

Testin

App Security Scanning

Report

Application Information



OpenRice
com.openrice.android

Application

Version: 5.8.1 (build 4091) Application Type: Android - APK
Size: 38.15 MB Detection Category: App Security Scanning
MD5: CFBCC9D34EDAD22FF30CF2523C5845EC Detection Time: 2018-06-21 14:41:18

Signature

Serial No.: 51bab676
Issuer: CN=itestin
Subject: CN=itestin
Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

Permission

Request Permission: Accessing Account List Accessing Calendar Accessing GPS Position Accessing Online Locations
Accessing Phone Status and Identity Accessing SD Card Content
Accessing/Altering/Deleting SD Card Content
Adding or Changing the Events in the Calendar and Sending Emails Altering Wi-Fi Status
Auto-starting Automatically Making Phone Calls Checking Network Status Checking Wi-Fi Status
Displaying System Alarm Full Network Access Keeping Phone from Sleep Mode
Managing Account List Searching Running Apps Sending Broadcasts Taking Pictures and Videos
Using Certificates Verifying Accounts com.android.launcher.permission.READ_SETTINGS
com.google.android.c2dm.permission.RECEIVE
com.google.android.providers.gsf.permission.READ_GSERVICES
com.openrice.android.permission.C2D_MESSAGE

Defining permissions: Protect-Level: signature Name: com.openrice.android.permission.C2D_MESSAGE

Results Overview

Repair Suggestions: phase has the risk of being attacked by attackers.
Remove the URL address from APP.

URL List: const-string v0 "Missing required android.permission.INTERNET. Google Analytics disabled. See <http://go.o.gl/8Rd3yj> for instructions"

const-string v1 "If you want to correctly receive onVpadnDismissScreen Callback function, you must set an android.configChanges property of Activity Tag in AndroidManifest.xml file. Reference: <https://developer.android.com/guide/topics/manifest/activity-element.html>"

STATUS_TYPE_COMPLETED = "http://schema.org/CompletedActionStatus"

const-string v1 "Missing google_app_id. Firebase Analytics disabled. See <https://goo.gl/NAOOOI>"

const-string v0 "http://android.azsg.api.opensnap.com"

const-string v2 "https://play.google.com/store/apps/details?id="

const-string v1 "https://www.google.com/dfp/inAppPreview"

const-string v1 "http://schema.org/CompletedActionStatus"

const-string v1 "https://www.googleapis.com/auth/fitness.body.read"

FITNESS_LOCATION_READ_WRITE = "https://www.googleapis.com/auth/fitness.location.write"

SNAP_API_CDN_CHINA = "http://cdn.az.api.opensnap.com.cn"

FACEBOOK_ACTIVITY_NOT_FOUND_REASON = "FacebookActivity is not declared in the AndroidManifest.xml, please add com.facebook.FacebookActivity to your AndroidManifest.xml file. See <https://developers.facebook.com/docs/android/getting-started> for more info."

STATUS_TYPE_FAILED = "http://schema.org/FailedActionStatus"

const-string v0 "http://android.azsg.api.opensnap.com"

const-string v0 "http://api.cn.openrice.com"

const-string v0 "http://cdn.api.snap.hk.openrice.com.cn"

const-string v0 "http://api.jp.openrice.com"

const-string v0 "http://cdn.api.snap.hk.openrice.com"

const-string v0 "http://cdn.azsg.api.opensnap.com"

OR_API_SG_CDN_INTERNATIONAL = "http://cdn.api.snap.sg.openrice.com"

DRIVE_APPFOLDER = "https://www.googleapis.com/auth/drive.appdata"

OR_API_TH = "http://api.th.openrice.com"

PAYPAL = "https://www.paypal.com"

OR_API_HTTPS_CN = "https://api-cn.openrice.com"

const-string v0 "https://api-tw.openrice.com"

const-string v0 "https://.facebook.com"

const-string v0 "http://cdn.api.snap.openrice.com.cn"

const-string v0 "https://api-jp.openrice.com"

const-string v0 "Missing required android.permission.ACCESS_NETWORK_STATE. Google Analytics disabled. See <http://goo.gl/8Rd3yj> for instructions"

const-string v0 "http://api.tw.openrice.com"

const-string v6 "https://www.openrice.com/info/tnc/OR-pp-tc.html"

const-string v0 "https://facebook.com"

const-string v1 "https://www.googleapis.com/auth/drive.apps"

const-string v1 "https://www.googleapis.com/auth/drive.appdata"

const-string v1 "http://mcgw.alipay.com/sdklog.do"

TYPE_SEARCH = "http://schema.org/SearchAction"

const-string v0 "http://api.jp.openrice.com"

const-string v1 "https://git-wip-us.apache.org/repos/asf?p=incubator-cordova-android.git;a=blob;f=framework/res/xml/plugins.xml"

const-string v1 "https://www.googleapis.com/auth/fitness.location.read"

const-string v0 "http://api.cn.openrice.com"

const-string v0 "http://api.sg.openrice.com"

MICROSOFT = "https://login.live.com"

const-string v0 "http://cdn.api.snap.tw.openrice.com.cn"

const-string v0 "http://api.id.openrice.com"

const-string v0 "http://api.sg.openrice.com"

const-string v0 "http://mobilegw-1-64.test.alipay.net/mgw.htm"

OR_API_HK_CDN_CHINA = "http://cdn.api.snap.hk.openrice.com.cn"

const-string v0 "https://graph.%s"

const-string v0 "https://api-sg.openrice.com"

const-string v0 "Quota for bucket exceeded, please view quota on www.firebase.google.com/storage."

const-string v0 "http://cdn.api.snap.my.openrice.com.cn"

const-string v0 "http://schema.org/ViewAction"

const-string v0 "http://cdn.api.snap.my.openrice.com"

const-string v5 "https://ssl.google-analytics.com"

const-string v0 "https://www.googleapis.com/auth/fitness.body.write"

const-string v1 "https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40.html"

const-string v1 "https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/mraid/v2/mraid_app_expanded_banner.js"

const-string v1 "https://www.googleapis.com/auth/fitness.blood_pressure.read"

const-string v0 "https://api.openrice.com"

const-string v0 "http://xmlpull.org/v1/doc/features.html#indent-output"

