MOBSF

ANDROID STATIC ANALYSIS REPORT

FuturHealth (2.5.1)

File Name:	com.futurhealth.futurhealth_119.apk
Package Name:	com.futurhealth.futurhealth
Scan Date:	Aug. 29, 2025, 10:41 p.m.
App Security Score:	49/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	7/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	22	5	2	1

FILE INFORMATION

File Name: com.futurhealth.futurhealth_119.apk
Size: 47.14MB
MD5: 9540996e29ebc23a17df20f133351cf2
SHA1: 2a1da5c6eb61a3e22cd0e09e29f6fc4b30c5256f
SHA256: e9fa3f6f4228869bf94b366ffa42c142223127d2c6dcc54120eb2f54c0e4df2e

APP INFORMATION

App Name: FuturHealth
Package Name: com.futurhealth.futurhealth
Main Activity: com.futurhealth.futurhealth.MainActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 2.5.1

Android Version Code: 119

APP COMPONENTS

Activities: 16
Services: 19
Receivers: 14
Providers: 14
Exported Activities: 3
Exported Services: 3
Exported Receivers: 3
Exported Providers: 1

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2024-01-12 14:07:52+00:00
Valid To: 2054-01-12 14:07:52+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x400d6962758420be1bd8c1abe5aac321e2208708
Hash Algorithm: sha256
md5: 0fc675450fae5405412a302bbd75de86
sha1: a6a99333b68fb36b0ecb3151bdb4dce5d1fa5df7
sha256: 9ac533a93aa171320704e6cb9bb2391429108c13bd69dd740886cd05f42436d7
sha512: 1b0dc2307de5fb001335aaaa8d64365e549618b2f2e964fa310288ff680de3ec2fcdd364551cf563f5dd76f77fafc0700dacd3ad41f6ac7998d256f069ff64df
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 1d0bae6be63928ddbed5ec928fe9c5709b0f55db0d00e18df80522e48cce7060
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.
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.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	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.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

PERMISSION	STATUS	INFO	DESCRIPTION
com.futurhealth.futurhealth.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.

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

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>9540996e29ebc23a17df20f133351cf2.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
possible Build.SERIAL check
network operator name check
device ID 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.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check possible VM 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.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>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.futurhealth.futurhealth.MainActivity	Schemes: https://, http://, futurhealthapp://, Hosts: futurhealth.page.link, autologin,
com.facebook.CustomTabActivity	Schemes: @string/FACEBOOK_CUSTOM_URL_SCHEME://, fbconnect://, Hosts: cct.com.futurhealth.futurhealth,
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: 1 | WARNING: 11 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Content Provider (com.facebook.FacebookContentProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Service (com.wix.reactnativenotifications.fcm.FcmInstanceIdListenerService) 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.
6	Broadcast Receiver (io.invertase.firebase.messaging.ReactNativeFirebaseMessagingReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
8	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.
9	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.
10	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.

NO	ISSUE	SEVERITY	DESCRIPTION
11	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.
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.

