ANDROID STATIC ANALYSIS REPORT

(המגן 1.1.2)

File Name:	1.1.2 המגן.apk
Package Name:	com.hamagen
Average CVSS Score:	5.8
App Security Score:	10/100 (CRITICAL RISK)
Trackers Detection:	1/285

FILE INFORMATION

File Name: 1.1.2 המגן.apk
Size: 22.13MB
MD5: 400dbc9a036b44a6ca802f978d99ddd2
SHA1: 2f0c9a1bf539ea49e126e77d24dada4390becd03
SHA256: 99081d0e7a022d713fb22f5ef6ad5b64b6b025bbf32576071f05d96fb7a5f80e

APP INFORMATION

App Name: המגן
Package Name: com.hamagen
Main Activity: com.hamagen.MainActivity
Target SDK: 28
Min SDK: 21
Max SDK:
Android Version Name: 1.1.2
Android Version Code: 26

APP COMPONENTS

Activities: 5
Services: 21
Receivers: 20
Providers: 6
Exported Activities: 0
Exported Services: 4
Exported Receivers: 6
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-03-16 17:17:22+00:00
Valid To: 2047-08-02 17:17:22+00:00
Issuer: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Serial Number: 0x2a1253fa
Hash Algorithm: sha256
md5: 3ffbb10bd174876590acc2bcfe8d5ce7
sha1: 83d01f3a66722354b83d9b5853076fbf6b7e7f30
sha256: 8c810cac999511eb89a4476ebb964df5d606cc5b2884db7cc5c074fdb55bcc34
sha512:
ddf73e3e071d4920cc5097a9323e1b8e073b595e2266242ffa46eaeda3cefc970a18149e7a06623f2df06324c0e700b7ac9432af7b165e68279cdb2dc2809cdd

PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 3af5e60a6434389d0384e391308206f36021cf2710ee108d8f550355d4d56ac2

Certificate Status: Good
Description: Certificate looks good.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	dangerous	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.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_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background. If you're requesting this permission, you must also request either
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.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	normal	access extra location provider commands	Access extra location provider commands. Malicious applications could use this to interfere with the operation of the GPS or other location sources.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
oppo.permission.OPPO_COMPONENT_SAFE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.huawei.permission.external_app_settings.USE_COMPONENT	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
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	dangerous	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.CHANGE_NETWORK_STATE	dangerous	change network connectivity	Allows an application to change the state of network connectivity.

PERMISSION	STATUS	INFO	DESCRIPTION
com.android.vending.CHECK_LICENSE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	dangerous	Unknown permission from android reference	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code DETAILS: 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 FINDINGS: Compiler DETAILS: dx

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
Service (com.transistorsoft.locationmanager.scheduler.ScheduleJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	high	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.

ISSUE	SEVERITY	DESCRIPTION
Broadcast Receiver (com.transistorsoft.locationmanager.BootReceiver) is not Protected. An intent-filter exists.	high	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
Broadcast Receiver (com.learnium.RNDeviceInfo.RNDeviceReceiver) is not Protected. [android:exported=true]	high	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.
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]	high	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.
Service (com.transistorsoft.rnbackgroundfetch.HeadlessJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	high	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.
Broadcast Receiver (com.transistorsoft.rnbackgroundfetch.HeadlessBroadcastReceiver) is not Protected. An intent-filter exists.	high	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

ISSUE	SEVERITY	DESCRIPTION
Service (com.transistorsoft.tsbackgroundfetch.FetchJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	high	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.
Broadcast Receiver (com.transistorsoft.tsbackgroundfetch.BootReceiver) is not Protected. An intent-filter exists.	high	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
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]	high	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.
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]	high	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.
High Intent Priority (999) [android:priority]	medium	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