OR_API_TW_CDN_CHINA = "http://cdn.api.snap.tw.openrice.com.cn"

OR_API_TW_CDN_INTERNATIONAL = "http://cdn.api.snap.tw.openrice.com"

const-string v1 "https://www.google.com/dfp/sendDebugData"

const-string v0 "http://android.az.api.opensnap.com.cn"

const-string v1 "http://hostname/"

const-string v0 "http://cdn.api.snap.ph.openrice.com"

PLUS_ME = "https://www.googleapis.com/auth/plus.me"

const-string v0 "https://mobilegw.alipaydev.com/mgw.htm"

const-string v0 "http://tw.adon.vpon.com/xpon/"

const-string v0 "http://api.in.openrice.com"

const-string v0 "http://api.id.openrice.com"

FITNESS_BODY_READ_WRITE = "https://www.googleapis.com/auth/fitness.body.write"

const-string v3 "https://www.googleapis.com/auth/games"

OR_API_HTTPS_SG = "https://api-sg.openrice.com"

const-string v0 "https://www.google-analytics.com"

const-string v0 "https://www.googleapis.com/auth/fitness.body_temperature.write"

const-string v0 "https://m.uber.com/?action=setPickup&client_id=ySQX8z37PWvmYYnPLXgNHvtsyIRU_Pne&access_token=%1\$s&pickup[latitude]=%2\$s&pickup[longitude]=%3\$s&pickup[nickname]=%4\$s&dropoff[latitude]=%5\$s&dropoff[longitude]=%6\$s&dropoff[nickname]=%7\$s"

const-string v1 "https://facebook.com/device?user_code=%1\$s&q=1"

const-string v1 "!url.toLowerCase().startsWith(http://) && !url.toLowerCase().startsWith(https://)"

const-string v0 "http://cdn.api.snap.sg.openrice.com.cn"

const-string v1 "http://schema.org/CompletedActionStatus"

const-string v0 "http://cdn.api.snap.th.openrice.com"

const-string v1 "Invalid google_app_id. Firebase Analytics disabled. See <https://goo.gl/NAOOOI>. provided id"

const-string v3 "http://icanhazip.com/"

const-string v1 "runTransaction() usage detected while persistence is enabled. Please be aware that transactions *will not* be persisted across database restarts. See <https://www.firebase.com/docs/android/guide/offline-capabilities.html#section-handling-transactions-offline> for more details."

FACEBOOK = "https://www.facebook.com"

const-string v0 "http://mobilegw.aaa.alipay.net/mgw.htm"

const-string v0 "https://www.googleapis.com/auth/fitness.location.write"

const-string v0 "Analytics service at risk of not starting. For more reliable analytics, add the WAKE_LOCK permission to your manifest. See <http://goo.gl/8Rd3yj> for instructions."

OR_API_TH_CDN_CHINA = "http://cdn.api.snap.th.openrice.com.cn"

STATUS_TYPE_COMPLETED = "http://schema.org/CompletedActionStatus"

const-string v5 "https://app-measurement.com/a"

CUSTOM_TAB_REDIRECT_ACTIVITY_NOT_FOUND_REASON = "FacebookActivity is declared incorrectly in the AndroidManifest.xml, please add com.facebook.FacebookActivity to your AndroidManifest.xml file. See

e <https://developers.facebook.com/docs/android/getting-started> for more info."

const-string v1 "https://www.googleapis.com/auth/fitness.location.write"

const-string v1 "http://www.example.com"

const-string v0 "https://api-ph.openrice.com"

OR_API_PH_CDN_CHINA = "http://cdn.api.snap.ph.openrice.com.cn"

const-string v0 "android-app://com.google.android.googlequicksearchbox/https/www.google.com"

TYPE_COMMUNICATE = "http://schema.org/CommunicateAction"

STATUS_TYPE_ACTIVE = "http://schema.org/ActiveActionStatus"

const-string v0 "https://gate.hockeyapp.net/v2/track"

const-string v0 "AnalyticsService is not registered or is disabled. Analytics service at risk of not starting. See <http://goo.gl/8Rd3yj> for instructions."

const-string v0 "Firebase Database encountered an OutOfMemoryError. You may need to reduce the amount of data you are syncing to the client (e.g. by using queries or syncing a deeper path). See https://firebase.google.com/docs/database/ios/structure-data#best_practices_for_data_structure and https://firebase.google.com/docs/database/android/retrieve-data#filtering_data"

const-string v0 "http://www.google.com"

const-string v6 "Provided authentication credentials are invalid. This usually indicates your FirebaseApp instance was not initialized correctly. Make sure your google-services.json file has the correct firebase_url and api_key. You can re-download google-services.json from <https://console.firebase.google.com/>."

const-string v0 "http://api.tw.openrice.com"

const-string v0 "http://api.th.openrice.com"

const-string v2 "https://www.googleapis.com/auth/plus.me"

APP_STATE = "https://www.googleapis.com/auth/appstate"

const-string v0 "http://cdn.api.snap.sg.openrice.com"

CLOUD_SAVE = "https://www.googleapis.com/auth/datastoremobile"

SNAP_API_CDN_INTERNATIONAL = "http://cdn.azsg.api.opensnap.com"

const-string v0 "http://cdn.az.api.opensnap.com.cn"

const-string v0 "https://www.googleapis.com/auth/fitness.nutrition.write"

OR_API_MY_CDN_INTERNATIONAL = "http://cdn.api.snap.my.openrice.com"

const-string v18 "<!doctype html> <html> <head> <meta charset='utf-8'/> <script type='text/javascript' charset='utf-8' src='http://m.vpon.com/sdk/vpadn-sdk-core-v1.js'></script> <script type='text/javascript' charset='utf-8'> VPSDK_LoadSdkConstants(JSON_REPLACE1); VPSDK_BuildAdReqUrl(JSON_REPLACE2); </script><body></body></html>"

const-string v0 "http://play.google.com/store/apps/details?id=com.facebook.orca"

const-string v1 "https://play.google.com/store/apps/details"

const-string v1 "A ContentProvider for this app was not set up in the AndroidManifest.xml, please add %s as a provider to your AndroidManifest.xml file. See <https://developers.facebook.com/docs/sharing/android> for more info."

