App Security Scanning Report

Application Information

Kaodim Beta

com.kaodim.kaodimuserapp.beta

Application

Version:	3.6.0.beta2.staging (build 241)	Application Type:	Android - APK
Size:	13.01 MB	Detection Category:	App Security Scanning
MD5:	04B494A55F3C86BFFB69C41C591317E3	Detection Time:	2018-07-12 12:26:50

Signature

Serial No.: 4c4537ef
Issuer: CN=Android Debug, O=Android, C=US
Subject: CN=Android Debug, O=Android, C=US
Signature Algorithm:SHA256withRSA, OID = 1.2.840.113549.1.1.11

Permission

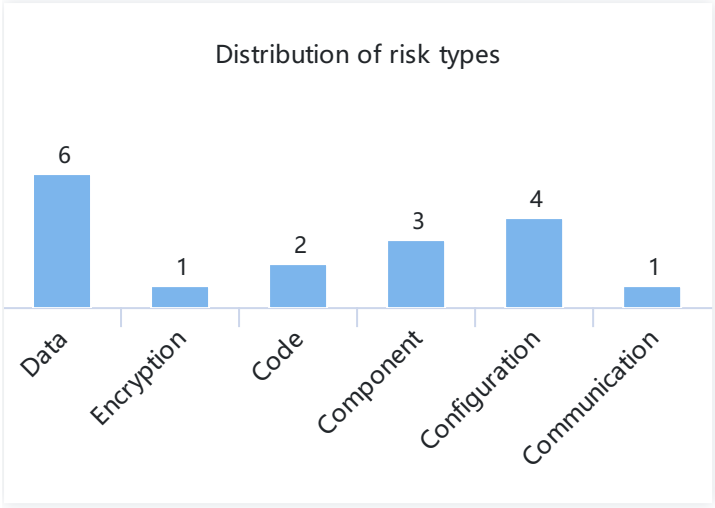
Request Permission: Accessing Account List Accessing GPS Position Accessing Phone Status and Identity Accessing SD Card Content Accessing/Altering/Deleting SD Card Content Automatically Making Phone Calls Checking Network Status Checking Wi-Fi Status Displaying System Alarm Full Network Access Keeping Phone from Sleep Mode Taking Pictures and Videos com.google.android.c2dm.permission.RECEIVE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE com.kaodim.kaodimuserapp.beta.permission.C2D_MESSAGE

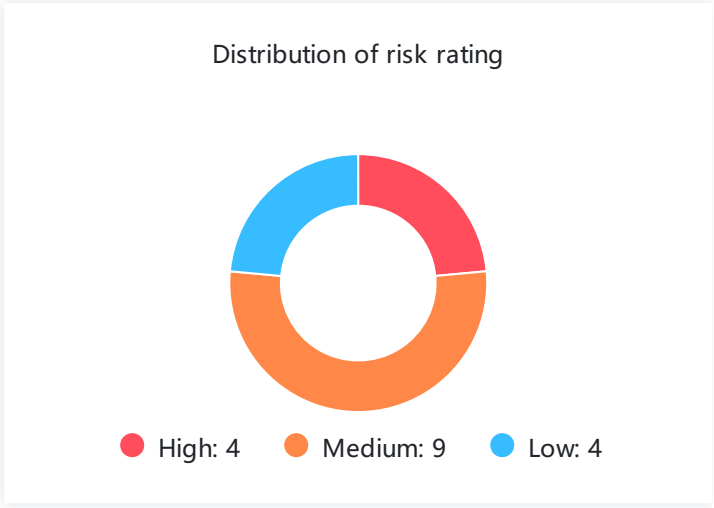
Defining permissions:Protect-Level:signature Name: com.kaodim.kaodimuserapp.beta.permission.C2D_MESSAGE

Results Overview

Security Score: 47

Risk Description: Common detection 40 items. Found 17 Risks





Data Security

[Medium] Residual Email — 9 risks

Risk Details: The email address which remain in the APP's configuration file during development or testing phase has the risk of conducting phishing attack

