ANDROID STATIC ANALYSIS REPORT

app_icon

MyDiabetes (2.18.0)

File Name:	health.mydiabetes_10080207.apk
Package Name:	health.mydiabetes
Scan Date:	Sept. 1, 2025, 1:32 p.m.
App Security Score:	49/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	5/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	29	4	2	1

FILE INFORMATION

File Name: health.mydiabetes_10080207.apk
Size: 27.69MB
MD5: 617e66d5dfdda34f378bf7130b67154c
SHA1: 31ce13fdbe8ceaeb705e2fada574fe4f92562f36
SHA256: e28b361b0dbee151460f8430176592f452434bea8c59a00058e05c654d0ef6c3

APP INFORMATION

App Name: MyDiabetes
Package Name: health.mydiabetes
Main Activity: diet.mydiabetes.MainActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 2.18.0

Android Version Code: 10080207

APP COMPONENTS

Activities: 29
Services: 18
Receivers: 18
Providers: 14
Exported Activities: 10
Exported Services: 3
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2023-09-12 14:00:24+00:00
Valid To: 2297-06-27 14:00:24+00:00
Issuer: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Serial Number: 0x4623a1b05817c2d5
Hash Algorithm: sha256
md5: fdd9ce1726b38b90e4a3963e382b5070
sha1: 67bbe8ca4865e1b46c34964a62a28a7cbff2fd4e
sha256: 8544cec777facab62e31b66d33392d62838f2d6b98ca2150c7551fa4e5fdfb9a
sha512: 5ae09df53e7542bcb16c8efeef8b1f987410a5282775c1642b4f3495bb24ca630392fde048d6808ad9d4092888e91cc937ba795b8ec0fdf949304652f6482c9b
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 27b94f7e671c9b1b1ba5a4e164ac81ee94ead5de69f47790c8cbc11f0a3c0565
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.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.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
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.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.health.READ_STEPS	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.health.READ_BLOOD_GLUCOSE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_BLOOD_GLUCOSE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_HYDRATION	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_HYDRATION	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_WEIGHT	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_WEIGHT	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_BLOOD_PRESSURE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_BLOOD_PRESSURE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_EXERCISE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_EXERCISE	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.DETECT_SCREEN_CAPTURE	normal	notifies when a screen capture of the app's windows is attempted.	Allows an application to get notified when a screen capture of its windows is attempted.
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.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

PERMISSION	STATUS	INFO	DESCRIPTION
health.mydiabetes.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
android.permission.BROADCAST_CLOSE_SYSTEM_DIALOGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.
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_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.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>617e66d5dfdda34f378bf7130b67154c.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table>
</td></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
ro.kernel.qemu check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes2.dex	<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.TAGS check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
network operator name check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
net.openid.appauth.RedirectUriReceiverActivity	Schemes: mydiabetes://,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.health.mydiabetes,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,

ACTIVITY	INTENT
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Activity (com.zoontek.rnbootsplash.RNBootSplashActivity) 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.
3	Activity-Alias (diet.mydiabetes.MainActivityChristmas) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity-Alias (diet.mydiabetes.MainActivityDefault) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Activity (diet.mydiabetes.PermissionsRationaleActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Activity-Alias (diet.mydiabetes.ViewPermissionUsageActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.START_VIEW_PERMISSION_USAGE [android:exported=true]	warning	An Activity-Alias 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
7	Service (androidx.health.platform.client.impl.sdkservice.HealthDataSdkService) 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.
8	Activity (net.openid.appauth.RedirectUriReceiverActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	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.
10	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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	Activity (com.google.firebase.auth.internal.RecaptchaActivity) 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.
12	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
13	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.
14	Broadcast Receiver (com.amazon.device.iap.ResponseReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.amazon.inapp.purchasing.Permission.NOTIFY [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.
15	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
16	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.
17	Activity (app.notifee.core.NotificationReceiverActivity) 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.
18	Broadcast Receiver (app.notifee.core.AlarmPermissionBroadcastReceiver) 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.