ISSUE	SEVERITY	STANDARDS	FILES
			org/slf4j/helpers/SubstituteLogger.java org/slf4j/helpers/BasicMarker.java org/greenrobot/eventbus/n.java org/greenrobot/eventbus/p.java ch/qos/logback/core/rolling/helper/FileNamePattern.java ch/qos/logback/core/joran/spi/ElementSelector.java ch/qos/logback/core/joran/spi/HostClassAndPropertyDouble.java ch/qos/logback/core/status/StatusBase.java ch/qos/logback/core/spi/AbstractComponentTracker.java ch/qos/logback/core/pattern/parser/FormattingNode.java ch/qos/logback/core/pattern/parser/Node.java ch/qos/logback/core/pattern/parser/CompositeNode.java ch/qos/logback/core/pattern/parser/Token.java ch/qos/logback/core/pattern/parser/SimpleKeywordNode.java ch/qos/logback/core/subst/Node.java ch/qos/logback/core/subst/Token.java ch/qos/logback/classic/spi/ClassPackagingData.java ch/qos/logback/classic/spi/ThrowableProxyVO.java ch/qos/logback/classic/spi/StackTraceElementProxy.java ch/qos/logback/classic/spi/LoggingEventVO.java ch/qos/logback/classic/spi/LoggerContextVO.java kotlinx/coroutines/B.java kotlinx/coroutines/C0950v.java kotlinx/coroutines/Y.java kotlinx/coroutines/C0946q.java io/invertase/firebase/c.java io/invertase/firebase/database/q.java io/invertase/firebase/database/RNFirebaseDatabase.java io/invertase/firebase/database/r.java io/invertase/firebase/firestore/RNFirebaseFirestore.java io/invertase/firebase/firestore/p.java io/invertase/firebase/auth/RNFirebaseAuth.java io/invertase/firebase/admob/h.java io/invertase/firebase/perf/RNFirebasePerformance.java io/invertase/firebase/notifications/d.java io/invertase/firebase/notifications/a.java io/radar/sdk/internal/d.java io/radar/sdk/internal/a.java io/radar/sdk/internal/LocationReceiver.java io/radar/sdk/internal/b/d.java io/radar/sdk/api/q.java

ISSUE	SEVERITY	STANDARDS	FILES
This App uses Java Hash Code. It's a weak hash function and should never be used in Secure Crypto Implementation.	warning	CVSS V2: 2.3 (low) CWE: CWE-327 - Use of a Broken or Risky Cryptographic Algorithm OWASP MASVS: MSTG-CRYPTO-4	io/radar/sdk/api/m.java g/k.java g/l.java g/f/a.java g/c/c.java g/e/a.java g/e/b/c.java g/e/b/k.java f/a/a/d/d.java f/a/a/d/e.java f/a/a/d/m.java f/a/a/e/b.java d/a/a/c/b.java d/a/a/c/d.java d/a/a/c/i.java d/a/a/d/c.java d/a/a/e/v.java d/a/a/e/I.java d/a/a/e/C0625g.java d/a/a/e/u.java d/c/a/a/b.java d/c/a/a/a.java d/c/a/a/a/b.java d/c/a/a/a/d.java d/c/a/a/a/f.java d/c/a/a/a/k.java d/c/a/a/a/c/a/C0689c.java d/c/a/c/a/h.java d/c/a/c/a/i.java d/c/a/b/f/f/C0766gc.java d/c/a/b/f/f/Wc.java d/c/a/b/f/f/Rc.java d/c/a/b/f/f/Pa.java d/c/a/b/f/f/Gb.java d/c/a/b/f/f/Cc.java d/c/a/b/f/f/Dc.java d/c/a/b/f/f/C0730bb.java d/c/a/b/f/f/C0767gd.java d/c/a/b/f/f/C0855tc.java d/c/a/b/f/e/F.java d/c/a/b/f/e/Y.java d/c/c/d.java d/c/c/f/a.java d/b/a/b.java d/b/h/a/a/b/d.java d/b/h/f/d.java d/b/j/d/C0649e.java d/b/j/e/b.java d/b/d/k/b.java d/b/e/j.java d/b/e/k.java d/b/b/a/i.java d/b/b/a/f.java d/b/b/b/b.java com/airbnb/android/react/lottie/e.java com/transistorsoft/tslocationmanager/Application.java com/transistorsoft/locationmanager/util/a.java com/transistorsoft/locationmanager/scheduler/TSScheduleManager.java com/reactnativecommunity/webview/RNCWebViewManager.java com/reactnativecommunity/netinfo/e.java