Repair Suggestions: Remove the Email address from APP.

mailing List:

const-string v15 "Limited exceeded. Please contact support@firebase.com."

const-string v2 "You have enabled persistence, but persistence is not supported on this platform. If you ha ve any questions around persistence please contact support@firebase.com."

const-string v2 "). Please report to support@firebase.com"

const-string v3 "An unexpected error occurred. Please contact support@firebase.com. Details: "

const-string v3 "Something went wrong, please report to support@firebase.com"

const-string v3 "An unexpected error occurred. Please contact support@firebase.com. Details: "

const-string v0 "0□□¨0□□□ □□□□□ □Õ□¸l}ÓNõ0□□ *□H□÷□□□□□□0□□1□0 □□U□□□□US1□0□□□U□□□ California1□0□□□U□□□□Mountain View1□0□□□U□ □□Android1□0□□□U□□□□Android1□0□□□U□□□□Android1"0 □ *□H□÷□□ □□□android@android.com0□□□080415233656Z□□350901233656Z0□□1□0 □□U□□ □□US1□0□□□U□□□□ California1□0□□□U□□□□Mountain View1□0□□□U□ □□Android1□0□□□U□□□□Android1□0□□□U□□□□Android1"0 □ *□H□÷□□ □□□android@android.com0□□ 0□□ *□H□÷□□□□□□□□□□□□0□□□□□□□□ÖÎ.□ ¿â1MÑ□³ÍÓ□\´=3ú□tá½¶ÑÛ□□ö,\9ßVøF□=e¾ÀóÊBk□Å¨íZ9□ÁgçkÉ□¹'□K□□"□□□©)□åråm*0□£oÅü□:ÖË□t5¡m#«}úîáeäß□ □½§ □□QIN□□□□Ê|□U□□[ÃuùHÅj®□□□¤O□¦¤Ý□}¿, 5"□□□¸Ì□^±Uyîøm□□□a□Àù¯□±ÂëÑ□êE«Ûh£Ç□□^T□ÇlSÔ□□□ç»Ó□b□□□áªaÛ¼□Ý<d_/UóÔÃuì@p©?qQØ6pÁj□□¾^òÑ□□á¸®ó)□ðf¿□láD¬□èm□□□□□□£□ü0□ù0□□□U□□□□□□□□Å¾□LC<a□:□°L¼□òOà²0□É□□U□#□□Á0□¾□□□□Å¾□LC<a□:□°L¼□òOà²¡□□¤□□0□□1□0 □□U□□□□US1□0□□□U□□□ California1□0□□□U□□□□Mountain View1□0□□□U□ □□Android1□0□□□U□□□□Android1□0□□□U□□□□Android1"0 □ *□H□÷□□ □□□android@android.com□ □Õ□¸l}ÓNõ0□□□U□□□□0□□□ÿ0□□ *□H□÷□□□□□□□□□□□□□Ó□ñ□ûx□?L□}Ò##=@□zÍÎ□□□[×ÆéÖí k□□ □□AI¢D□□□ÒkJ àõ$ÊÒ»\nL¡□j□□n¡ì]ÉZ^:□□6ô□HÕ□□¿.□a□□g:;åm¯□w±Â)ãÂUãèL□]#□ïº Ëñ; +NZ"É2cHJ#Òü)ú□□9u□3¯Ø ª□□B□ÂÐ□>□□□□fCéÁ□/ Á□33[À□ÿ□k"ÞÑ□DB)¥9©Nï□«ÐeÎÒK>QåÝ{fx{i□þ□û¤□Ä#ûOøÌlL□ðõ□□□ÿe)9>□FêÅ»!òwÁQª_*¦'Ñè□§ ¶□5iÞ;□□¿ÿ|©Ú>□Cö□"

const-string v1 "Validation of queries failed. Please report to support@firebase.com"

const-string v1 "). Please report to support@firebase.com"

[Medium] Residual intranet IP — 2 risks

Risk Details: The intranet network IP which remain in the APP's configuration file during development or testing phase has the risk of being exploited by attackers to attack intranet hosts.