</> CODE ANALYSIS

HIGH: **1** | WARNING: **9** | INFO: **4** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A/f0.java B2/b.java B6/A.java B6/C0707c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				B6/C0707c.java B6/j.java B6/t.java B6/x.java C7/g.java C9/d.java E6/a.java H0/c.java H2/b.java H4/D.java H4/Y.java I2/d.java I2/e.java I7/C0837b0.java I7/C0842e.java I7/D.java I7/K.java I7/Q.java I7/V.java I7/Y.java J2/a.java J6/s.java L2/c.java L2/e.java M/x.java M2/h.java M2/i.java M2/k.java M2/q.java M2/z.java M7/g.java N0/a.java N1/c.java N2/i.java N2/k.java O/d.java O1/f.java O2/e.java O2/i.java P2/a.java P8/C.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				P8/C0972g.java P8/C0976k.java P8/F.java P8/I.java Q2/c.java Q2/d.java Q2/g.java Q2/s.java Q2/t.java Q2/u.java Q4/c.java Q8/a.java R0/n.java R8/c.java S2/l.java Sb/c.java T2/A.java T2/C1034c.java T2/C1037f.java T2/I.java T2/L.java T2/o.java T2/v.java T2/w.java V0/a.java Wb/c.java X2/a.java X2/d.java X2/j.java Y9/A.java Y9/k.java Y9/m.java Y9/n.java Y9/q.java Y9/s.java Y9/t.java Y9/z.java Z2/d.java b3/d.java b3/k.java c1/AbstractC1372a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	cloud/mindbox/mobile_sdk/utils/b.java com/appsflyer/internal/AFa1aSDK.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1uSDK.java com/appsflyer/internal/AFc1vSDK.java com/appsflyer/internal/AFf1cSDK.java com/appsflyer/internal/AFf1dSDK.java com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1kSDK.java com/appsflyer/internal/AFf1lSDK.java com/appsflyer/internal/AFf1tSDK.java com/appsflyer/internal/AFg1hSDK.java com/appsflyer/internal/AFg1jSDK.java com/appsflyer/internal/AFg1nSDK.java com/appsflyer/reactnative/RNAppsFlyerModule.java com/appsflyer/share/CrossPromotionHelper.java com/appsflyer/share/LinkGenerator.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/manager/f.java com/bumptech/glide/manager/p.java com/bumptech/glide/manager/r.java com/bumptech/glide/manager/t.java com/bumptech/glide/manager/u.java com/bumptech/glide/manager/v.java com/bumptech/glide/request/j.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/f.java com/lugg/RNCConfig/RNCConfigModule.java com/microsoft/codepush/react/k.java com/mrousavy/camera/core/AbstractC1975k.java com/mrousavy/camera/core/AbstractC19