ISSUE	SEVERITY	STANDARDS	FILES
			com/intentfilter/androidpermissions/c.java com/intentfilter/androidpermissions/b/b.java com/RNFetchBlob/t.java b/f/i/I.java b/f/i/a/c.java b/f/i/a/d.java b/f/a/a/b.java b/d/h.java b/d/d.java b/d/i.java b/q/Ga.java b/q/ja.java b/q/Ha.java b/b/a/b/b.java
			org/slf4j/helpers/Util.java org/greenrobot/eventbus/b.java org/greenrobot/eventbus/e.java ch/qos/logback/core/net/SocketConnectorBase.java ch/qos/logback/core/net/DefaultSocketConnector.java ch/qos/logback/core/subst/Node.java ch/qos/logback/classic/net/SimpleSocketServer.java ch/qos/logback/classic/spi/ThrowableProxy.java ch/qos/logback/classic/android/LogcatAppender.java ch/qos/logback/classic/pattern/TargetLengthBasedClassNameAbbreviator.java io/invertase/firebase/RNFirebaseModule.java io/invertase/firebase/c.java io/invertase/firebase/database/q.java io/invertase/firebase/database/RNFirebaseDatabase.java io/invertase/firebase/database/r.java io/invertase/firebase/instanceid/RNFirebaseInstanceId.java io/invertase/firebase/firestore/n.java io/invertase/firebase/firestore/v.java io/invertase/firebase/firestore/c.java io/invertase/firebase/firestore/h.java io/invertase/firebase/firestore/q.java io/invertase/firebase/firestore/e.java io/invertase/firebase/firestore/i.java io/invertase/firebase/firestore/s.java io/invertase/firebase/firestore/f.java io/invertase/firebase/firestore/g.java io/invertase/firebase/firestore/u.java io/invertase/firebase/config/RNFirebaseRemoteConfig.java io/invertase/firebase/auth/B.java io/invertase/firebase/auth/w.java io/invertase/firebase/auth/n.java io/invertase/firebase/auth/z.java io/invertase/firebase/auth/C0915b.java io/invertase/firebase/auth/C.java io/invertase/firebase/auth/H.java io/invertase/firebase/auth/C0916c.java io/invertase/firebase/auth/D.java io/invertase/firebase/auth/C0919f.java

ISSUE	SEVERITY	STANDARDS	FILES
			io/invertase/firebase/auth/C0920g.java io/invertase/firebase/auth/p.java io/invertase/firebase/auth/E.java io/invertase/firebase/auth/C0917d.java io/invertase/firebase/auth/I.java io/invertase/firebase/auth/j.java io/invertase/firebase/auth/s.java io/invertase/firebase/auth/C0922i.java io/invertase/firebase/auth/F.java io/invertase/firebase/auth/C0914a.java io/invertase/firebase/auth/G.java io/invertase/firebase/auth/r.java io/invertase/firebase/auth/u.java io/invertase/firebase/auth/RNFirebaseAuth.java io/invertase/firebase/auth/y.java io/invertase/firebase/auth/l.java io/invertase/firebase/auth/m.java io/invertase/firebase/auth/C0921h.java io/invertase/firebase/auth/x.java io/invertase/firebase/auth/A.java io/invertase/firebase/auth/C0918e.java io/invertase/firebase/auth/t.java io/invertase/firebase/admob/RNFirebaseAdMob.java io/invertase/firebase/storage/v.java io/invertase/firebase/storage/RNFirebaseStorage.java io/invertase/firebase/storage/j.java io/invertase/firebase/storage/k.java io/invertase/firebase/storage/a.java io/invertase/firebase/links/b.java io/invertase/firebase/links/c.java io/invertase/firebase/links/RNFirebaseLinks.java io/invertase/firebase/links/a.java io/invertase/firebase/functions/b.java io/invertase/firebase/functions/RNFirebaseFunctions.java io/invertase/firebase/functions/a.java io/invertase/firebase/fabric/crashlytics/RNFirebaseCrashlytics.java io/invertase/firebase/perf/RNFirebasePerformance.java io/invertase/firebase/messaging/RNFirebaseMessaging.java io/invertase/firebase/messaging/k.java io/invertase/firebase/messaging/l.java io/invertase/firebase/messaging/m.java io/invertase/firebase/messaging/RNFirebaseMessagingService.java io/invertase/firebase/notifications/RNFirebaseNotifications.java io/invertase/firebase/notifications/d.java io/invertase/firebase/notifications/RNFirebaseNotificationsRebootReceiver.java io/invertase/firebase/notifications/a.java io/invertase/firebase/analytics/RNFirebaseAnalytics.java io/radar/sdk/internal/b.java d/a/a/C0632h.java d/a/a/f/c.java d/c/a/a/a/a/a.java d/c/a/c/a/h.java