</> CODE ANALYSIS

HIGH: **2** | WARNING: **9** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a6/c.java a6/c0.java a6/e.java a6/f0.java a6/n.java a6/p.java a6/q.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a6/u.java aa/d0.java aa/e0.java aa/y.java af/g.java app/notifee/core/AlarmPermissionBroadcastReceiver.java app/notifee/core/Logger.java app/notifee/core/RebootBroadcastReceiver.java bi/l.java br/c.java cf/b.java cf/c.java cf/g.java cf/q.java cf/r.java cf/t.java cf/w.java cf/x.java cl/json/RNShareModule.java com/amazon/a/a/g/d.java com/amazon/a/a/o/c.java com/amazon/c/a/a/d.java com/amazon/device/drm/LicensingService.java com/amazon/device/drm/a/d/c.java com/amazon/device/iap/PurchasingService.java com/amazon/device/iap/internal/c/e.java com/amazon/device/simplesignin/BroadcastHandler.java com/amazon/device/simplesignin/SimpleSignInService.java com/amazon/device/simplesignin/a/a/c/b.java com/amazon/device/simplesignin/a/c.java com/amazon/device/simplesignin/a/c/b.java com/appsflyer/AFLogger.java com/appsflyer/internal/AFa1eSDK.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/appsflyer/internal/AFb1nSDK.java com/appsflyer/internal/AFb1sSDK.java com/appsflyer/internal/AFc1bSDK.java com/appsflyer/internal/AFd1fSDK.java com/appsflyer/internal/AFd1gSDK.java com/appsflyer/internal/AFd1hSDK.java com/appsflyer/internal/AFd1jSDK.java com/appsflyer/internal/AFd1lSDK.java com/appsflyer/internal/AFd1nSDK.java com/appsflyer/internal/AFd1oSDK.java com/appsflyer/internal/AFd1pSDK.java com/appsflyer/internal/AFd1rSDK.java com/appsflyer/internal/AFd1zSDK.java com/appsflyer/internal/AFe1pSDK.java com/appsflyer/internal/AFe1rSDK.java com/appsflyer/internal/AFf1hSDK.java com/appsflyer/reactnative/RNAppsFlyerModule.java com/appsflyer/share/LinkGenerator.java com/brentvatne/exoplayer/g.java com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/c.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java com/bumptech/glide/request/j.java com/dooboolab/rniap/RNIapModule.java com/dooboolab/rniap/b.java com/dooboolab/rniap/d.java com/github/barteksc/pdfviewer/e.java com/github/barteksc/pdfviewer/h.java com/heanoria/library/reactnative/locationenabler/RNAndroidLocationEnablerModule.java com/henninghall/date_picker/c.java com/henninghall/date_picker/pickers/AndroidNative.java com/ibits/react_native_in_app_review/AppReviewModule.java com/imagepicker/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/imagepicker/d.java com/imagepicker/g.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/f.java com/microsoft/codepush/react/k.java com/mrousavy/camera/core/CameraSession.java com/mrousavy/camera/core/p.java com/mrousavy/camera/core/p0.java com/mrousavy/camera/frameprocessors/FrameProcessorPluginRegistry.java com/mrousavy/camera/frameprocessors/VisionCameraProxy.java com/mrousavy/camera/react/CameraDevicesManager.java com/mrousavy/camera/react/CameraViewModule.java com/mrousavy/camera/react/k.java com/mrousavy/camera/react/n.java com/mrousavy/camera/react/q.java com/mrousavy/camera/react/r.java com/reactcommunity/rndatetimepicker/d.java com/reactnativecommunity/asyncstorage/c.java com/reactnativecommunity/slider/a.java com/reactnativecommunity/webview/RNCWebViewManager.java com/reactnativecommunity/webview/RNCWebViewModule.java com/reactnativegooglesignin/RNGoogleSigninModule.java com/reactnativegooglesignin/b.java com/reactnativemmkv/MmkvModule.java com/revenuecat/purchases/common/DefaultLogHandler.java com/revenuecat/purchases/hybridcommon/CommonKt.java com/revenuecat/purchases/hybridcommon/mappers/PurchasesPeriod.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/revenuecat/purchases/react/RNPurchasesModule.java com/shockwave/pdfium/PdfiumCore.java com/swmansion/gesturehandler/react/RNGestureHandlerModule.java com/swmansion/gesturehandler/react/i.java com/swmansion/gesturehandler/react/j.java com/swmansion/reanimated/NativeMethodsHelper.java com/swmansion/reanimated/ReanimatedModule.java com/swmansion/reanimated/ReanimatedUIManagerFactory.java com/swmansion/reanimated/layoutReanimation/AnimationsManager.java com/swmansion/reanimated/layoutReanimation/ReanimatedNativeHierarchyManager.java com/swmansion/reanimated/layoutReanimation/SharedTransitionManager.java com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java com/swmansion/reanimated/sensor/ReanimatedSensorContainer.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/swmansion/rnscreens/ScreensModule.java com/th3rdwave/safeareacontext/l.java d8/f.java dc/k.java df/c0.java df/e.java df/h0.java df/j.java df/k.java df/m.java df/m0.java df/p.java
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	