OR_API_CN_CDN_CHINA = "http://cdn.api.snap.openrice.com.cn"

const-string v0 "https://api.openrice.com"

FITNESS_NUTRITION_READ_WRITE = "https://www.googleapis.com/auth/fitness.nutrition.write"

TWITTER = "https://twitter.com"

const-string v0 "https://www.googleapis.com/auth/fitness.reproductive_health.write"

const-string v0 "http://m.alipay.com/?action=h5quit"

OR_API_HTTPS_MY = "https://api-my.openrice.com"

const-string v1 "https://www.googleapis.com/auth/fitness.blood_glucose.read"

const-string v1 "https://www.googleapis.com/auth/fitness.oxygen_saturation.read"

const-string v0 "https://api-id.openrice.com"

const-string v2 "www.google.com"

FITNESS_NUTRITION_READ = "https://www.googleapis.com/auth/fitness.nutrition.read"

const-string v0 "http://api.ph.openrice.com"

GRAPH_VIDEO_URL_FORMAT = "https://graph-video.%s"

const-string v0 "https://pagead2.googlesyndication.com/pagead/gen_204"

SNAP_API_AZCN = "http://android.az.api.opensnap.com.cn"

const-string v1 "https://www.googleapis.com/auth/fitness.body.write"

const-string v1 "https://www.googleapis.com/auth/fitness.nutrition.read"

YAHOO = "https://login.yahoo.com"

const-string v0 "https://sdk.hockeyapp.net/"

const-string v0 "https://api-th.openrice.com"

const-string v1 "https://imasdk.googleapis.com/admob/sdkloader/native_video.html"

const-string v1 "http://api.map.baidu.com/marker?location="

const-string v0 "AnalyticsReceiver is not registered or is disabled. Register the receiver for reliable dispatching on non-Google Play devices. See <http://goo.gl/8Rd3yj> for instructions."

STATUS_TYPE_ACTIVE = "http://schema.org/ActiveActionStatus"

const-string v0 "http://cdn.api.snap.id.openrice.com"

STATUS_TYPE_FAILED = "http://schema.org/FailedActionStatus"

const-string v1 "FacebookActivity is not declared in the AndroidManifest.xml, please add com.facebook.FacebookActivity to your AndroidManifest.xml file. See <https://developers.facebook.com/docs/android/getting-started> for more info."

const-string v0 "https://graph-video.%s"

const-string v1 "https://www.googleapis.com/auth/games"

const-string v6 "https://www.openrice.com/info/tnc/OR-terms-tc.html"

OR_API_PH_CDN_INTERNATIONAL = "http://cdn.api.snap.ph.openrice.com"

const-string v0 "https://api-sg.openrice.com"

FITNESS_ACTIVITY_READ_WRITE = "https://www.googleapis.com/auth/fitness.activity.write"

const-string v0 "http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=\$OrderId\$&"

OR_API_HTTPS_JP = "https://api-jp.openrice.com"

const-string v3 "https://play.google.com/store/apps/details?id="

OR_API_HTTPS_PH = "https://api-ph.openrice.com"

OR_API_SG_CDN_CHINA = "http://cdn.api.snap.sg.openrice.com.cn"

const-string v1 "!url.toLowerCase().startsWith(http://) && !url.toLowerCase().startsWith(https://)"

const-string v0 "https://api-in.openrice.com"

const-string v0 "https://api-in.openrice.com"

LINKEDIN = "https://www.linkedin.com"

const-string v7 "https://www.openrice.com/info/tnc/OR-terms-tc.html"

const-string v0 "https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps"

OR_API_MO = "http://api.openrice.com"

const-string v1 "http://hostname?"

const-string v0 "http://th.openrice.com/static/truehit.html"

const-string v0 "http://xmlpull.org/v1/doc/features.html#indent-output"

const-string v0 "http://schemas.android.com/apk/lib/com.google.android.gms.plus"

const-string v1 "https://www.googleapis.com/auth/drive.file"

const-string v0 "http://cdn.api.snap.tw.openrice.com"

const-string v14 "<!doctype html> <html> <head> <meta charset='utf-8'/> <script type='text/javascript' charset='utf-8' src='http://m.vpon.com/sdk/vpadn-sdk-core-v1.js'></script> <script type='text/javascript' charset='utf-8'> VPSDK_LoadSdkConstants(JSON_REPLACE1); VPSDK_BuildAdReqUrl(JSON_REPLACE2); </script><body></body></html>"

TYPE_LIKE = "http://schema.org/LikeAction"

OR_API_JP = "http://api.jp.openrice.com"

const-string v0 "http://api.ph.openrice.com"

const-string v0 "https://www.google.com"

GOOGLE = "https://accounts.google.com"

const-string v1 "https://www.googleapis.com/auth/fitness.activity.read"

const-string v6 "https://www.openrice.com/info/tnc/OR-pp-tc.html"

GAMES = "https://www.googleapis.com/auth/games"

OR_API_HTTPS_TH = "https://api-th.openrice.com"

OR_API_ID_CDN_CHINA = "http://cdn.api.snap.id.openrice.com.cn"

OR_API_HTTPS_MO = "https://api.openrice.com"

const-string v0 "https://accounts.google.com"

const-string v0 "https://api-my.openrice.com"

const-string v0 "http://mobilegw.stable.alipay.net/mgw.htm"

const-string v1 "https://csi.gstatic.com/csi"

const-string v0 "CampaignTrackingReceiver is not registered, not exported or is disabled. Installation campaign tracking is not possible. See <http://goo.gl/8Rd3yj> for instructions."

const-string v1 "https://www.googleapis.com/auth/fitness.nutrition.read"

TYPE_ACTIVATE = "http://schema.org/ActivateAction"

TYPE_VIEW = "http://schema.org/ViewAction"

OR_API_MY_CDN_CHINA = "http://cdn.api.snap.my.openrice.com.cn"

const-string v0 "https://api-th.openrice.com"

const-string v1 "http://img.youtube.com/vi/"

const-string v1 "https://www.googleapis.com/auth/fitness.reproductive_health.read"

const-string v1 "https://www.googleapis.com/auth/fitness.activity.write"

const-string v1 "https://www.googleapis.com/auth/games"

const-string v0 "https://api-cn.openrice.com"

const-string v1 "https://sdk.hockeyapp.net/"

const-string v1 "https://www.google.com/dfp/linkDevice"