ISSUE	SEVERITY	STANDARDS	FILES
The App logs information. Sensitive information should never be logged.	info	CVSS V2: 7.5 (high) CWE: CWE-532 - Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	d/c/a/c/b/a.java d/c/a/b/g/a/a.java d/c/a/b/a/a/b.java d/c/a/b/a/a/c.java d/c/a/b/a/a/a.java d/c/a/b/f/f/Ba.java d/c/a/b/f/f/Jc.java d/c/a/b/f/f/Da.java d/c/a/b/f/f/C0895za.java d/c/a/b/f/f/C0791ka.java d/c/a/b/f/f/C0782ie.java d/c/a/b/f/f/Ea.java d/c/a/b/f/f/C0881xa.java d/c/a/b/f/f/Va.java d/c/a/b/f/f/C0728b.java d/c/a/b/f/f/C0860ua.java d/c/a/b/f/f/C0798la.java d/c/a/b/f/f/C0888ya.java d/c/a/b/f/f/mg.java d/c/a/b/f/d/l.java d/c/a/b/f/e/C.java d/c/a/b/f/e/D.java d/c/a/b/f/e/A.java d/c/a/b/h/a.java d/c/a/b/c/w.java d/c/a/b/c/o.java d/c/a/b/c/q.java d/c/a/b/c/e.java d/c/a/b/c/i.java d/c/a/b/c/j.java d/c/a/b/c/y.java d/c/c/d.java d/b/h/c/i.java com/transistorsoft/rnbackgroundfetch/HeadlessBroadcastReceiver.java com/transistorsoft/rnbackgroundfetch/HeadlessTask.java com/transistorsoft/rnbackgroundfetch/HeadlessJobService.java com/transistorsoft/rnbackgroundgeolocation/RNBackgroundGeolocationModule.java com/transistorsoft/rnbackgroundgeolocation/HeadlessTask.java com/transistorsoft/locationmanager/BootReceiver.java com/transistorsoft/locationmanager/logger/TSLogReader.java com/transistorsoft/locationmanager/logger/TSLog.java com/transistorsoft/locationmanager/logger/a.java com/transistorsoft/locationmanager/util/b.java com/transistorsoft/locationmanager/util/BackgroundTaskManager.java com/transistorsoft/locationmanager/util/c.java com/transistorsoft/locationmanager/util/a.java com/transistorsoft/locationmanager/config/TSNotification.java com/transistorsoft/locationmanager/config/TSAuthorization.java com/transistorsoft/locationmanager/con

ISSUE	SEVERITY	STANDARDS	FILES
			fig/TransistorAuthorizationToken.java com/transistorsoft/locationmanager/activity/TSLocationManagerActivity.java com/transistorsoft/locationmanager/location/TSLocation.java com/transistorsoft/locationmanager/location/TSWatchPositionRequest.java com/transistorsoft/locationmanager/location/TSLocationManager.java com/transistorsoft/locationmanager/location/SingleLocationRequest.java com/transistorsoft/locationmanager/scheduler/TSScheduleManager.java com/transistorsoft/locationmanager/scheduler/ScheduleEvent.java com/transistorsoft/locationmanager/adapter/TSConfig.java com/transistorsoft/locationmanager/adapter/BackgroundGeolocation.java com/transistorsoft/locationmanager/a/a.java com/transistorsoft/locationmanager/geofence/TSGeofence.java com/transistorsoft/locationmanager/geofence/TSGeofenceManager.java com/transistorsoft/locationmanager/http/HttpService.java com/transistorsoft/locationmanager/http/HttpResponse.java com/transistorsoft/locationmanager/device/DeviceInfo.java com/transistorsoft/locationmanager/device/a.java com/transistorsoft/locationmanager/service/ForegroundNotification.java com/transistorsoft/locationmanager/service/ActivityRecognitionService.java com/transistorsoft/locationmanager/service/GeofencingService.java com/transistorsoft/locationmanager/service/AbstractService.java com/transistorsoft/locationmanager/service/BackgroundTaskService.java com/transistorsoft/locationmanager/service/LocationRequestService.java com/transistorsoft/locationmanager/service/TrackingService.java com/transistorsoft/locationmanager/data/LocationModel.java com/transistorsoft/locationmanager/data/sqlite/b.java com/transistorsoft/locationmanager/data/sqlite/a.java com/transistorsoft/locationmanager/data/sqlite/GeofenceDAO.java com/transistorsoft/locationmanager/c/a.java com/transistorsoft/locationmanager/d/b.java com/transistorsoft/locationmanager/event/AuthorizationEvent.java com/transistorsoft/locationmanager/event/TerminateEvent.java com/transistorsoft/locationmanager/event/ActivityChangeEvent.java