NO	ISSUE	SEVERITY	STANDARDS	FILES
				df/y.java dh/i.java e1/f.java e3/a.java e6/a.java e6/d.java e6/j.java eg/a.java ej/c.java f0/e.java fg/a.java fi/a.java g6/e.java g6/f.java g6/o.java g6/p.java g6/r.java g6/s.java gc/a.java h3/d.java h6/d.java h9/d.java h9/j.java hf/a.java hj/c.java hn/h.java i3/a.java i4/q0.java i5/c.java ig/c.java io/invertase/firebase/app/a.java io/invertase/firebase/auth/ReactNativeFirebaseAuthModule.java io/invertase/firebase/database/a.java io/invertase/firebase/dynamiclinks/ReactNativeFirebaseDynamicLinksModule.java io/invertase/firebase/installations/ReactNativeFirebaseInstallationsModule.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/invertase/notifee/l0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				j6/d.java j6/k.java k0/z.java k1/c.java k3/o.java k3/r.java k3/u.java k3/y.java ks/k.java l6/b.java lf/b.java li/g.java lr/e.java m0/e.java m3/a.java mf/h.java mf/t.java mf/u.java mh/e.java n6/a.java n8/d.java ne/p.java net/time4j/android/ApplicationStarter.java nq/a.java o3/h.java o5/a.java o6/d.java o6/g.java o6/n.java o6/n0.java o6/s.java org/wonday/orientation/a.java os/c.java p3/d.java p4/b.java p5/d.java p5/e.java pq/d.java q3/a.java q4/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				q4/n.java q5/a.java q9/a0.java q9/d0.java q9/k.java q9/k0.java q9/m0.java q9/t0.java q9/u0.java qf/d.java ql/a.java r6/l.java rd/m0.java re/a.java re/d.java rh/a0.java rh/b0.java rh/c.java rh/i0.java rh/l0.java rh/q.java rh/q0.java rh/t.java rh/z0.java rl/d.java s5/c.java s5/e.java s6/e.java s6/f.java se/o.java sh/g.java sh/n.java sl/k.java t3/a.java t5/h.java t5/i.java t5/k.java t5/q.java t5/z.java tb/a.java u3/m0.java u5/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				u3/f.java u5/j.java u6/a.java u9/c.java uh/m.java v2/c.java v5/e.java v5/i.java vg/d.java vn/a.java vn/g.java vn/l.java w2/a.java w4/j.java w5/a.java w6/f.java w6/i.java w6/j.java w6/m.java wf/k.java wg/b.java wj/m.java x/t0.java x5/c.java x5/d.java x5/f.java x5/r.java x5/s.java xi/b.java xq/i.java yg/g.java yi/c.java yr/g.java z/b1.java z3/i.java z5/i.java z6/a.java z9/c.java zq/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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/d.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/reactnativecommunity/webview/RNCWebViewModule.java e7/a.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java p7/a.java q9/t0.java v4/a.java
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/amazon/a/a/o/b/a.java hn/h.java kr/c.java kr/d.java kr/i.java kr/j.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	ar/z.java com/amazon/a/a/b/b.java com/amazon/a/a/i/b.java com/amazon/a/a/l/c.java com/appsflyer/internal/AFa1vSDK.java com/appsflyer/internal/AFb1oSDK.java fp/a.java fp/b.java gp/a.java hi/i.java mj/d.java or/d.java or/h.java q9/t0.java rd/p0.java xh/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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/appsflyer/reactnative/RNAppsFlyerConstants.java com/heanoria/library/reactnative/locationenabler/RNAndroidLocationEnablerModule.java com/revenuecat/purchases/amazon/AmazonBillingKt.java com/revenuecat/purchases/amazon/AmazonCacheKt.java com/revenuecat/purchases/common/BackendKt.java com/revenuecat/purchases/common/BackgroundAwareCallbackCacheKey.java com/revenuecat/purchases/common/caching/DeviceCache.java com/revenuecat/purchases/common/diagnostics/DiagnosticsEntry.java com/revenuecat/purchases/common/diagnostics/DiagnosticsHelper.java com/revenuecat/purchases/common/diagnostics/DiagnosticsTracker.java com/revenuecat/purchases/common/offlineentitlements/ProductEntitlementMapping.java com/revenuecat/purchases/common/verification/DefaultSignatureVerifier.java com/revenuecat/purchases/common/verification/Signature.java com/revenuecat/purchases/common/verification/SigningManager.java com/revenuecat/purchases/strings/ConfigureStrings.java com/revenuecat/purchases/subscriberattributes/SubscriberAttribute.java com/revenuecat/purchases/subscriberattributes/SubscriberAttributeKt.java e4/d.java io/invertase/notifee/NotifeeEventSubscriber.java q6/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				r5/h.java t5/d.java t5/p.java t5/x.java x8/g.java
6	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/reactnativecommunity/clipboard/ClipboardModule.java
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	t4/c.java
8	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	cg/b.java com/RNFetchBlob/a.java com/reactnativecommunity/webview/RNCWebViewModule.java com/rumax/reactnative/pdfviewer/c.java e7/a.java k3/y.java tl/f.java xi/c.java z/z.java
9	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	bi/l.java com/amazon/a/a/o/b/a.java com/revenuecat/purchases/common/UtilsKt.java s7/c.java xi/b.java z9/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/reactnativecommunity/asyncstorage/f.java kc/m0.java kc/t0.java p3/c.java uh/n.java
11	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	a7/b.java aa/d0.java u6/j.java
12	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	hi/c.java
13	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	am/a.java com/amazon/device/drm/LicensingService.java com/amazon/device/iap/PurchasingService.java ta/a.java
14	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 f5/g.java o6/e.java w6/m.java
15	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	dh/w.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
16	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	wd/a.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/RNFetchBlob/d.java com/RNFetchBlob/g.java com/amazon/a/a/b/b.java com/appsflyer/internal/AFb1nSDK.java com/microsoft/codepush/react/a.java com/microsoft/codepush/react/j.java com/microsoft/codepush/react/k.java com/microsoft/codepush/react/n.java com/mrousavy/camera/react/r.java com/oblador/vectoricons/VectorIconsModule.java com/reactlibrary/createthumbnail/CreateThumbnailModule.java com/rumax/reactnative/pdfviewer/c.java e7/f.java f5/g.java f5/h.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java j7/c.java k3/y.java p0/r0.java p3/d.java p4/b.java p4/c.java p4/d.java p7/a.java q3/a.java v4/a.java w4/t.java yh/g.java z/z.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	a7/a.java c7/b.java com/RNFetchBlob/a.java com/RNFetchBlob/d.java com/amazon/c/a/a/c.java com/appsflyer/internal/AFa1hSDK.java com/appsflyer/internal/AFb1nSDK.java com/bumptech/glide/load/a.java com/imagepicker/g.java com/microsoft/codepush/react/j.java com/microsoft/codepush/react/n.java com/reactnativecommunity/asyncstorage/c.java com/revenuecat/purchases/common/FileHelper.java com/rumax/reactnative/pdfviewer/c.java f5/g.java f5/h.java k3/y.java m3/b.java me/g.java o5/a.java o6/g.java pr/r.java q9/k0.java s9/k.java w6/m.java x5/f.java x6/j.java xi/c.java z/z.java zo/j.java