NO	ISSUE	SEVERITY	STANDARDS	FILES
				76l.java com/mrousavy/camera/core/AbstractC1977m.java com/mrousavy/camera/core/AbstractC1979o.java com/mrousavy/camera/core/CameraSession.java com/mrousavy/camera/core/V.java com/mrousavy/camera/core/b0.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/o.java com/mrousavy/camera/react/r.java com/mrousavy/camera/react/u.java com/mrousavy/camera/react/v.java com/reactnative/googlefit/GoogleFitModule.java com/reactnative/ivpusic/imagepicker/a.java com/reactnativecommunity/asyncstorage/h.java com/shopify/reactnative/skia/PlatformContext.java com/shopify/reactnative/skia/c.java com/swmansion/gesturehandler/react/i.java com/swmansion/gesturehandler/react/j.java com/swmansion/reanimated/layoutReanimation/AnimationsManager.java com/vonovak/AddCalendarEventModule.java com/yalantis/ucrop/UCropActivity.java com/yalantis/ucrop/task/BitmapCropTask.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/yalantis/ucrop/view/b.java e4/M.java f3/AbstractC2139a.java fb/AsyncTaskC2160a.java fr/greweb/reactnativeviewshot/RNViewShotModule.java gb/AbstractC2198a.java gb/AbstractC2200c.java gb/C2203f.java gc/e.java h2/C2223j.java i6/AbstractC2285a.java io/invertase/firebase/app/ReactNativeFirebaseApp.java io/invertase/firebase/app/ReactNativeFirebaseAppModule.java io/invertase/firebase/auth/ReactNativeFirebaseAuthModule.java io/invertase/firebase/common/RCTConvertFirebase.java io/invertase/firebase/common/SharedUtils.java io/invertase/firebase/crashlytics/ReactNativeFirebaseCrashlyticsInitProvider.java io/invertase/firebase/crashlytics/ReactNativeFirebaseCrashlyticsModule.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingReceiver.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/legere/pdfiumandroid/DefaultLogger.java io/legere/pdfiumandroid/PdfiumCore.java io/sentry/X2.java io/sentry/android/core/C2370u.java io/sentry/android/core/v0.java io/sentry/android/replay/w.java io/sentry/android/replay/z.java j0/d.java j1/AbstractC2497k.java l8/C2641a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				m0/f.java m7/C2577d.java o3/l.java org/wonday/orientation/a.java org/wonday/pdf/a.java r/C1.java r/C2940e0.java t2/C3117e.java u7/i.java v/t.java v1/AbstractC3191d.java x2/C3296g.java x7/p.java x7/w.java y/AbstractC3335h0.java y/X.java y9/C3394a.java z6/g.java
2	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	Y0/c.java a8/n.java com/reactnativecommunity/asyncstorage/k.java m6/M.java m6/U.java x2/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	A/AbstractC0653z.java D8/c.java E9/i.java T0/A.java aa/C1153f.java com/ReactNativeBlobUtil/a.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnativecommunity/webview/l.java fr/greweb/reactnativeviewshot/RNViewShotModule.java io/sentry/react/m.java w3/b.java
4	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	B2/a.java H3/a.java H4/Y.java com/ReactNativeBlobUtil/c.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnative/ivpusic/imagepicker/a.java com/reactnativecommunity/webview/l.java g2/AbstractC2166c.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/sentry/android/core/V.java w3/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	Cb/a.java H4/Y.java Vb/A.java com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFb1gSDK.java d8/C2040a.java jc/d.java jc/h.java n8/i.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	fc/c.java fc/d.java fc/i.java fc/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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	K2/h.java M2/d.java M2/p.java M2/x.java O8/b.java Q7/b.java R7/C1011e.java R7/w.java cloud/mindbox/mobile_sdk/models/operation/Ids.java cloud/mindbox/mobile_sdk/pushes/PushAction.java com/appsflyer/reactnative/RNAppsFlyerConstants.java com/futurhealth/futurhealth/BuildConfig.java com/reactnative/ivpusic/imagepicker/PickerModule.java i3/g.java io/invertase/firebase/common/TaskExecutorService.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingHeadlessService.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingSerializer.java o4/C2826b.java
8	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	O1/j.java R4/D.java m3/j.java s3/b.java
9	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	com/reactnativecommunity/clipboard/ClipboardModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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	J1/d.java O1/m.java com/reactnativecommunity/clipboard/ClipboardModule.java
11	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/ReactNativeBlobUtil/i.java g3/C2179e.java o3/l.java q2/C2881g.java
12	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/m.java
13	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	P7/AbstractC0949i.java io/sentry/android/core/internal/util/m.java u7/w.java
14	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	D8/b.java K3/c.java Q4/a.java h8/l.java io/sentry/util/w.java
15	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	M9/a.java q5/AbstractC2887a.java
16	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	n8/c.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
			A/AbstractC0653z.java B1/l.java B3/c.java E9/i.java H3/a.java Q7/f.java R1/a.java T0/A.java U/S.java Y0/d.java aa/C1153f.java com/ReactNativeBlobUtil/c.java com/ReactNativeBlobUtil/g.java com/appsflyer/internal/AFg1jSDK.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/v.java com/oblador/vectoricons/a.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnative/ivpusic/imagepicker/a.java com/reactnative/ivpusic/imagepicker/e.java e8/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	fr/greweb/reactnativeviewshot/RNViewShotModule.java g2/AbstractC2166c.java h2/AbstractC2233u.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java
			io/sentry/AbstractC2441q.java io/sentry/C2451s2.java io/sentry/C2473x.java io/sentry/S0.java io/sentry/U0.java io/sentry/android/core/AbstractC2375z.java io/sentry/android/core/V.java io/sentry/android/core/cache/b.java io/sentry/android/replay/capture/f.java io/sentry/android/replay/h.java io/sentry/cache/c.java io/sentry/cache/d.java io/sentry/cache/f.java io/sentry/instrumentation/file/a.java io/sentry/react/m.java q2/C2881g.java q2/C2882h.java v1/AbstractC3191d.java v1/C3192e.java v1/f.java w3/k.java z0/m.java
00024	Write file after Base64 decoding	reflection file	com/ReactNativeBlobUtil/a.java com/ReactNativeBlobUtil/g.java h2/AbstractC2233u.java v1/C3192e.java v1/f.java
			A/AbstractC0653z.java D8/c.java F2/a.java H2/b.java H4/K.java J4/k.java P7/A.java