ISSUE	SEVERITY	STANDARDS	FILES
			com/transistorsoft/locationmanager/event/GeofenceEvent.java com/transistorsoft/locationmanager/event/HeartbeatEvent.java com/transistorsoft/locationmanager/event/GeofencesChangeEvent.java com/transistorsoft/locationmanager/event/MotionChangeEvent.java com/transistorsoft/locationmanager/event/LocationProviderChangeEvent.java com/transistorsoft/locationmanager/e/a.java com/transistorsoft/locationmanager/b/a.java com/transistorsoft/tsbackgroundfetch/BackgroundFetch.java com/transistorsoft/tsbackgroundfetch/BackgroundFetchConfig.java com/transistorsoft/tsbackgroundfetch/BootReceiver.java com/transistorsoft/tsbackgroundfetch/FetchJobService.java com/reactnativecommunity/webview/b.java com/reactnativecommunity/webview/RNCWebViewModule.java com/intentfilter/androidpermissions/a/b.java com/swmansion/reanimated/nodes/C0599i.java com/swmansion/gesturehandler/react/j.java com/pusherman/networkinfo/RNNetworkInfo.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/a/a.java b/r/a/a/k.java b/s/a/f.java b/a/a/a/a.java b/a/e/g.java b/f/i/B.java b/f/i/C0208e.java b/f/i/z.java b/f/i/C0210g.java b/f/i/C0205b.java b/f/i/y.java b/f/i/a/d.java b/f/a/a.java b/f/a/a/b.java b/f/a/a/h.java b/f/a/a/a.java b/f/f/a.java b/f/h/a.java b/f/b/b.java b/f/b/d.java b/f/b/e.java b/f/b/f.java b/f/b/k.java b/f/b/l.java b/o/a/c.java b/h/b/c.java b/m/a/b.java b/q/ya.java

ISSUE	SEVERITY	STANDARDS	FILES
			b/q/Ba.java b/q/Ea.java b/q/Aa.java
			b/q/za.java b/q/Ca.java b/q/ra.java b/q/sa.java b/k/a/a.java b/l/a/b.java
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.	high	CVSS V2: 5.9 (medium) CWE: CWE-89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	b/p/a/m.java org/pgsqlite/SQLitePlugin.java ch/qos/logback/classic/android/SQLiteAppender.java d/c/a/a/a/c/a/B.java d/c/a/a/a/c/a/F.java d/c/a/a/a/c/a/G.java com/transistorsoft/locationmanager/logger/TSSQLiteAppender.java com/transistorsoft/locationmanager/data/sqlite/b.java com/transistorsoft/locationmanager/data/sqlite/a.java com/transistorsoft/locationmanager/data/sqlite/GeofenceDAO.java com/reactnativecommunity/asyncstorage/l.java b/o/a/a/c.java
Files may contain hardcoded sensitive informations like usernames, passwords, keys etc.	high	CVSS V2: 7.4 (high) CWE: CWE-312 - Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	ch/qos/logback/core/CoreConstants.java ch/qos/logback/core/net/ssl/SSL.java ch/qos/logback/core/rolling/helper/DateTokenConverter.java ch/qos/logback/core/rolling/helper/IntegerTokenConverter.java ch/qos/logback/classic/sift/ContextBasedDiscriminator.java ch/qos/logback/classic/joran/action/ConfigurationAction.java io/invertase/firebase/functions/RNFirebaseFunctions.java io/invertase/firebase/notifications/RNFirebaseNotifications.java
The App uses an insecure Random Number Generator.	high	CVSS V2: 7.5 (high) CWE: CWE-330 - Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	kotlinx/coroutines/b/a.java d/c/a/b/f/f/mg.java
App can write to App Directory. Sensitive Information should be encrypted.	info	CVSS V2: 3.9 (low) CWE: CWE-276 - Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	io/radar/sdk/internal/b/a.java
This App may have root detection capabilities.	secure	CVSS V2: 0 (info) OWASP MASVS: MSTG-RESILIENCE-1	d/c/a/b/f/f/C0888ya.java
SHA-1 is a weak hash known to have hash collisions.	high	CVSS V2: 5.9 (medium) CWE: CWE-327 - Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	d/b/d/k/c.java com/sha1lib/Sha1Module.java