RULE ID	BEHAVIOUR	LABEL	FILES
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFf1mSDK.java q9/m0.java s7/f.java v4/a.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFa1dSDK.java p4/b.java v4/a.java
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFf1mSDK.java q9/m0.java s7/f.java v4/a.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFf1mSDK.java com/appsflyer/internal/AFf1nSDK.java q9/m0.java v4/a.java
00191	Get messages in the SMS inbox	sms	com/RNFetchBlob/g.java com/appsflyer/internal/AFf1lSDK.java com/appsflyer/internal/AFf1mSDK.java q9/b.java q9/m0.java q9/t0.java v4/a.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFf1mSDK.java q9/m0.java s7/f.java v4/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFf1mSDK.java q9/m0.java s7/f.java v4/a.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFf1mSDK.java com/appsflyer/internal/AFf1nSDK.java q9/m0.java s5/c.java v4/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	aa/c.java app/notifee/core/Notifee.java cl/json/RNShareModule.java com/RNFetchBlob/g.java com/amazon/a/a/i/a.java com/amazon/a/a/i/g.java com/amazon/device/iap/internal/a/a.java com/appsflyer/internal/AFa1eSDK.java com/appsflyer/internal/AFb1sSDK.java com/appsflyer/internal/AFd1sSDK.java com/rnappauth/RNAppAuthModule.java df/f.java dq/n.java io/invertase/firebase/dynamiclinks/ReactNativeFirebaseDynamicLinksModule.java li/g.java net/openid/appauth/c.java q4/g.java q4/n.java q9/b.java q9/m0.java q9/t0.java q9/u0.java q9/y0.java tb/a.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	app/notifee/core/Notifee.java df/f.java dq/n.java q4/g.java q9/t0.java q9/u0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	a7/a.java com/appsflyer/internal/AFb1nSDK.java s9/k.java x6/j.java xi/c.java
00091	Retrieve data from broadcast	collection	aa/i0.java com/amazon/device/drm/a/d/c.java com/amazon/device/iap/internal/c/e.java com/amazon/device/simplesignin/a/c/b.java com/appsflyer/internal/AFa1eSDK.java com/appsflyer/internal/AFb1sSDK.java net/openid/appauth/AuthorizationManagementActivity.java q9/m0.java
00036	Get resource file from res/raw directory	reflection	app/notifee/core/Notifee.java b7/a.java com/amazon/a/a/i/g.java com/appsflyer/internal/AFa1eSDK.java com/appsflyer/internal/AFf1lSDK.java com/appsflyer/internal/AFf1nSDK.java com/brentvatne/exoplayer/ReactExoplayerViewManager.java com/dylanvann/fastimage/FastImageSource.java df/f.java dq/o.java ib/a.java p4/b.java q9/b.java q9/t0.java q9/u0.java q9/y0.java
00043	Calculate WiFi signal strength	collection wifi	an/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00003	Put the compressed bitmap data into JSON object	camera	r6/l.java
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/a.java q9/t0.java
00109	Connect to a URL and get the response code	network command	af/f.java com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFc1lSDK.java com/appsflyer/internal/AFc1tSDK.java com/appsflyer/internal/AFd1kSDK.java com/bumptech/glide/load/data/j.java com/revenuecat/purchases/common/HTTPClient.java me/s.java q6/g.java re/d.java yi/c.java
00004	Get filename and put it to JSON object	file collection	s9/c.java w9/a.java x6/f.java
00096	Connect to a URL and set request method	command network	com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFc1lSDK.java com/appsflyer/internal/AFc1tSDK.java com/revenuecat/purchases/common/HTTPClient.java com/rumax/reactnative/pdfviewer/a.java f5/b.java me/s.java q6/g.java yi/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00072	Write HTTP input stream into a file	command network file	com/microsoft/codepush/react/h.java com/rumax/reactnative/pdfviewer/a.java
00089	Connect to a URL and receive input stream from the server	command network	com/appsflyer/internal/AFc1lSDK.java com/appsflyer/internal/AFc1tSDK.java com/bumptech/glide/load/data/j.java com/microsoft/codepush/react/h.java com/revenuecat/purchases/common/HTTPClient.java com/rumax/reactnative/pdfviewer/a.java me/s.java q6/g.java yi/c.java z9/c.java
00030	Connect to the remote server through the given URL	network	com/appsflyer/internal/AFa1uSDK.java com/bumptech/glide/load/data/j.java com/rumax/reactnative/pdfviewer/a.java f5/b.java me/s.java
00094	Connect to a URL and read data from it	command network	com/rumax/reactnative/pdfviewer/a.java me/s.java zq/a.java
00108	Read the input stream from given URL	network command	com/rumax/reactnative/pdfviewer/a.java me/s.java
00162	Create InetSocketAddress object and connecting to it	socket	kr/b.java kr/j.java
00163	Create new Socket and connecting to it	socket	kr/b.java kr/j.java

