onesignal/d3.java com/onesignal/g.java com/onesignal/t4/c.java com/reactnative/ivpusic/imagepicker/a.java com/reactnative/ivpusic/imagepicker/e.java com/reactnativecommunity/webview/RNCWebViewManager.java com/reactnativecommunity/webview/RNCWebViewModule.java com/rssignaturecapture/RSSignatureCaptureViewManager.java com/rssignaturecapture/a.java com/rt2zz/reactnativecontacts/a.java com/shockwave/pdfium/PdfiumCore.java com/swmansion/gesturehandler/react/g.java com/yalantis/ucrop/UCropActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/yalantis/ucrop/l/a.java com/yalantis/ucrop/l/c.java com/yalantis/ucrop/l/e.java com/yalantis/ucrop/l/f.java com/yalantis/ucrop/task/BitmapCropTask.java com/yalantis/ucrop/task/a.java com/yalantis/ucrop/view/b.java d/a/a/a/a.java d/b/a/a/e.java d/b/a/a/h.java d/b/a/a/j/a.java d/c/a/b/i/v/a.java d/c/a/d/a/a/a.java d/c/a/d/a/a/b.java d/c/a/d/a/a/c.java d/c/a/d/c/b.java d/c/a/d/c/d.java d/c/a/d/c/e.java d/c/a/d/c/i.java d/c/a/d/c/j.java d/c/a/d/c/s.java d/c/a/d/c/u.java d/c/a/d/c/v.java d/c/a/d/d/c0.java d/c/a/d/d/e.java d/c/a/d/d/e0.java d/c/a/d/d/j.java d/c/a/d/d/k.java d/c/a/d/d/m.java d/c/a/d/d/p/a.java d/c/a/d/d/u.java d/c/a/d/d/w.java d/c/a/d/e/i.java d/c/a/d/g/i/z.java d/c/a/d/g/k/a2.java d/c/a/d/g/k/j1.java d/c/a/d/g/k/k1.java d/c/a/d/g/k/l7.java d/c/a/d/g/k/na.java d/c/a/d/g/k/nc.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				d/c/a/d/g/k/oc.java d/c/a/d/g/k/s1.java d/c/a/d/g/k/v1.java d/c/a/d/g/k/x1.java d/c/a/d/g/k/y1.java d/c/a/d/h/b/a.java d/c/a/d/i/a.java d/c/d/a/c/k/m.java io/invertase/firebase/RNFirebaseModule.java io/invertase/firebase/admob/RNFirebaseAdMob.java io/invertase/firebase/analytics/RNFirebaseAnalytics.java io/invertase/firebase/auth/RNFirebaseAuth.java io/invertase/firebase/c.java io/invertase/firebase/config/RNFirebaseRemoteConfig.java io/invertase/firebase/database/RNFirebaseDatabase.java io/invertase/firebase/database/a.java io/invertase/firebase/database/b.java io/invertase/firebase/fabric/crashlytics/RNFirebaseCrashlytics.java io/invertase/firebase/firestore/RNFirebaseFirestore.java io/invertase/firebase/firestore/b.java io/invertase/firebase/firestore/d.java io/invertase/firebase/firestore/e.java io/invertase/firebase/functions/RNFirebaseFunctions.java io/invertase/firebase/instanceid/RNFirebaseInstanceId.java io/invertase/firebase/links/RNFirebaseLinks.java io/invertase/firebase/messaging/RNFirebaseMessaging.java io/invertase/firebase/notifications/R