Repair Suggestions: Remove the intranet IP from APP.

Risk Code:

com.ipay.IPayIHSelectionActivity.<init> : 112

const-string v0 "http://10.0.2.2:8080/logserver/log"

com.ipay.IPayIHSelectionActivity.logToServer : 269

const-string v1 "http://10.0.2.2:8080/logserver/log"

[Medium] Residue URL — 236 risks

Risk Details: The URL address which remain in the APP's configuration file during development or testing phase has the risk of being attacked by attackers.

Repair Suggestions: Remove the URL address from APP.

URL List:

SG_ZENDESK_URL = "https://kaodim-sg.zendesk.com"

const-string v1 "https://branch.app.link/link-settings-page"

PLUS_PAGES_MANAGE = "https://www.googleapis.com/auth/plus.pages.manage"

const-string v5 "https://play.google.com/store/apps/details?id="

const-string v1 "https://stats.%s/stats"

const-string v0 "https://kaodim-sg.zendesk.com"

const-string v0 "https://twitter.com/beres_id"

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

const-string v7 "https://decide.mixpanel.com/decide"

EVENT_LOG_URL = "https://api.amplitude.com/"

CIRCLES_WRITE = "https://www.googleapis.com/auth/plus.circles.write"

const-string v3 "https://cdn.branch.io/sdk/uriskiplist_v#.json"

const-string v3 "runTransaction() usage detected while persistence is enabled. Please be aware that transactions *will not* be persisted across app restarts. See https://www.firebase.com/docs/android/guide/offline-capabilities.html#section-handling-transactions-offline for more details."

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."

const-string v7 "https://support.kaodim.com/hc/en-us/articles/360004916934-Why-communicate-through-Kaodim-directly-"

const-string v1 "https://@.staging.kaodim.com"

const-string v0 "http://dashboard.beres.id/reset-password"

const-string v0 "https://@.staging.kaodim.com"

const-string v0 "https://gawin.zendesk.com"

const-string p1 "https://play.google.com/store/apps/details?id=%1$s&rdid=%1$s&rdot=%2$d"

const-string v0 "https://kaodim-sg.zendesk.com"

const-string v3 "https://ssl.google-analytics.com"

PH_ZENDESK_URL = "https://gawin.zendesk.com"

const-string v0 "https://twitter.com/kaodim"

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

ID_ZENDESK_URL = "https://beres.zendesk.com"

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

const-string v2 "https://www.kaodim.com/privacy"

LEGACY_USERINFO_PROFILE = "https://www.googleapis.com/auth/userinfo.profile"

const-string v3 "https://tap-nexus.appspot.com"

SG_ZENDESK_URL = "https://kaodim-sg.zendesk.com"

SETTINGS_URL_FORMAT = "https://settings.crashlytics.com/spi/v2/platforms/android/apps/%s/settings"

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

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

const-string v0 "https://auth.firebase.com/"

const-string v1 "https://@.staging.kaodim.com"

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

FITNESS_BODY_TEMPERATURE_READ_WRITE = "https://www.googleapis.com/auth/fitness.body_temperature.write"

const-string v1 "https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps"

API_AUDIT_GRANTS = "https://www.googleapis.com/auth/grants.audit"

const-string v0 "http://dashboard.gawin.ph/reset-password"

const-string v0 "http://10.0.2.2:8080/logserver/log"

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 v2 "https://www.kaodim.com/terms"

const-string v1 "Firebase authentication is supported on production Firebases only (*.firebaseio.com). To secure your Firebase, create a production Firebase at https://www.firebase.com."

const-string v5 "https://tap-nexus.appspot.com"

FITNESS_BLOOD_GLUCOSE_READ = "https://www.googleapis.com/auth/fitness.blood_glucose.read"

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

const-string v0 "http://hostname/?"

const-string v0 "http://hostname/?"

const-string v0 "https://twitter.com/beres_id"

const-string v3 "FacebookActivity is not declared in the AndroidManifest.xml, please add com.facebook.F

acebookActivity to your AndroidManifest.xml file. See https://developers.facebook.com/docs/android/getting-started for more info."