OR_API_IN_CDN_CHINA = "http://cdn.api.snap.in.openrice.com.cn"

const-string v5 "http://www.google-analytics.com"

const-string v0 "http://cdn.api.snap.in.openrice.com.cn"

const-string v1 "https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/mraid/v2/mraid_app_banner.js"

const-string v1 "https://www.googleapis.com/auth/games_lite"

const-string v1 "http://cn.adon.vpon.com/xpon/activity"

const-string v0 "https://play.google.com/store/apps/details"

const-string v0 "Hit delivery not possible. Missing network permissions. See <http://goo.gl/8Rd3yj> for instructions"

OR_API_CN = "http://api.cn.openrice.com"

FITNESS_BODY_READ = "https://www.googleapis.com/auth/fitness.body.read"

const-string v2 "https://www.googleapis.com/auth/games"

const-string v0 "https://api-cn.openrice.com"

const-string v3 "http://maps.google.com/maps?daddr="

const-string v0 "https://api-id.openrice.com"

OR_API_ID_CDN_INTERNATIONAL = "http://cdn.api.snap.id.openrice.com"

const-string v0 "https://api-my.openrice.com"

OR_API_HK = "http://api.openrice.com"

const-string v0 "https://www.googleapis.com/auth/fitness.blood_pressure.write"

const-string v0 "https://orga.openrice.com"

TYPE_ADD = "http://schema.org/AddAction"

OR_API_HTTPS_HK = "https://api.openrice.com"

TYPE_WANT = "http://schema.org/WantAction"

const-string v14 "<!doctype html> <html> <head> <meta charset='utf-8'/> <script type='text/javascript' charset='utf-8' src='http://m.vpon.com/sdk/vpadn-sdk-core-v1.js'></script> <script type='text/javascript' charset='utf-8'> VPSDK_LoadSdkConstants(JSON_REPLACE1); VPSDK_BuildAdReqUrl(JSON_REPLACE2); </script><body></body></html>"

const-string v0 "http://cn.adon.vpon.com/xpon/"

SNAP_API_AZSG = "http://android.azsg.api.opensnap.com"

const-string v0 "http://android.azsg.uat.api.opensnap.com"

const-string v0 "http://api.openrice.com"

const-string v0 "https://mobilegw.alipay.com/mgw.htm"

const-string v1 "http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=\$OrderId&"

OR_API_IN_CDN_INTERNATIONAL = "http://cdn.api.snap.in.openrice.com"

FITNESS_ACTIVITY_READ = "https://www.googleapis.com/auth/fitness.activity.read"

const-string v0 "https://plus.google.com/"

const-string v0 "https://www.googleapis.com/auth/games.firstparty"

const-string v1 "https://www.google.com/dfp/debugSignals"

const-string v1 "https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/native_ads.html"

const-string v0 "http://schemas.android.com/apk/lib/com.google.android.gms.plus"

PLUS_LOGIN = "https://www.googleapis.com/auth/plus.login"

const-string v1 "!url.toLowerCase().startsWith(http://) && !url.toLowerCase().startsWith(https://)"

const-string v0 "https://api-ph.openrice.com"

const-string v0 "http://api.my.openrice.com"

OR_API_PH = "http://api.ph.openrice.com"

const-string v1 "http://schema.org/ViewAction"

const-string v1 "http://schema.org/ViewAction"

const-string v1 "https://www.googleapis.com/auth/fitness.body_temperature.read"

const-string v1 "https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/mraid/v2/mraid_app_interstitial.js"

const-string v1 "https://www.googleapis.com/auth/fitness.activity.read"

const-string v1 "https://www.googleapis.com/auth/fitness.location.read"

const-string v1 "FacebookActivity is declared incorrectly in the AndroidManifest.xml, please add com.facebook.FacebookActivity to your AndroidManifest.xml file. See <https://developers.facebook.com/docs/android/getting-started> for more info."

OR_API_IN = "http://api.in.openrice.com"

const-string v0 "http://api.openrice.com"

const-string v0 "http://cdn.api.snap.in.openrice.com"

const-string v0 "https://www.googleapis.com/auth/fitness.oxygen_saturation.write"

const-string v0 "https://www.googletagmanager.com"

const-string v1 "https://www.googleapis.com/auth/games.firstparty"

const-string v0 "https://www.googleapis.com/auth/games"

UBER_RIDE_URL = "https://m.uber.com/?action=setPickup&client_id=ySQX8z37PWvmYYnPLXgNHvtsyIR
U_Pne&access_token=%1\$s&pickup[latitude]=%2\$s&pickup[longitude]=%3\$s&pickup[nickname]=%4\$s
&dropoff[latitude]=%5\$s&dropoff[longitude]=%6\$s&dropoff[nickname]=%7\$s"

const-string v1 "https://www.googleapis.com/auth/fitness.body.read"

const-string v5 "https://www.openrice.com/info/tnc/OR-terms-tc.html"

OR_API_CN_CDN_INTERNATIONAL = "http://cdn.api.snap.openrice.com.cn"

const-string v0 "http://api.in.openrice.com"

const-string v0 "http://cdn.api.snap.openrice.com.cn"

const-string v0 "https://www.googleapis.com/auth/fitness.activity.write"

const-string v0 "http://www.opensnap.com/about_opensnap/web/images/inx_snap_ico.png"

CONTENT_PROVIDER_NOT_FOUND_REASON = "A ContentProvider for this app was not set up in the Andr
oidManifest.xml, please add %s as a provider to your AndroidManifest.xml file. See [https://developers.face
book.com/docs/sharing/android](https://developers.face
book.com/docs/sharing/android) for more info."

const-string v1 "!url.toLowerCase().startsWith(http://) && !url.toLowerCase().startsWith(https://)"