RULE ID	BEHAVIOUR	LABEL	FILES
			Q2/g.java Q7/f.java T0/A.java U7/e.java
00013	Read file and put it into a stream	file	V0/b.java W7/a.java com/ReactNativeBlobUtil/a.java com/ReactNativeBlobUtil/c.java com/ReactNativeBlobUtil/e.java com/ReactNativeBlobUtil/h.java com/airbnb/android/react/lottie/h.java com/appsflyer/internal/AFb1iSDK.java com/appsflyer/internal/AFg1jSDK.java com/bumptech/glide/load/a.java com/microsoft/codepush/react/j.java com/microsoft/codepush/react/n.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnativecommunity/asyncstorage/h.java g3/C2181g.java gb/AbstractC2202e.java io/sentry/C2473x.java io/sentry/S0.java io/sentry/U0.java io/sentry/android/core/SentryPerformanceProvider.java io/sentry/android/replay/h.java io/sentry/cache/c.java io/sentry/cache/d.java io/sentry/cache/f.java io/sentry/config/e.java io/sentry/instrumentation/file/b.java io/sentry/instrumentation/file/h.java io/sentry/util/e.java kc/r.java o3/l.java p3/j.java q2/C2881g.java q2/C2882h.java s3/C3079a.java u3/C3151b.java vb/C3232j.java

RULE ID	BEHAVIOUR	LABEL	FILES
			z0/m.java com/microsoft/codepush/react/n.java g3/C2181g.java io/sentry/C2473x.java
00012	Read data and put it into a buffer stream	file	io/sentry/S0.java io/sentry/cache/c.java io/sentry/cache/f.java io/sentry/config/e.java io/sentry/util/e.java o3/l.java
00191	Get messages in the SMS inbox	sms	H4/C0788b.java H4/M.java H4/Y.java com/ReactNativeBlobUtil/g.java com/appsflyer/internal/AFi1bSDK.java com/appsflyer/internal/AFi1iSDK.java com/appsflyer/internal/AFi1jSDK.java g2/AbstractC2166c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	H4/C0788b.java H4/M.java H4/Y.java H4/Z.java H4/d0.java J1/b.java R4/C0989c.java U5/a.java com/ReactNativeBlobUtil/d.java com/ReactNativeBlobUtil/g.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1bSDK.java com/appsflyer/internal/AFc1vSDK.java com/appsflyer/internal/AFf1vSDK.java com/futurhealth/futurhealth/OpenSettingsModule.java com/reactnative/ivpusic/imagepicker/PickerModule.java io/invertase/firebase/dynamiclinks/ReactNativeFirebaseDynamicLinksModule.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java r8/C3043g.java v1/C3188a.java w1/h.java w1/o.java x7/x.java
00004	Get filename and put it to JSON object	file collection	J4/c.java N4/a.java p3/f.java
00125	Check if the given file path exist	file	com/ReactNativeBlobUtil/g.java p3/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00189	Get the content of a SMS message	sms	H4/M.java com/appsflyer/internal/AFi1bSDK.java com/vonovak/a.java g2/AbstractC2166c.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1jSDK.java g2/AbstractC2166c.java v1/AbstractC3191d.java
00188	Get the address of a SMS message	sms	H4/M.java com/appsflyer/internal/AFi1bSDK.java com/vonovak/a.java g2/AbstractC2166c.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	H4/M.java com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1bSDK.java g2/AbstractC2166c.java
00200	Query data from the contact list	collection contact	H4/M.java com/appsflyer/internal/AFi1bSDK.java com/vonovak/a.java g2/AbstractC2166c.java
00201	Query data from the call log	collection calllog	H4/M.java com/appsflyer/internal/AFi1bSDK.java com/vonovak/a.java g2/AbstractC2166c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	H4/M.java L2/c.java com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1bSDK.java g2/AbstractC2166c.java
00091	Retrieve data from broadcast	collection	H4/M.java R4/I.java Ya/f.java com/ReactNativeBlobUtil/g.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1vSDK.java com/masteratul/exceptionhandler/DefaultErrorScreen.java
00036	Get resource file from res/raw directory	reflection	H4/C0788b.java H4/Y.java H4/Z.java H4/d0.java Za/p.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFf1qSDK.java com/appsflyer/internal/AFi1iSDK.java com/appsflyer/internal/AFi1nSDK.java com/dylanvann/fastimage/FastImageSource.java com/reactnative/ivpusic/imagepicker/PickerModule.java io/invertase/firebase/common/SharedUtils.java me/leolin/shortcutbadger/impl/NovaHomeBadger.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java t3/C3125a.java v1/AbstractC3191d.java x7/x.java
00003	Put the compressed bitmap data into JSON object	camera	j3/l.java