RULE ID	BEHAVIOUR	LABEL	FILES
00012	Read data and put it into a buffer stream	file	com/amazon/c/a/a/c.java com/microsoft/codepush/react/n.java o6/g.java w6/m.java
00132	Query The ISO country code	telephony collection	ne/m0.java
00024	Write file after Base64 decoding	reflection file	com/RNFetchBlob/a.java com/RNFetchBlob/d.java p4/c.java p4/d.java w4/t.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00078	Get the network operator name	collection telephony	com/appsflyer/internal/AFa1kSDK.java com/learnium/RNDeviceInfo/RNDeviceModule.java q9/t0.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
00125	Check if the given file path exist	file	x6/f.java
00187	Query a URI and check the result	collection sms calllog calendar	q9/m0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00005	Get absolute path of file and put it to JSON object	file	com/appsflyer/internal/AFb1nSDK.java com/microsoft/codepush/react/k.java
00015	Put buffer stream (data) to JSON object	file	q9/t0.java
00115	Get last known location of the device	collection location	com/mrousavy/camera/core/p0.java
00114	Create a secure socket connection to the proxy address	network command	fr/f.java
00123	Save the response to JSON after connecting to the remote server	network command	net/openid/appauth/h.java
00028	Read file from assets directory	file	me/c.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://my-diabetes-prod-8d132-default-rtdb.firebaseio.com