TYPE_FILM = "http://schema.org/FilmAction"

const-string v0 "http://api.my.openrice.com"

const-string v6 "<!DOCTYPE html> <html> <head> <meta charset='utf-8'><script type='text/javascript'
charset='utf-8' src='http://m.vpon.com/sdk/vpadn-sdk-util-v1.js'> </script></head> <body> <script ty
pe='text/javascript'> var hookEvent; hookEvent = function(ret) { REPLACE_JS_CLICK }; vpsdk.addEventList
ener('ready', hookEvent); </script> </body> </html>"

const-string v0 "http://android.az.api.opensnap.com.cn"

const-string v1 "https://www.googleapis.com/auth/fitness.nutrition.write"

const-string v5 "https://www.openrice.com/info/tnc/OR-pp-tc.html"

OR_API_HTTPS_ID = "https://api-id.openrice.com"

const-string v0 "IllegalStateException getting Ad Id Info. If you would like to see Audience reports, please
ensure that you have added '<meta-data android:name='com.google.android.gms.version' android:val
ue='@integer/google_play_services_version' />' to your application manifest file. See <http://goo.gl/naFqQk>
for details."

const-string v1 "http://tw.adon.vpon.com/xpon/activity"

const-string v0 "http://cdn.api.snap.th.openrice.com.cn"

FITNESS_LOCATION_READ = "https://www.googleapis.com/auth/fitness.location.read"

OR_API_MY = "http://api.my.openrice.com"

const-string v1 "https://www.googleapis.com/auth/plus.login"

OR_API_TH_CDN_INTERNATIONAL = "http://cdn.api.snap.th.openrice.com"

const-string v0 "http://schemas.android.com/apk/res/android"

const-string v4 "https://play.google.com/store/apps/details?id="

const-string v3 "https://www.googleapis.com/auth/games.firstparty"

GRAPH_URL_FORMAT = "https://graph.%s"

const-string v2 "https://www.googleapis.com/auth/plus.login"

const-string v1 "http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=\$OrderId\$&"

const-string v0 "http://mobilegw.alipay.com/mgw.htm"

OR_API_ID = "http://api.id.openrice.com"

const-string v1 "https://www.googleapis.com/auth/plus.me"

const-string v0 "http://cdn.api.snap.ph.openrice.com.cn"

const-string v0 "AnalyticsService not registered in the app manifest. Hits might not be delivered reliably. See <http://goo.gl/8Rd3yj> for instructions."

const-string v0 "https://api-jp.openrice.com"

TYPE_LISTEN = "http://schema.org/ListenAction"

OR_API_HTTPS_TW = "https://api-tw.openrice.com"

const-string v0 "https://www.facebook.com"

const-string v0 "http://cdn.api.snap.id.openrice.com.cn"

const-string v0 "https://api-tw.openrice.com"

const-string v5 "https://mobilecrashreporting.googleapis.com/v1/crashes:batchCreate?key="

const-string v1 "https://www.googleapis.com/auth/drive"

const-string v1 "http://schema.org/CompletedActionStatus"

TYPE_RESERVE = "http://schema.org/ReserveAction"

TYPE_PHOTOGRAPH = "http://schema.org/PhotographAction"

const-string v1 "https://support.google.com/dfp_premium/answer/7160685#push"

OR_API_HK_CDN_INTERNATIONAL = "http://cdn.api.snap.hk.openrice.com"

TYPE_WATCH = "http://schema.org/WatchAction"

TYPE_BOOKMARK = "http://schema.org/BookmarkAction"

const-string v0 "http://api.th.openrice.com"

const-string v0 "http://localhost"

DRIVE_FILE = "https://www.googleapis.com/auth/drive.file"

OR_API_TW = "http://api.tw.openrice.com"

OR_API_HTTPS_IN = "https://api-in.openrice.com"

OR_API_SG = "http://api.sg.openrice.com"

const-string v1 "http://www.example.com"

const-string v0 "https://www.googleapis.com/auth/fitness.blood_glucose.write"

const-string v1 "http://hostname/?"

[Medium] Residue apk file

1 risks

Risk Details: There is a risk of leaking sensitive information such as IP and Email when there are unnecessary APK files remained in APP.

Repair Suggestions: Remove the unnecessary APK files from APP.

File Path: /res/raw/android_wear_micro_apk.apk

[Medium] Secret key hard coded

36 risks

Risk Details: There are plaintext secret keys in the APP, the attacker can decrypt the data with the secret key, and there is the risk of sensitive data information leakage.

Repair Suggestions: 1. Avoid storing secret keys in plaintext in code. 2. Strengthen the APP.

Risk Code: **com.facebook.internal.FacebookSignatureValidator.FBF_HASH**

FBF_HASH = "2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3"

com.facebook.internal.FacebookSignatureValidator.FBI_HASH

FBI_HASH = "a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc"

com.facebook.internal.FacebookSignatureValidator.FBL2_HASH

FBL2_HASH = "df6b721c8b4d3b6eb44c861d4415007e5a35fc95"

com.facebook.internal.FacebookSignatureValidator.FBL_HASH

FBL_HASH = "5e8f16062ea3cd2c4a0d547876baa6f38cabf625"

com.facebook.internal.FacebookSignatureValidator.FBR2_HASH

FBR2_HASH = "cc2751449a350f668590264ed76692694a80308a"

com.facebook.internal.FacebookSignatureValidator.FBR_HASH

FBR_HASH = "8a3c4b262d721acd49a4bf97d5213199c86fa2b9"

com.facebook.internal.FacebookSignatureValidator.MSR_HASH

MSR_HASH = "9b8f518b086098de3d77736f9458a3d2f6f95a37"

com.google.android.gms.internal.zzdhw.zzbng

const-string v0 "115792089210356248762697446949407573530086143415290314195533631308867097853951"

com.facebook.internal.FacebookSignatureValidator.buildAppSignatureHashes : 57

const-string v0 "2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3"

com.google.android.gms.internal.zzdhw.zzbnh

const-string v0 "39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319"

com.facebook.internal.FacebookSignatureValidator.buildAppSignatureHashes : 54

const-string v0 "5e8f16062ea3cd2c4a0d547876baa6f38cabf625"

com.google.android.gms.internal.zzdhw.zzbni

const-string v0 "6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151"

com.google.android.gms.internal.zzdhw.zzbng

const-string v3 "6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296"

com.google.android.gms.internal.zzdhw.zzbnh

const-string v3 "aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7"

com.google.android.gms.internal.zzdhw.zzbni

const-string v3 "c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66"

com.google.android.gms.internal.zzdhw.zzbni

const-string v4 "11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650"

com.google.android.gms.internal.zzdhw.zzbnh

const-string v4 "3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f"

com.google.android.gms.internal.zzdhw.zzbng

const-string v4 "4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5"

[Low] Local database SQL injection

4 risks

Risk Details: There is a risk of local database injection when APP using.rawQuery or execSql to execute SQL queries.