ISSUE	SEVERITY	STANDARDS	FILES
IP Address disclosure	warning	**CVSS V2:** 4.3 (medium) **CWE:** CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor **OWASP MASVS:** MSTG-CODE-2	com/pusherman/networkinfo/RNNetworkInfo.java com/pusherman/networkinfo/g.java
MD5 is a weak hash known to have hash collisions.	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-4	com/RNFetchBlob/D.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	good	**IP:** 83.173.251.158 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.55 **View:** Google Map
logback.qos.ch	good	**IP:** 83.173.251.158 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.55 **View:** Google Map
app-measurement.com	good	**IP:** 172.217.167.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	good	No Geolocation information available.
api.radar.io	good	**IP:** 104.16.51.85 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xml.org	good	**IP:** 104.239.240.11 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
pagead2.googlesyndication.com	good	**IP:** 172.217.167.98 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gl	good	**IP:** 216.58.203.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.w3.org	good	**IP:** 128.30.52.100 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.365078 **Longitude:** -71.104523 **View:** Google Map
hamagen-aa88d.firebaseio.com	good	**IP:** 35.201.97.85 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
graph.facebook.com	good	**IP:** 157.240.8.18 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map

URLS

URL	FILE
http://www.slf4j.org/codes.html#no_static_mdc_binder http://www.slf4j.org/codes.html#null_MDCA	org/slf4j/MDC.java
http://www.slf4j.org/codes.html http://www.slf4j.org/codes.html#loggerNameMismatch http://www.slf4j.org/codes.html#multiple_bindings http://www.slf4j.org/codes.html#StaticLoggerBinder http://www.slf4j.org/codes.html#null_LF http://www.slf4j.org/codes.html#replay http://www.slf4j.org/codes.html#substituteLogger http://www.slf4j.org/codes.html#unsuccessfulInit http://www.slf4j.org/codes.html#version_mismatch	org/slf4j/LoggerFactory.java
http://logback.qos.ch/codes.html#null_CS	org/slf4j/impl/StaticLoggerBinder.java
http://logback.qos.ch/codes.html#layoutInsteadOfEncoder	ch/qos/logback/core/OutputStreamAppender.java
http://logback.qos.ch/codes.html http://logback.qos.ch/manual/ http://logback.qos.ch/codes.html#tbr_fnp_not_set http://logback.qos.ch/codes.html#sat_missing_integer_token	ch/qos/logback/core/CoreConstants.java
http://logback.qos.ch/codes.html#earlier_fa_collision	ch/qos/logback/core/FileAppender.java
http://logback.qos.ch/codes.html#1andOnly1	ch/qos/logback/core/sift/SiftingJoranConfiguratorBase.java
http://logback.qos.ch/codes.html#syslog_layout	ch/qos/logback/core/net/SyslogAppenderBase.java
http://logback.qos.ch/codes.html#socket_no_port http://logback.qos.ch/codes.html#socket_no_host	ch/qos/logback/core/net/AbstractSocketAppender.java
http://logback.qos.ch/codes.html#smtp_no_layout	ch/qos/logback/core/net/SMTPAppenderBase.java
http://logback.qos.ch/codes.html#tbr_fnp_not_set	ch/qos/logback/core/rolling/TimeBasedRollingPolicy.java
http://logback.qos.ch/manual/appenders.html#SizeAndTimeBasedRollingPolicy	ch/qos/logback/core/rolling/SizeAndTimeBasedFNATP.java
http://logback.qos.ch/codes.html#tbr_fnp_prudent_unsupported http://logback.qos.ch/codes.html#fwrp_parentFileName_not_set http://logback.qos.ch/codes.html#tbr_fnp_not_set	ch/qos/logback/core/rolling/FixedWindowRollingPolicy.java
http://logback.qos.ch/codes.html#sbtp_size_format	ch/qos/logback/core/rolling/SizeBasedTriggeringPolicy.java
http://logback.qos.ch/codes.html#rfa_collision_in_dateFormat	ch/qos/logback/core/rolling/TimeBasedFileNamingAndTriggeringPolicyBase.java
http://logback.qos.ch/codes.html#rfa_collision http://logback.qos.ch/codes.html#rfa_file_after http://logback.qos.ch/codes.html#rfa_no_rp http://logback.qos.ch/codes.html#rfa_no_tp	ch/qos/logback/core/rolling/RollingFileAppender.java
http://logback.qos.ch/codes.html#renamingError	ch/qos/logback/core/rolling/helper/RenameUtil.java