PLUS_MEDIA_UPLOAD = "https://www.googleapis.com/auth/plus.media.upload"

const-string v3 "https://monitorsdk.%s/remote-debug?app_id="

const-string v2 "https://docs.branch.io/pages/apps/android/#configure-app"

const-string v2 "http://localhost/"

const-string v2 "http://localhost/"

const-string v1 "https://@.staging.kaodim.com"

ONLINE_WALLET = "https://www.googleapis.com/auth/payments.make_payments"

AF_BASE_URL_FORMAT = "https://%s/%s"

MY_ZENDESK_URL = "https://kaodim.zendesk.com"

DEF_BASE_URL = "https://bnc.lt/a/"

UPDATE_URL_PATH = "https://cdn.branch.io/sdk/uriskiplist_v#.json"

FITNESS_OXYGEN_SATURATION_READ_WRITE = "https://www.googleapis.com/auth/fitness.oxygen_saturation.write"

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

const-string v0 "https://api.%s/install_data/v3/"

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

const-string v0 "http://dashboard.gawin.ph/reset-password"

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

const-string v1 "https://app.%s"

const-string v0 "http://dashboard.kaodim.com/reset-password"

const-string v1 "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."

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

const-string v2 "https://www.example.com"

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

PLUS_APPLICATIONS_MANAGE = "https://www.googleapis.com/auth/plus.applications.manage"

const-string v1 "https://@.cs.staging.kaodim.com"

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

PRODUCTION_URL = "https://tap-nexus.appspot.com"

GOOGLE_PLAY_STORE_GAMES_URI_STRING = "http://play.google.com/store/apps/category/GAME"

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://@.staging.kaodim.com"

MY_PHONE_NUMBERS = "https://www.googleapis.com/auth/myphonenumbers"

const-string v1 "https://validate.%s/api/v"

FITNESS_REPRODUCTIVE_HEALTH_READ = "https://www.googleapis.com/auth/fitness.reproductive_health.read"

const-string v2 "https://www.kaodim.com/terms"

CIRCLES_READ = "https://www.googleapis.com/auth/plus.circles.read"

const-string v7 "https://help.kaodim.com/hc/en-us/articles/360004164872-Why-communicate-and-book-through-Kaodim-directly-"

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

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

const-string v2 "https://api.mixpanel.com/track?ip=1"

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

const-string v0 "https://twitter.com/kaodim"

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

DRIVE_FULL = "https://www.googleapis.com/auth/drive"

LEGACY_USERINFO_EMAIL = "https://www.googleapis.com/auth/userinfo.email"

const-string v2 "https://docs.branch.io/pages/deep-linking/android-app-links/#add-intent-filter-to-manifest"

YOUTUBE_DATA_API = "https://www.googleapis.com/auth/youtube"

CIRCLE_MEMBERS = "https://www.googleapis.com/auth/plus.circles.members"

const-string v9 "https://dashboard.zopim.com/bin/"

const-string v0 "https://kaodim.zendesk.com"

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

const-string v1 "https://docs.branch.io/pages/apps/android/#configure-app"

const-string v1 "http://play.google.com/store/apps/category/GAME"

const-string v4 "https://settings.crashlytics.com/spi/v2/platforms/android/apps/%s/settings"

const-string v3 "http://www.google-analytics.com"

PLUS_PROFILE_WRITE = "https://www.googleapis.com/auth/plus.profiles.write"

const-string v1 "https://register.%s/api/v"

BASE_URL = "https://@.staging.kaodim.com"

const-string v1 "https://events.%s/api/v"

const-string p0 "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."