NO	ISSUE	SEVERITY	STANDARDS	FILES
				NFirebaseNotifications.java io/invertase/firebase/notifications/a.java io/invertase/firebase/notifications/d.java io/invertase/firebase/perf/RNFirebasePerformance.java io/invertase/firebase/storage/RNFirebaseStorage.java org/wonday/orientation/a.java org/wonday/pdf/a.java
2	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/RNFetchBlob/a.java com/airbnb/android/react/maps/AirMapModule.java com/airbnb/android/react/maps/k.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnativecommunity/webview/RNCWebViewModule.java
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/geektime/rnonesignalandroid/RNOneSignal.java com/onesignal/g4.java com/onesignal/j1.java com/onesignal/q1.java com/reactnative/ivpusic/imagepicker/PickerModule.java io/invertase/firebase/functions/RNFirebaseFunctions.java io/invertase/firebase/notifications/RNFirebaseNotifications.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	com/onesignal/OSUtils.java d/c/a/d/g/k/oc.java d/c/d/a/c/k/n.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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/RNFetchBlob/Utils/a.java com/RNFetchBlob/d.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnative/ivpusic/imagepicker/a.java com/reactnative/ivpusic/imagepicker/d.java com/reactnativecommunity/webview/RNCWebViewModule.java com/rssignaturecapture/a.java com/yalantis/ucrop/l/e.java io/invertase/firebase/storage/RNFirebaseStorage.java
6	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	d/c/a/d/g/k/b2.java
7	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	com/onesignal/p4.java
8	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/onesignal/p4.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	b/n/a/g/a.java com/onesignal/k3.java com/onesignal/s4/a/k.java com/reactnativecommunity/asyncstorage/e.java d/c/a/b/i/x/j/f0.java d/c/a/b/i/x/j/h0.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/RNFetchBlob/h.java
11	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/RNFetchBlob/g.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00009	Put data in cursor to JSON object	file	com/onesignal/g0.java com/onesignal/j0.java com/onesignal/n0.java com/onesignal/s.java com/reactnativecommunity/asyncstorage/a.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/RNFetchBlob/RNFetchBlob.java com/RNFetchBlob/g.java com/onesignal/OSUtils.java com/onesignal/e0.java com/onesignal/shortcutbadger/impl/OPPOHomeBader.java com/onesignal/shortcutbadger/impl/SonyHomeBadger.java com/reactnative/ivpusic/imagepicker/PickerModule.java d/b/a/a/j/a.java io/invertase/firebase/links/RNFirebaseLinks.java io/invertase/firebase/notifications/d.java
00036	Get resource file from res/raw directory	reflection	com/airbnb/android/react/maps/e.java com/airbnb/android/react/maps/m.java com/onesignal/OSUtils.java com/onesignal/e0.java com/onesignal/shortcutbadger/impl/EverythingMeHomeBadger.java com/onesignal/shortcutbadger/impl/HuaweiHomeBadger.java com/onesignal/shortcutbadger/impl/NovaHomeBadger.java com/onesignal/shortcutbadger/impl/OPPOHomeBader.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java com/onesignal/shortcutbadger/impl/SonyHomeBadger.java io/invertase/firebase/notifications/d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	b/f/e/e.java b/f/e/k.java com/RNFetchBlob/a.java com/RNFetchBlob/d.java com/airbnb/android/react/maps/d.java com/airbnb/android/react/maps/k.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/yalantis/ucrop/l/e.java f/l.java
00024	Write file after Base64 decoding	reflection file	com/RNFetchBlob/a.java com/RNFetchBlob/d.java
00192	Get messages in the SMS inbox	sms	com/RNFetchBlob/Utils/a.java com/reactnative/ivpusic/imagepicker/d.java com/yalantis/ucrop/l/e.java io/invertase/firebase/notifications/d.java
00175	Get notification manager and cancel notifications	notification	io/invertase/firebase/notifications/d.java
00091	Retrieve data from broadcast	collection	com/onesignal/FCMBroadcastReceiver.java com/onesignal/PermissionsActivity.java com/onesignal/u1.java io/invertase/firebase/notifications/RNFirebaseNotifications.java io/invertase/firebase/notifications/b.java
00078	Get the network operator name	collection telephony	com/learnium/RNDeviceInfo/RNDeviceModule.java com/onesignal/OSUtils.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/onesignal/OSUtils.java com/onesignal/e0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00189	Get the content of a SMS message	sms	com/RNFetchBlob/Utils/a.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java com/rt2zz/reactnativecontacts/a.java
00022	Open a file from given absolute path of the file	file	b/n/a/g/b.java com/RNFetchBlob/Utils/a.java com/RNFetchBlob/d.java com/RNFetchBlob/g.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnative/ivpusic/imagepicker/d.java com/rssignaturecapture/a.java io/invertase/firebase/storage/RNFirebaseStorage.java
00188	Get the address of a SMS message	sms	com/RNFetchBlob/Utils/a.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java com/rt2zz/reactnativecontacts/a.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/RNFetchBlob/Utils/a.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java d/c/a/d/g/k/i1.java
00191	Get messages in the SMS inbox	sms	com/RNFetchBlob/Utils/a.java com/RNFetchBlob/g.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java com/reactnative/ivpusic/imagepicker/d.java
00200	Query data from the contact list	collection contact	com/RNFetchBlob/Utils/a.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java com/rt2zz/reactnativecontacts/a.java
00201	Query data from the call log	collection calllog	com/RNFetchBlob/Utils/a.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java com/rt2zz/reactnativecontacts/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/RNFetchBlob/Utils/a.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00096	Connect to a URL and set request method	command network	com/onesignal/o3.java
00089	Connect to a URL and receive input stream from the server	command network	com/onesignal/o3.java io/invertase/firebase/notifications/a.java
00109	Connect to a URL and get the response code	network command	com/onesignal/o3.java d/c/a/d/a/a/b.java
00053	Monitor data identified by a given content URI changes(SMS, MMS, etc.)	sms	d/c/a/d/g/k/i1.java
00187	Query a URI and check the result	collection sms calllog calendar	com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java com/rt2zz/reactnativecontacts/a.java d/c/a/d/g/k/i1.java d/c/a/d/g/k/j1.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00038	Query the phone number	collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00130	Get the current WIFI information	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00134	Get the current WiFi IP address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00082	Get the current WiFi MAC address	collection wifi	com/learnium/RNDeviceInfo/RNDeviceModule.java
00092	Send broadcast	command	com/onesignal/j0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	b/f/k/g0/b.java
00030	Connect to the remote server through the given URL	network	io/invertase/firebase/notifications/a.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://kare-246912.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/61228390818/namespaces/firebase:fetch?key=AIzaSyBrZAkLQ2eQCul0VfumoMuaKriRjF2NIAE. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	13/25	android.permission.CAMERA, android.permission.SYSTEM_ALERT_WINDOW, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_WIFI_STATE, android.permission.READ_CONTACTS, android.permission.WAKE_LOCK, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	4/44	android.permission.CHANGE_WIFI_STATE, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
kare-246912.firebaseio.com	ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
api.onesignal.com	ok	**IP:** 104.16.160.145 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
app-measurement.com	ok	**IP:** 142.251.40.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.250.72.130 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
goo.gl	ok	**IP:** 142.250.217.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	d/c/a/d/d/b0.java