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/257113240904/namespaces/firebase:fetch?key=AIzaSyBxbPrPBEfbch4g6AOSESrTB9k1SaAQxeQ is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'ab_guided_first_meal': 'true', 'ab_guided_morning_routine': 'true', 'ab_health_summary_placement': 'true', 'ab_nutrition_insights_v2': 'true', 'ab_paywall_skip_button': 'false', 'ab_smart_photo_log': 'true', 'ab_sso': 'true', 'ab_welcome_screen_v2': 'true'}, 'state': 'UPDATE', 'templateVersion': '10'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	13/25	android.permission.VIBRATE, android.permission.INTERNET, android.permission.SYSTEM_ALERT_WINDOW, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.RECORD_AUDIO, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION
Other Common Permissions	9/44	android.permission.ACTIVITY_RECOGNITION, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE, android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.ACCESS_NOTIFICATION_POLICY

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
pinterest.com	ok	**IP:** 151.101.0.84 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
appleid.apple.com	ok	**IP:** 17.32.194.6 **Country:** United States of America **Region:** California **City:** Cupertino **Latitude:** 37.316605 **Longitude:** -122.046486 **View:** Google Map
mydiabetes.health	ok	**IP:** 172.67.72.204 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
graph-video.s	ok	No Geolocation information available.
codepush.appcenter.ms	ok	No Geolocation information available.
api.revenuecat.com	ok	**IP:** 54.158.163.245 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
sinapps.s	ok	No Geolocation information available.
www.firebase.com	ok	**IP:** 151.101.65.195 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
plus.google.com	ok	**IP:** 216.58.211.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
issuetracker.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
.facebook.com	ok	No Geolocation information available.
play.google.com	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
graph.s	ok	No Geolocation information available.
facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.114.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.74.110 **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

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sconversions.s	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.
developer.android.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
android.googlesource.com	ok	**IP:** 64.233.165.82 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sgcdsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
exoplayer.dev	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
notifee.app	ok	**IP:** 52.52.192.191 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
docs.swmansion.com	ok	**IP:** 104.21.27.136 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
ssdk-services.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
sattr.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
developers.facebook.com	ok	**IP:** 31.13.70.1 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
sars.s	ok	No Geolocation information available.
rev.cat	ok	**IP:** 52.72.49.79 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.250.74.66 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sregister.s	ok	No Geolocation information available.
scdn-ssettings.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
accounts.google.com	ok	**IP:** 209.85.233.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
scdn-stestsettings.s	ok	No Geolocation information available.
api-diagnostics.revenuecat.com	ok	**IP:** 34.196.55.80 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
appleid.a	ok	No Geolocation information available.
developer.apple.com	ok	**IP:** 17.253.83.135 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api-paywalls.revenuecat.com	ok	**IP:** 52.21.13.22 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
sstats.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.
ns.adobe.com	ok	No Geolocation information available.
schemas.microsoft.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
www.googleapis.com	ok	**IP:** 142.250.74.10 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sapp.s	ok	No Geolocation information available.
errors.rev.cat	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
docs.revenuecat.com	ok	**IP:** 18.238.109.116 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sviap.s	ok	No Geolocation information available.
dashif.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.amazon.com	ok	**IP:** 18.238.90.46 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
shopify.github.io	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
svalidate.s	ok	No Geolocation information available.
aomedia.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
console.firebase.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
my-diabetes-prod-8d132-default-rtdb.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	df/x.java

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
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

TRACKER	CATEGORIES	URL
Instabug	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/206