URL	FILE
http://logback.qos.ch/codes.html#appender_order	ch/qos/logback/core/joran/action/AppenderRefAction.java
http://xml.org/sax/features/validation http://xml.org/sax/features/namespaces	ch/qos/logback/core/joran/event/SaxEventRecorder.java
http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd	ch/qos/logback/core/html/HTMLLayoutBase.java
http://logback.qos.ch/codes.html#missingRightParenthesis	ch/qos/logback/core/pattern/parser/Parser.java
http://logback.qos.ch/codes.html#receiver_no_port http://logback.qos.ch/codes.html#receiver_no_host	ch/qos/logback/classic/net/SocketReceiver.java
http://logback.qos.ch/css/classic.css	ch/qos/logback/classic/html/UrlCssBuilder.java
https://api.radar.io/ https://graph.facebook.com/	io/radar/sdk/api/k.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	d/c/a/b/a/a/b.java
https://app-measurement.com/a	d/c/a/b/f/f/Od.java
https://goo.gl/J1sWQy	d/c/a/b/f/f/mg.java
http://schemas.android.com/apk/res/android	b/f/a/a/i.java
https://hamagen-aa88d.firebaseio.com	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://hamagen-aa88d.firebaseio.com	info App talks to a Firebase Database.

EMAILS

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

TRACKERS

TRACKER	URL
Google Firebase Analytics	https://reports.exodus-privacy.eu.org/trackers/49

PLAYSTORE INFORMATION

Title: המגן - האפליקציה הלאומית למלחמה בנגיף הקורונה

Score: 3.8765824 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** 5.0 and up **Category:** Health & Fitness **Play Store URL:** com.hamagen

Developer Details: משרד הבריאות Gov, %D7%9E%D7%A9%D7%A8%D7%93+%D7%94%D7%91%D7%A8%D7%99%D7%90%D7%95%D7%AA+Gov, None, None, Hamagen@MOH.GOV.IL,

Release Date: Mar 22, 2020 **Privacy Policy:** Privacy link

Description:

כדי שנוכל להגן על בריאותם של האנשים בקבוצות הסיכון, של בני משפחתנו ושל כל אחד מאיתנו - על כולנו לקחת חלק במאמץ הלאומי נגד נגיף הקורונה. אפליקציית המגן מצליבה את מיקומך עם מפות המסלולים של חולי הקורונה המאומתים ומעדכנת אותך במקרה של חפיפה. האפליקציה של משרד הבריאות פועלת ברקע והמידע שלך נשאר על המכשיר שלך בלבד.

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.
For every findings with severity high we reduce 15 from the score.
For every findings with severity warning we reduce 10 from the score.
For every findings with severity good we add 5 to the score.
If the calculated score is greater than 100, then the app security score is considered as 100.
And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM
71 - 100	LOW

Report Generated by - MobSF v3.0.8 Beta

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.