RULE ID	BEHAVIOUR	LABEL	FILES
00016	Get location info of the device and put it to JSON object	location collection	x2/C3295f.java
00175	Get notification manager and cancel notifications	notification	ab/C1157b.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	H4/Y.java H4/Z.java com/ReactNativeBlobUtil/g.java com/futurhealth/futurhealth/OpenSettingsModule.java w1/h.java x7/x.java
00162	Create InetSocketAddress object and connecting to it	socket	fc/b.java fc/j.java
00163	Create new Socket and connecting to it	socket	fc/b.java fc/j.java
00014	Read file into a stream and put it into a JSON object	file	D8/c.java J4/k.java Q7/f.java W7/a.java com/appsflyer/internal/AFg1jSDK.java p3/j.java s3/C3079a.java
00072	Write HTTP input stream into a file	command network file	com/microsoft/codepush/react/h.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	E8/c.java Q4/c.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java com/bumptech/glide/load/data/j.java com/microsoft/codepush/react/h.java i3/g.java io/sentry/transport/o.java x2/C3299j.java
00187	Query a URI and check the result	collection sms calllog calendar	H4/M.java
00114	Create a secure socket connection to the proxy address	network command	ac/f.java
00078	Get the network operator name	collection telephony	H4/Y.java com/appsflyer/internal/AFi1xSDK.java com/learnium/RNDeviceInfo/RNDeviceModule.java x2/n.java
00137	Get last known location of the device	location collection	x2/n.java
00115	Get last known location of the device	collection location	com/mrousavy/camera/core/V.java x2/n.java
00132	Query The ISO country code	telephony collection	x2/n.java
00009	Put data in cursor to JSON object	file	H4/Y.java com/reactnativecommunity/asyncstorage/a.java x2/l.java

RULE ID	BEHAVIOUR	LABEL	FILES
00112	Get the date of the calendar event	collection calendar	Y9/k.java
00005	Get absolute path of file and put it to JSON object	file	Q7/f.java com/appsflyer/internal/AFg1jSDK.java com/microsoft/codepush/react/k.java
00079	Hide the current app's icon	evasion	s1/g.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00038	Query the phone number	collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00130	Get the current WIFI information	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00134	Get the current WiFi IP address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00082	Get the current WiFi MAC address	collection wifi	com/learnium/RNDeviceInfo/RNDeviceModule.java
00096	Connect to a URL and set request method	command network	E8/c.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java i3/g.java io/sentry/transport/o.java q2/C2876b.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/j.java io/sentry/transport/o.java q2/C2876b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	E8/c.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java com/appsflyer/internal/AFf1jSDK.java com/bumptech/glide/load/data/j.java i3/g.java io/sentry/transport/o.java r6/AbstractC3035a.java x2/C3299j.java z6/RunnableC3448f.java
00094	Connect to a URL and read data from it	command network	T7/a.java com/shopify/reactnative/skia/PlatformContext.java
00015	Put buffer stream (data) to JSON object	file	H4/Y.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://futurhealth-8e4d8-default-rtdb.firebaseio.com