TRACKERS

TRACKER	CATEGORIES	URL
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
OneSignal		https://reports.exodus-privacy.eu.org/trackers/193

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://kare-246912.firebaseio.com"
"google_api_key" : "AIzaSyBrZAkLQ2eQCul0VfumoMuaKriRjF2NIAE"
"google_crash_reporting_api_key" : "AIzaSyBrZAkLQ2eQCul0VfumoMuaKriRjF2NIAE"
c103703e120ae8cc73c9248622f3cd1e
c682b8144a8dd52bc1ad63
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
B3EEABB8EE11C2BE770B684D95219ECB
5e8f16062ea3cd2c4a0d547876baa6f38cabf625
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
5eb5a37e-b458-11e3-ac11-000c2940e62c
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
9b8f518b086098de3d77736f9458a3d2f6f95a37

POSSIBLE SECRETS
49f946663a8deb7054212b8adda248c6
b2f7f966-d8cc-11e4-bed1-df8f05be55ba
cc2751449a350f668590264ed76692694a80308a

PLAYSTORE INFORMATION

Title: KARE Heroes

Score: 3.26 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.kareheroes

Developer Details: Kare Technologies, LLC, Kare+Technologies,+LLC, None, https://www.doyoukare.com/, herosupport@doyoukare.com,

Release Date: Oct 14, 2019 **Privacy Policy:** Privacy link

Description:

Join the KARE Revolution and gain access to hundreds of assisted living and skilled nursing facilities in your area that need your help. Earn extra income and control your own schedule by working on a per shift basis with these communities! Sign up today!

SCAN LOGS

Timestamp	Event	Error
2025-08-30 22:34:18	Generating Hashes	OK

2025-08-30 22:34:18	Extracting APK	OK
2025-08-30 22:34:18	Unzipping	OK
2025-08-30 22:34:18	Parsing APK with androguard	OK
2025-08-30 22:34:19	Extracting APK features using aapt/aapt2	OK
2025-08-30 22:34:19	Getting Hardcoded Certificates/Keystores	OK
2025-08-30 22:34:20	Parsing AndroidManifest.xml	OK
2025-08-30 22:34:20	Extracting Manifest Data	OK
2025-08-30 22:34:20	Manifest Analysis Started	OK
2025-08-30 22:34:21	Performing Static Analysis on: Kare (com.kareheroes)	OK
2025-08-30 22:34:21	Fetching Details from Play Store: com.kareheroes	OK
2025-08-30 22:34:22	Checking for Malware Permissions	OK

2025-08-30 22:34:22	Fetching icon path	OK
2025-08-30 22:34:22	Library Binary Analysis Started	OK
2025-08-30 22:34:22	Reading Code Signing Certificate	OK
2025-08-30 22:34:22	Running APKiD 2.1.5	OK
2025-08-30 22:34:24	Detecting Trackers	OK
2025-08-30 22:34:25	Decompiling APK to Java with JADX	OK
2025-08-30 22:34:35	Converting DEX to Smali	OK
2025-08-30 22:34:35	Code Analysis Started on - java_source	OK
2025-08-30 22:34:36	Android SBOM Analysis Completed	OK
2025-08-30 22:34:42	Android SAST Completed	OK
2025-08-30 22:34:42	Android API Analysis Started	OK

2025-08-30 22:34:47	Android API Analysis Completed	OK
2025-08-30 22:34:48	Android Permission Mapping Started	OK
2025-08-30 22:34:53	Android Permission Mapping Completed	OK
2025-08-30 22:34:53	Android Behaviour Analysis Started	OK
2025-08-30 22:35:00	Android Behaviour Analysis Completed	OK
2025-08-30 22:35:00	Extracting Emails and URLs from Source Code	OK
2025-08-30 22:35:00	Email and URL Extraction Completed	OK
2025-08-30 22:35:00	Extracting String data from APK	OK
2025-08-30 22:35:00	Extracting String data from Code	OK

2025-08-30 22:35:00	Extracting String values and entropies from Code	OK
2025-08-30 22:35:02	Performing Malware check on extracted domains	OK
2025-08-30 22:35:03	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.