Repair Suggestions: Avoid using.rawQuery Or execSql.

Risk Code: **com.google.android.gms.internal.zzcrx.zza**
invoke-virtual {p0 v0 v1} Landroid/database/sqlite/SQLiteDatabase;.rawQuery (Ljava/lang/String; [Ljava/lang/String;)Landroid/database/Cursor;
SQL: "SELECT * FROM " + p1 + " WHERE 0"

com.google.android.gms.internal.zzane.zzb
invoke-virtual {p0 v3 v0} Landroid/database/sqlite/SQLiteDatabase;.rawQuery (Ljava/lang/String; [Ljava/lang/String;)Landroid/database/Cursor;
SQL: "SELECT * FROM " + p1 + " LIMIT 0"

com.google.android.gms.internal.zzcw.zzg
invoke-virtual {v1 v0 v2} Landroid/database/sqlite/SQLiteDatabase;.rawQuery (Ljava/lang/String; [Ljava/lang/String;)Landroid/database/Cursor;
SQL: "select app_id, metadata_fingerprint from raw_events where " + "select app_id, metadata_fingerprint from raw_events where " + "app_id in (select app_id from apps where config_fetched_time >= ?) order by rowid limit 1;"

com.google.android.gms.internal.zzcay.zzb
invoke-virtual {p0 v3 v0} Landroid/database/sqlite/SQLiteDatabase;.rawQuery (Ljava/lang/String; [Ljava/lang/String;)Landroid/database/Cursor;
SQL: "SELECT * FROM " + p1 + " LIMIT 0"

[Low] PendingIntent hijacking

1 risks

Risk Details: APP uses empty Intent to construct 'PendingIntent' and handed to other APPs, will be tampered with by other APPs, there is the risk of the embezzled permission.

Repair Suggestions: 1. Avoid using 'Intent' with unset 'action' and 'component' to construct 'PendingIntent'. 2. Avoid using 'Intent' with seted action unset 'component' to construct 'Pendingintent' which 'flag' is FILL_IN_ACTION. 3. Avoid using 'Intent' with seted 'component' construct 'PendingIntent' which 'flag' is FILL_IN_COMPONENT.

Risk Code:

u.` : 147

```
invoke-static {p1 v0 v7 v1} Landroid/app/PendingIntent; getActivity (Landroid/content/Context; I Landroi  
d/content/Intent; I)Landroid/app/PendingIntent;
```

Encryption Security

— [Medium] AES/DES weak encryption

2 risks

Risk Details: When APP uses the AES/DES encryption algorithm, there is a risk that encrypted data is cracked if you use the ECB mode.

Repair Suggestions: Use CBC (group link) or CFB (password feedback) encryption mode.

Risk Code:

com.google.android.gms.internal.zzdhu.<init>

```
invoke-static {v0} Ljavax/crypto/Cipher; getInstance (Ljava/lang/String;)Ljavax/crypto/Cipher;  
v0 = "AES/ECB/NOPADDING"
```

com.google.android.gms.internal.zzdhu.zzd

```
invoke-static {v0} Ljavax/crypto/Cipher; getInstance (Ljava/lang/String;)Ljavax/crypto/Cipher;  
v0 = "AES/ECB/NOPADDING"
```

— [Medium] Insecure hash algorithm

18 risks

Risk Details: When APP uses the MD5/SHA-1 encryption algorithm, there is a risk of encrypted data being collided.

Repair Suggestions: Use SHA-256 to encrypt data.

Risk Code:

com.google.android.gms.tagmanager.zzbw.zzp

```
invoke-static {v6} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDi  
gest;  
v6 = "MD5"
```

ai.toString : 1026

```
invoke-static {v0} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDi  
gest;  
v0 = "MD5"
```

com.google.android.gms.internal.zzbv.run

```
invoke-static {v0} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDi  
gest;  
v0 = "MD5"
```

com.google.android.gms.internal.zzajf.zzcp

```
invoke-static {v0} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDi  
gest;  
v0 = "MD5"
```

com.openrice.android.ui.activity.uploadPhoto.Util.hashKeyFromPathName : 171

```
invoke-static {v0} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDi
```


gest;
v0 = "MD5"

com.google.android.gms.internal.zzcyl.zza

invoke-static {v5} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;
gest;
v5 = "MD5"

com.squareup.okhttp.internal.Util. : 216

invoke-static {v0} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;
gest;
v0 = "MD5"

okio.ByteString.toString : 249

invoke-static {v2} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;
gest;
v2 = "MD5"

com.google.firebase.iid.FirebaseInstanceId.zza

invoke-static {v0} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;
gest;
v0 = "SHA1"

com.google.android.gms.iid.InstanceID.zza

invoke-static {v0} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;
gest;
v0 = "SHA1"

com.openrice.android.network.ApiManager.md5 : 143

invoke-static {v0} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;
gest;
v0 = "MD5"

vpadn.au.a : 1073

invoke-static {v0} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;
gest;
v0 = "MD5"

120 : '■

invoke-static {v0} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;
gest;
v0 = "MD5"

com.google.android.gms.internal.zzahg.zzqx

invoke-static {v0} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;
gest;
v0 = "MD5"

com.facebook.appevents.AppEvent.md5Checksum : 280

invoke-static {v0} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;
gest;
v0 = "MD5"

com.google.android.gms.internal.zzgk.zzgx

invoke-static {v0} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;
gest;
v0 = "MD5"

com.openrice.android.network.utils.DeviceUtil.encrypt : 56

```
invoke-static {v0} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;
v0 = "MD5"
```

net.hockeyapp.android.LoginActivity. : 191

```
invoke-static {v0} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;
v0 = "MD5"
```

— **[Medium] Signature Weak encryption**

1 risks

Risk Details: APP uses SHA-1 signature algorithm to sign, there is the risk of being cracked.