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/593850785656/namespaces/firebase:fetch?key=AIzaSyC8JNP08hztOoioJjGeNLTOxEiB4Y8wFmM is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'ambassador_banner_config': 'baseline', 'is_mandatory_update': 'true', 'meal_setup': 'false', 'onboarding_mealbox_setup_v2': 'true', 'test_param': 'false'}, 'state': 'UPDATE', 'templateVersion': '21'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/25	android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.CAMERA, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.READ_PHONE_STATE, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK
Other Common Permissions	6/44	android.permission.ACTIVITY_RECOGNITION, android.permission.READ_CALENDAR, com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
pinterest.com	ok	**IP:** 151.101.192.84 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sentry20.kube.g-plans.com	ok	**IP:** 34.68.56.245 **Country:** United States of America **Region:** Iowa **City:** Council Bluffs **Latitude:** 41.261940 **Longitude:** -95.860832 **View:** Google Map
graph-video.s	ok	No Geolocation information available.
codepush.appcenter.ms	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
futurhealth-8e4d8-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
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
api.eu.amplitude.com	ok	**IP:** 35.158.245.182 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
plus.google.com	ok	**IP:** 64.233.185.100 **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:** 64.233.177.138 **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:** 172.253.124.138 **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
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
github.com	ok	**IP:** 140.82.113.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase.google.com	ok	**IP:** 74.125.136.139 **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
sconversions.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
simpression.s	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
developer.android.com	ok	**IP:** 64.233.176.113 **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.
sattr.s	ok	No Geolocation information available.
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

DOMAIN	STATUS	GEOLOCATION
ssdk-services.s	ok	No Geolocation information available.
futurhealth.com	ok	**IP:** 172.66.43.51 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sadrevenue.s	ok	No Geolocation information available.
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.
sregister.s	ok	No Geolocation information available.
scdn-ssettings.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
accounts.google.com	ok	**IP:** 172.217.215.84 **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.
api2.amplitude.com	ok	**IP:** 52.37.138.108 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
aps-webhandler.appsflyer.com	ok	**IP:** 18.238.109.53 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sonelink.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
svalidate-and-log.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.googleapis.com	ok	**IP:** 64.233.185.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sapp.s	ok	No Geolocation information available.
firebase-settings.crashlytics.com	ok	**IP:** 142.250.9.94 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sviap.s	ok	No Geolocation information available.
regionconfig.eu.amplitude.com	ok	**IP:** 18.238.96.19 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
shopify.github.io	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
regionconfig.amplitude.com	ok	**IP:** 18.155.173.45 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
svalidate.s	ok	No Geolocation information available.
console.firebase.google.com	ok	**IP:** 64.233.176.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
5412696e57deb98e7cda@sentry20.kube	com/futurhealth/futurhealth/BuildConfig.java
5412696e57deb98e7cda@sentry20.kube	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Amplitude	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/125
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 CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

HARDCODED SECRETS

POSSIBLE SECRETS
"AMPLITUDE_API_KEY" : "4a298d0460e26fc3a985ab0ff7d5fa1e"
"APPSFLYER_DEV_KEY" : "MF4iiEhHuw5U3SgJMmLEgj"
"CODEPUSH_ANDROID_KEY" : "hHIQQcsqR65hw3h1kw3CH8psm8QTr-5NVA8Jk"
"CODEPUSH_IOS_KEY" : "hI-96rp0Exk9oARvgtFEmNJc7kvKBktbvCvSQ"
"FACEBOOK_CLIENT_TOKEN" : "871b5ce007ce5d4ad27e940090db0d90"
"com.google.firebase.crashlytics.mapping_file_id" : "b4f4cc4d375645e18e7c4b97fcb420c9"
"facebook_client_token" : "871b5ce007ce5d4ad27e940090db0d90"
"firebase_database_url" : "https://futurhealth-8e4d8-default-rtdb.firebaseio.com"
"google_api_key" : "AIzaSyC8JNP08hztOoioJjGeNLTOxEiB4Y8wFmM"
"google_crash_reporting_api_key" : "AIzaSyC8JNP08hztOoioJjGeNLTOxEiB4Y8wFmM"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
1157920892373161954235709850086879078532699846656405640394575840079088346716 63
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575
41058363725152142129326129780047268409114441015993725554835256314039467401291