HARDCODED SECRETS

POSSIBLE SECRETS
"CodePushDeploymentKey" : "X0az3OiminRJkVkLB-fzqdR_0HsVxIVJWndq-"
"facebook_client_token" : "dacea94f5cd70502b76734f8e53fafb6"
"firebase_database_url" : "https://my-diabetes-prod-8d132-default-rtdb.firebaseio.com"
"google_api_key" : "AIzaSyBxbPrPBEfbch4g6AOSESrTB9k1SaAQxeQ"
"google_crash_reporting_api_key" : "AIzaSyBxbPrPBEfbch4g6AOSESrTB9k1SaAQxeQ"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
2758019355995970587784901184038904809305690585636156852142870730198868924130986086513626076488374510776543976123057 5
4105836372515214212932612978004726840911444101599372555483525631403946740129 1
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

POSSIBLE SECRETS
7fmduHKTdHHrlMvldlEqAIlSfii1tl35bxj1OXN5Ve8c4lU6URVu4xtSHc3BVZxS6WWJnxMDhIfQN0N0K2NDJg==
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
ABi2fbt8vkzj7SJ8aD5jc4xJFTDFntdkMrYXL3itsvqY1QIw
ae2044fb577e65ee8bb576ca48a2f06e
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
c56fb7d591ba6704df047fd98f535372fea00211
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
1093849038073734274511112390766805569936207598951683748994586394495953116150735016013708737573759623248592132296706313309438452531591012912142327488478985984
UC1upXWg5QVmyOSwozp755xLqquBKjjU+di6U8QhMIM=
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
9a04f079-9840-4286-ab92-e65be0885f95

POSSIBLE SECRETS
484395612939064517590525852527979142027629495260417479958440807170824046352 86
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
9b8f518b086098de3d77736f9458a3d2f6f95a37
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
375718002577002046354550722449118360359445513476976248669456777961554447744055631669123440501294553956214444453728942852258566672919658081012434427757837678 4
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 16
dZozdop5rgKNxjbrQAd5nntAGpgh9w84O1Xgg==
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
115792089210356248762697446949407573530086143415290314195533631308867097853951

POSSIBLE SECRETS
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
266174080205021706322876871672336096072985916875697314770667136841880294499642780849154508062777190235209424122506555866215711354557091681416163731589599984 6
cc2751449a350f668590264ed76692694a80308a
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
5181942b9ebc31ce68dacb56c16fd79f
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
1ddaa4b892e61b0f7010597ddc582ed3
1157920892103562487626974469494075735300861434152903141955336313088670978539 48
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
832571096148902998554675128952010817928785304886131559470920590248050319988441922443864376039294733307808651162787 1
24b2477514809255df232947ce7928c4
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087
36134250956749795798585127919587881956611106672985015071877198253568414405109
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
1157920892103562487626974469494075735299969552241357603424222590610685120443 69

POSSIBLE SECRETS

PLAYSTORE INFORMATION

Title: MyDiabetes: Meal, Carb Tracker

Score: 4.33 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** health.mydiabetes

Developer Details: Diabetes Solutions, Diabetes+Solutions, None, https://mydiabetes.health, hello@mydiabetes.health,

Release Date: Oct 17, 2023 **Privacy Policy:** Privacy link

Description:

Navigating the challenges of diabetes? Whether you're living with diabetes or managing prediabetes, the MyDiabetes app is here to support your journey. Track your glucose, HbA1c (hemoglobin A1c), and blood sugar levels with our built-in blood sugar monitor. Get personalized meal suggestions tailored to your preferences and glycemic index needs. Easily monitor your weight, blood sugar trends, and overall health. MyDiabetes is designed for people dealing with high blood sugar, weight concerns, and other diabetes-related issues – offering trusted guidance for effective diabetes management. Try MyDiabetes for FREE and take the first step toward better health. Use our tools to track blood sugar, A1c, water intake, medications, carbs (with our carb tracker), calorie intake, and more. You can even track calories daily and use the glucose blood sugar tracker to stay on top of your numbers. And when you're ready for more... Upgrade to Premium to unlock exclusive features: personalized diabetic meal plans, weekly grocery lists, no-equipment workouts for weight loss, and more – designed to help you live well with diabetes. Created with the help of health experts and nutritionists, MyDiabetes offers practical strategies for diabetes management, plus delicious recipes that support your lifestyle and diet plan weight loss goals. It's your path to improved health, better weight control, and smarter tracking with our all-in-one food and carb tracker. We believe you should be able to enjoy food while managing diabetes. That's why our Premium plan offers personalized meal options – so you can stay on track without giving up the foods you love. Our mission: to help you feel better and stay supported every step of the way. MyDiabetes FREE Features: Health Tracker Easily log your glucose, blood sugar, A1c, medications, and carbs. Spot trends for doctor visits and keep your health goals on track. Syncs with Health Connect. Use the built-in blood sugar monitor for daily insights. Activity Overview Keep tabs on meals, workouts, and hydration to maintain a consistent diabetes record and support your routine. MyDiabetes Premium Perks: Personalized Meal Planner Get meals tailored to your calorie, carb, sugar, and glycemic index needs. Includes healthy diabetic recipes and an advanced carb tracker. Smart Grocery Lists Plan your weekly shop with ease using auto-generated grocery lists based on your selected meal plan. Home-Friendly Workouts Access no-equipment workouts designed to support energy levels and weight loss goals for people living with diabetes. Advanced Health Tracker Monitor all your key health metrics, including blood sugar, with our glucose blood sugar tracker. Ideal for checkups and syncing with Health Connect. Daily Activity Snapshot Stay organized with a full view of your meals, hydration, and exercise – fully integrated with Health Connect. SUBSCRIPTION INFO MyDiabetes offers both Free and Premium plans. Pricing may vary by location and will be charged in your local currency. Subscriptions renew automatically unless canceled beforehand. Download MyDiabetes and start building a healthier routine today. Discover easy, nutritious recipes and take control of your health with our advanced meal planner, carb tracking tools, and diet plan weight loss support. Disclaimer: Always consult your doctor before making medical decisions. Terms and Conditions: https://mydiabetes.health/general-conditions/ Privacy Policy: https://mydiabetes.health/data-protection-policy/

SCAN LOGS

Timestamp	Event	Error
2025-09-01 13:32:38	Generating Hashes	OK
2025-09-01 13:32:38	Extracting APK	OK
2025-09-01 13:32:38	Unzipping	OK
2025-09-01 13:32:38	Parsing APK with androguard	OK
2025-09-01 13:32:39	Extracting APK features using aapt/aapt2	OK
2025-09-01 13:32:39	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 13:32:41	Parsing AndroidManifest.xml	OK
2025-09-01 13:32:41	Extracting Manifest Data	OK
2025-09-01 13:32:41	Manifest Analysis Started	OK

2025-09-01 13:32:41	Performing Static Analysis on: MyDiabetes (health.mydiabetes)	OK
2025-09-01 13:32:43	Fetching Details from Play Store: health.mydiabetes	OK
2025-09-01 13:32:44	Checking for Malware Permissions	OK
2025-09-01 13:32:44	Fetching icon path	OK
2025-09-01 13:32:44	Library Binary Analysis Started	OK
2025-09-01 13:32:44	Reading Code Signing Certificate	OK
2025-09-01 13:32:45	Running APKiD 2.1.5	OK
2025-09-01 13:32:50	Detecting Trackers	OK
2025-09-01 13:32:53	Decompiling APK to Java with JADX	OK
2025-09-01 13:33:09	Converting DEX to Smali	OK

2025-09-01 13:33:09	Code Analysis Started on - java_source	OK
2025-09-01 13:33:14	Android SBOM Analysis Completed	OK
2025-09-01 13:33:21	Android SAST Completed	OK
2025-09-01 13:33:21	Android API Analysis Started	OK
2025-09-01 13:33:28	Android API Analysis Completed	OK
2025-09-01 13:33:28	Android Permission Mapping Started	OK
2025-09-01 13:33:39	Android Permission Mapping Completed	OK
2025-09-01 13:33:39	Android Behaviour Analysis Started	OK
2025-09-01 13:33:49	Android Behaviour Analysis Completed	OK
2025-09-01 13:33:49	Extracting Emails and URLs from Source Code	OK

2025-09-01 13:33:53	Email and URL Extraction Completed	OK
2025-09-01 13:33:53	Extracting String data from APK	OK
2025-09-01 13:33:53	Extracting String data from Code	OK
2025-09-01 13:33:53	Extracting String values and entropies from Code	OK
2025-09-01 13:33:56	Performing Malware check on extracted domains	OK
2025-09-01 13:34:01	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.