Repair Suggestions: Sign with SHA-256.

Related Data: Encryption Type: [SHA1withRSA](#)

Code Security

— **[High] WebView Remote Code Execution**

2 risks

Risk Details: APP using 'addJavascriptInterface' method when the Android API level ≤ 16 , there is a risk of information leakage and remote control.

Repair Suggestions: 1. Avoid using the addJavascriptInterface when API level is 16 and lower. 2. Ensure that trusted JavaScript is loaded.

Risk Code: **com.google.android.gms.internal.zzakz.<init>**

```
invoke-virtual {p0 v0 v1} Lcom/google/android/gms/internal/zzakz; addJavascriptInterface (Ljava/lang/Object; Ljava/lang/String;)V
```

vpadn.f.j : 397

```
invoke-virtual {p0 v0 v1} Lvpadn/f; addJavascriptInterface (Ljava/lang/Object; Ljava/lang/String;)V
```

— **[High] WebView Unverified HTTPS Certificate**

3 risks

Risk Details: The APP's WebView certificate authentication error, the page was not stopped loading, there is a man-in-the-middle attack risk.

Repair Suggestions: Use 'handler.cancel()' to stop loading the problem page.

Risk Code: **v.onReceivedSslError : 48**

```
invoke-virtual {p2} Landroid/webkit/SslErrorHandler; proceed ()V
```

Risk: invoke proceed() on SSL Error

vpadn.g.onReceivedSslError : 399

```
invoke-virtual {p2} Landroid/webkit/SslErrorHandler; proceed ()V
```

Risk: invoke proceed() on SSL Error

com.alipay.sdk.auth.AuthActivity\$IF.onReceivedSslError : 193

```
invoke-virtual {p2} Landroid/webkit/SslErrorHandler; proceed ()V
```

Risk: invoke proceed() on SSL Error

Risk Details: APP using 'addJavascriptInterface' method when the Android API level ≤ 16, there is a risk of information leakage and remote control when the dangerous interface is not removed.

Repair Suggestions: 1. Avoid using 'addJavascriptInterface' in API level ≤ 16. 2. When you have to use addJavascriptInterface, ensure that remove the searchBoxJavaBridge_, accessibility and accessibilityTraversal

Risk Code: com.google.android.gms.internal.zzakz.<init>
invoke-virtual {p0 v0 v1} Lcom/google/android/gms/internal/zzakz; addJavascriptInterface (Ljava/lang/Object; Ljava/lang/String;)V
vpadn.f.j : 397
invoke-virtual {p0 v0 v1} Lvpadn/f; addJavascriptInterface (Ljava/lang/Object; Ljava/lang/String;)V

Risk Details: When APP calls an API to get user privacy information, there is a risk of user privacy leakage.

Repair Suggestions: Confirm that calling sensitive function behavior is authorized by the user.

Risk Code: vpadn.bp.e : 79
invoke-virtual {v2} Landroid/telephony/TelephonyManager; getCellLocation ()Landroid/telephony/CellLocation;
vpadn.bp.f : 95
invoke-virtual {v2} Landroid/telephony/TelephonyManager; getCellLocation ()Landroid/telephony/CellLocation;
□. : 35
invoke-virtual {v2} Landroid/telephony/TelephonyManager; getDeviceId ()Ljava/lang/String;
com.google.android.gms.cast.zzu.onRouteUnselected
invoke-virtual {v1} Lcom/google/android/gms/cast/CastDevice; getDeviceId ()Ljava/lang/String;
478 : █
invoke-virtual {p2} Landroid/view/KeyEvent; getDeviceId ()
vpadn.bm.e : 98
invoke-virtual {v3} Landroid/telephony/TelephonyManager; getDeviceId ()Ljava/lang/String;
com.newrelic.agent.android.harvest.crash.DeviceInfo.<init> : 43
invoke-virtual {p1} Lcom/newrelic/agent/android/harvest/DeviceInformation; getDeviceId ()Ljava/lang/String;
□.<init> : 38
invoke-virtual {v3} Landroid/telephony/TelephonyManager; getDeviceId ()Ljava/lang/String;
□.□
invoke-virtual {p0} Landroid/telephony/TelephonyManager; getDeviceId ()Ljava/lang/String;
com.google.android.gms.people.protomodel.zzc.equals
invoke-interface {v3} Lcom/google/android/gms/people/protomodel/zza; getDeviceId ()Ljava/lang/String;
com.google.android.gms.internal.zzbap.zza
invoke-virtual {v3} Lcom/google/android/gms/cast/CastDevice; getDeviceId ()Ljava/lang/String;
com.google.android.gms.cast.zzu.onRouteUnselected

invoke-virtual {v0} Lcom/google/android/gms/cast/CastDevice; getDeviceId ()Ljava/lang/String;

com.google.android.gms.people.protomodel.zzc.equals

invoke-interface {p0} Lcom/google/android/gms/people/protomodel/zza; getDeviceId ()Ljava/lang/String ;

■.□

invoke-virtual {v2} Landroid/telephony/TelephonyManager; getDeviceId ()Ljava/lang/String;

com.google.android.gms.people.protomodel.zzc.hashCode

invoke-interface {v3} Lcom/google/android/gms/people/protomodel/zza; getDeviceId ()Ljava/lang/String;

1407 : '■

invoke-virtual {p2} Landroid/view/KeyEvent; getDeviceId ()

com.vpadn.ads.VpadnAdRequest.isTestDevice : 345

invoke-virtual {v2} Landroid/telephony/TelephonyManager; getDeviceId ()Ljava/lang/String;

com.google.android.gms.cast.zzq.zza

invoke-virtual {v3} Lcom/google/android/gms/cast/CastDevice; getDeviceId ()Ljava/lang/String;

└.□ : 668

invoke-virtual {v0 v1} Landroid/content/pm/PackageManager; getInstalledPackages ()Ljava/util/List;