POSSIBLE SECRETS
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa
96rp0Exk9oARvgtFEmNJc7kvKBktbvCvSQ
199075f688d5412696e57deb98e7cda
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
49f946663a8deb7054212b8adda248c6
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
af60eb711bd85bc1e4d3e0a462e074eea428a8
3267051002075881697808308513050704318447127338065924327593890433575733748242 4
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
c56fb7d591ba6704df047fd98f535372fea00211
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
1093849038073734274511112390766805569936207598951683748994586394495953116150735016013708737573759623248592132296706313309438452531591012912142327488478985984

POSSIBLE SECRETS
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
a4b63c1cca619b8f8c7a2617427805dd
36864200e0eaf5284d884a0e77d31646
55066263022277343669578718895168534326250603453777594175500187360389116729240
484395612939064517590525852527979142027629495260417479958440807170824046352 86
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
9b8f518b086098de3d77736f9458a3d2f6f95a37
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196 5808101243442775783767 84
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112316
1157920892373161954235709850086879078528375642790749043826051631415181614943 37

POSSIBLE SECRETS
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
115792089210356248762697446949407573530086143415290314195533631308867097853951
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
2661740802050217063228768716723360960729859168756973147706671368418802944996427808491545080627771902352094241225065558662157113545570916814161637315895999846
cc2751449a350f668590264ed76692694a80308a
00fd6e8c1e516a697ab698be896615e9
871b5ce007ce5d4ad27e940090db0d90
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
c103703e120ae8cc73c9248622f3cd1e
4a298d0460e26fc3a985ab0ff7d5fa1e
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449

POSSIBLE SECRETS
d8a714418753fef6b4f7ce8daaaf5331
1157920892103562487626974469494075735300861434152903141955336313088670978539 48
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
832571096148902998554675128952010817928785304886131559470920590248050319988441922443864376039294733307808651162787 1
262470350957996892686231567445669818918529234911092133878156159009255188547380500890223880539757197866508724767320 87
361342509567497957985851279195878819566111066729850150718771982535684144051 09
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
bae8e37fc83441b16034566b
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
a44db91caef4e28596f27e6278a09f28

PLAYSTORE INFORMATION

Title: FuturHealth

Score: 4.0540543 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.futurhealth.futurhealth

Developer Details: FuturHealth, FuturHealth, None, https://futurhealth.com/, support@futurhealth.com,

Release Date: Jan 15, 2024 **Privacy Policy:** Privacy link

Description:

It all starts by downloading the FuturHealth app and taking our free quiz to get approved for weight loss medication within just a few minutes. You won't believe the information you'll find out about your body... And you'll quickly be joining thousands of people just like you who want to live a healthier happier and better life! That's what makes FuturHealth different... A prescribed, medical approach to weight loss and nutrition! Featured in the New York Times, Cosmopolitan, Men's health, Vogue, MSN, People magazine and more, we've helped millions of people around the world live their best live and achieve their health and wellness goals. What is FuturHealth? FuturHealth is the only prescription weight loss program that combines medication and nutrition seamlessly. FuturHealth provides weekly prescribed medication shipped to your door and fully customized meal programming and conditioning based on one's metabolic type. Join the community and get access to the full suite of tools available and start being your best self today! Here's what you'll get with FuturHealth: Weight Loss Medication Program: - Get approved for weight loss medication within minutes today. - Have complete oversight by a board-certified doctor in your state. - Ozempic(R) or compounded semaglutide shipped direct to your door at 70% off pharmacy prices. Nutrition: - Perfectly matched meals to your body and prescription medication. - Weekly (changing) meal plans (with custom recipes) matched to you and your metabolic-ID and synched to your devices. - Professional nutrition coaching and guidance. - Programs suitable for many dietary restrictions and allergies - Paleo, vegetarian, pescatarian, vegan etc. - Built-in exchange list so you can create your own delicious meals easily. - Calorie, macro and daily performance tracking tools to keep you accountable. - Built-in recipe generator to keep your plan delicious and easy to follow. - Dedicated custom support team available around the clock to help you hit your goals. SUBSCRIPTION TERMS & PRICING The FuturHealth Weight Loss RX Program is just USD $129.99 per month for full access which includes your own doctor and medication prescription. Medication costs are additional and based on type, which start at just $229 per month. Payment will be charged to your credit card at confirmation of purchase. Subscription auto-renews automatically (unless canceled) at least 24 hours prior to the end of the subscription period. There is no increase in price when renewing. Subscriptions can be managed in the application. Once purchased, refunds will not be provided for any unused portion of the term. Read full Terms of Service and our Privacy Policy at https://futurhealth.com/new/pages/terms/, and https://futurhealth.com/new/pages/privacy. Results from RX Path may vary. Medication prescriptions are at the discretion of medical providers and may not be suitable for everyone. FuturHealth typically result in 1-2 lbs per week weight loss in 4 weeks, involving a healthy diet and exercise changes. Consult a healthcare professional before using RX Path or starting any weight loss program.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 22:41:57	Generating Hashes	OK
2025-08-29 22:41:57	Extracting APK	OK

2025-08-29 22:41:57	Unzipping	OK
2025-08-29 22:41:57	Parsing APK with androguard	OK
2025-08-29 22:41:57	Extracting APK features using aapt/aapt2	OK
2025-08-29 22:41:57	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 22:41:59	Parsing AndroidManifest.xml	OK
2025-08-29 22:41:59	Extracting Manifest Data	OK
2025-08-29 22:41:59	Manifest Analysis Started	OK
2025-08-29 22:42:00	Performing Static Analysis on: FuturHealth (com.futurhealth.futurhealth)	OK
2025-08-29 22:42:00	Fetching Details from Play Store: com.futurhealth.futurhealth	OK
2025-08-29 22:42:01	Checking for Malware Permissions	OK
2025-08-29 22:42:01	Fetching icon path	OK

2025-08-29 22:42:01	Library Binary Analysis Started	OK
2025-08-29 22:42:01	Reading Code Signing Certificate	OK
2025-08-29 22:42:02	Running APKiD 2.1.5	OK
2025-08-29 22:42:06	Detecting Trackers	OK
2025-08-29 22:42:08	Decompiling APK to Java with JADX	OK
2025-08-29 22:42:23	Converting DEX to Smali	OK
2025-08-29 22:42:23	Code Analysis Started on - java_source	OK
2025-08-29 22:42:28	Android SBOM Analysis Completed	OK
2025-08-29 22:42:37	Android SAST Completed	OK
2025-08-29 22:42:37	Android API Analysis Started	OK

2025-08-29 22:42:47	Android API Analysis Completed	OK
2025-08-29 22:42:47	Android Permission Mapping Started	OK
2025-08-29 22:42:54	Android Permission Mapping Completed	OK
2025-08-29 22:42:54	Android Behaviour Analysis Started	OK
2025-08-29 22:43:06	Android Behaviour Analysis Completed	OK
2025-08-29 22:43:06	Extracting Emails and URLs from Source Code	OK
2025-08-29 22:43:09	Email and URL Extraction Completed	OK
2025-08-29 22:43:09	Extracting String data from APK	OK
2025-08-29 22:43:09	Extracting String data from Code	OK
2025-08-29 22:43:09	Extracting String values and entropies from Code	OK
2025-08-29 22:43:12	Performing Malware check on extracted domains	OK

2025-08-29 22:43:19	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.