└.□ : 281

invoke-virtual {v0 v1} Landroid/content/pm/PackageManager; getInstalledPackages ()Ljava/util/List;

com.google.android.gms.internal.zzacj.zzm

invoke-virtual {v2} Landroid/telephony/TelephonyManager; getNetworkOperator ()Ljava/lang/String;

vpadn.bp.a : 14

invoke-virtual {v2} Landroid/telephony/TelephonyManager; getNetworkOperator ()Ljava/lang/String;

vpadn.bp.c : 45

invoke-virtual {v2} Landroid/telephony/TelephonyManager; getNetworkOperator ()Ljava/lang/String;

com.google.android.gms.internal.zzacj.zzm

invoke-virtual {v2} Landroid/telephony/TelephonyManager; getPhoneType ()

com.google.android.gms.internal.zzbpr.zzcx

invoke-virtual {v0} Landroid/telephony/TelephonyManager; getPhoneType ()

e.` : 214

invoke-virtual {v2} Landroid/telephony/TelephonyManager; getPhoneType ()

□.<init> : 39

invoke-virtual {v3} Landroid/telephony/TelephonyManager; getSubscriberId ()Ljava/lang/String;

□.□ : 54

invoke-virtual {v2} Landroid/telephony/TelephonyManager; getSubscriberId ()Ljava/lang/String;

└.:

invoke-virtual {p0} Landroid/telephony/TelephonyManager; getSubscriberId ()Ljava/lang/String;

Risk Details: When the APP's WebView turns on debug mode, there is a risk of being debugged.

Repair Suggestions: Remove the 'setWebContentsDebuggingEnabled(true)'.

Risk Code: vpadn.dg.i : 136

invoke-static {v0} Landroid/webkit/WebView; setWebContentsDebuggingEnabled (Z)V
v0 = 0x1

Component Security



— [Medium] Activity component exposure

5 risks

Risk Details: The 'Activity' component exported by APP does not have reasonable permissions, there is a risk that functionality is abused or information is leaked.

Repair Suggestions: 1. Avoid exporting 'Activity' components. 2. Set reasonable permissions when you have to export the 'Activity' component.

Related Data: Component Type: **Activity**
Component Name: **com.openrice.android.ui.activity.settings.region.RegionPickerActivity**
Reason for Export: **intent-filter**

Component Type: **Activity**
Component Name: **com.openrice.android.push.DeepLinkActivity**
Reason for Export: **intent-filter**

Component Type: **Activity**
Component Name: **com.alipay.sdk.app.PayResultActivity**
Reason for Export: **android:exported=true**

Component Type: **Activity**
Component Name: **com.google.android.gms.appinvite.PreviewActivity**
Reason for Export: **android:exported=true**

Component Type: **Activity**
Component Name: **com.google.android.gms.tagmanager.TagManagerPreviewActivity**
Reason for Export: **android:exported=true**

— [Medium] Broadcast component exposure

2 risks

Risk Details: The 'BroadcastReceiver' component exported by APP does not have reasonable permissions, there is a risk that functionality is abused or information is leaked.

Repair Suggestions: Set reasonable invocation permissions for exported 'Broadcastreceiver' component.

Related Data: Component Type: **Broadcast Receiver**
Component Name: **com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver**
Reason for Export: **android:exported=true**

Component Type: **Broadcast Receiver**
Component Name: **com.google.firebase.iid.FirebaseInstanceIdReceiver**
Reason for Export: **android:exported=true**

— [Medium] Service component exposure

6 risks

Risk Details: The APP defines the exported 'Service' component, and there is a risk of functionality being abused.

Repair Suggestions: 1. Avoid exporting 'Service' components. 2. Set reasonable invocation permissions when you have to export the 'Service' component.

Related Data:

Component Type: [Service](#)

Component Name: [com.openrice.android.push.OpenRiceFcmlIntentService](#)

Reason for Export: [intent-filter](#)

Component Type: [Service](#)

Component Name: [com.openrice.android.push.OpenRiceInstanceDLListenerService](#)

Reason for Export: [intent-filter](#)

Component Type: [Service](#)

Component Name: [com.openrice.android.service.ORWearableListenerService](#)

Reason for Export: [intent-filter](#)

Component Type: [Service](#)

Component Name: [com.google.android.gms.auth.api.signin.RevocationBoundService](#)

Reason for Export: [android:exported=true](#)

Component Type: [Service](#)

Component Name: [com.google.firebase.messaging.FirebaseMessagingService](#)

Reason for Export: [android:exported=true](#)

Component Type: [Service](#)

Component Name: [com.google.firebase.iid.FirebaseInstanceIdService](#)

Reason for Export: [android:exported=true](#)

Configuration Security

[High] Proxy environment identification

1 risks

Risk Details: When APP does not detect network proxies, insecure network proxy may hijack the communication data, there is a risk of man-in-the-middle hijacking.

Repair Suggestions: Prompts the user when using proxy.

[Medium] Root environment identification

1 risks

Risk Details: When the APP runs in the Root environment, it can read in-memory data, and there is a risk of information leakage.

Repair Suggestions: Prompts the user when running in Root environment.

[Low] Unnecessary runtime permissions

4 risks

Risk Details: APP requests unnecessary runtime permissions to increase the attack surface.

Repair Suggestions: Remove the unnecessary permissions.

Request Permission: [Searching Running Apps](#) [Displaying System Alarm](#) [Accessing Phone Status and Identity](#) [Automatically Making Phone Calls](#)



[High] Server-side certificate weak validation

2 risks

Risk Details: The APP uses HTTPS to submit data without verifying the certificate, and an attacker can falsify an HTTPS certificate with a man-in-the-middle attack risk.

Repair Suggestions: Custom the 'SSL X509TrustManager', using 'checkServerTrusted' method verifies the certificate on the server side.

Risk Code: `c.FileTransfer$3.checkServerTrusted`

`□$`2.checkServerTrusted`

[Medium] Host name weak validation



1 risks

Risk Details: APP submits the data without verifying the target domain name, the attacker can falsify domain name or IP, there is the risk of man-in-the-middle attack.

Repair Suggestions: 1. Must use STRICT_HOSTNAME_VERIFIER and verify the certificate. 2.Reasonable override the 'HostnameVerifier.verifier(...)'.
3. Reasonable override the 'HostnameVerifier.verifier(...)'.

Risk Code: `c.FileTransfer$2.verify`

If you have questions about the contents of the report or need other customized security testing, please contact us

 Email: seconsult@testin.cn  Phone number: 400-900-5577