const-string v7 "https://help.kaodim.sg/hc/en-us/articles/360004965613-Why-communicate-and-book-through-Kaodim-directly-"

const-string v0 "https://twitter.com/GawinPH"

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

const-string v7 "https://help.beres.id/hc/id/articles/360004920874-Kenapa-lebih-baik-berkomunikasi-dan-membooking-melalui-Beres-"

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

FITNESS_BODY_TEMPERATURE_READ = "https://www.googleapis.com/auth/fitness.body_temperature.read"

const-string v0 "http://dashboard.kaodim.com/reset-password"

const-string v0 "http://dashboard.kaodim.sg/reset-password"

const-string v7 "https://support.gawin.ph/hc/en-us/articles/360004243351-Why-communicate-through-Gawin-directly-"

GAMES_LITE = "https://www.googleapis.com/auth/games_lite"

const-string v7 "https://support.beres.id/hc/id/articles/360004967873-Kenapa-lebih-baik-berkomunikasi-melalui-Beres-"

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

const-string v0 "Missing google_app_id. Firebase Analytics disabled. See https://goo.gl/NAOOOI"

const-string v3 "https://sdk-services.%s/validate-android-signature"

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

ONLINE_WALLET_SANDBOX = "https://www.googleapis.com/auth/paymentssandbox.make_payments"

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

const-string v2 "Invalid google_app_id. Firebase Analytics disabled. See https://goo.gl/NAOOOI. provided id"

const-string v1 "https://attr.%s/api/v"

const-string v7 "https://vm-mpayment.cloudapp.net:8243/PaymentGateway/RHX"

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

const-string v1 "https://onelink.%s/shortlink-sdk/v1"

const-string v0 "https://beres.zendesk.com"

MISSING_BUILD_ID_MSG = "This app relies on Crashlytics. Please sign up for access at https://fabric.io/sign_up, install an Android build tool and ask a team member to invite you to this app's organization."

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

const-string v2 "https://www.mobile88.com/ePayment/enquiry.asp"

const-string v0 "https://api.branch.io/"

CONNECTIONS_READ = "https://www.googleapis.com/auth/connections.read"

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

const-string v1 "https://t.%s/api/v"

const-string v7 "http://maps.google.com/maps?q=loc:"

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:value="@integer/google_play_services_version" />' to your application manifest file. See http://goo.gl/naFqQk

for details."

ANALYTICS_URL_DEFAULT = "https://e.crashlytics.com/spi/v2/events"

PLUS_PEOPLE_READWRITE = "https://www.googleapis.com/auth/plus.peopleapi.readwrite"

PLUS_STREAM_READ = "https://www.googleapis.com/auth/plus.stream.read"

DISPLAY_ADS = "https://www.googleapis.com/auth/display_ads"

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

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

const-string v2 "https://e.crashlytics.com/spi/v2/events"

const-string v0 "https://beres.zendesk.com"

const-string v8 "https://app-measurement.com/a"

const-string v2 "This app relies on Crashlytics. Please sign up for access at https://fabric.io/sign_up, install an Android build tool and ask a team member to invite you to this app's organization."

const-string v3 "http://api.mixpanel.com/track?ip=1"

const-string v0 "https://@.staging.kaodim.com"

GAMES_1P = "https://www.googleapis.com/auth/games.firstparty"

GOOGLE_PLAY_STORE_URI_STRING = "http://play.google.com/store/apps/"

FITNESS_BLOOD_GLUCOSE_READ_WRITE = "https://www.googleapis.com/auth/fitness.blood_glucose.write"

const-string v1 "https://@.staging.kaodim.com"

const-string v3 "https://bnc.lt/a/"

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

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

PRODUCTION_URL = "https://tap-nexus.appspot.com"

const-string v2 "https://www.kaodim.com/terms"

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

PH_ZENDESK_URL = "https://gawin.zendesk.com"

const-string v1 "AnalyticsService is not registered or is disabled. Analytics service at risk of not starting. See http://goo.gl/8Rd3yj for instructions."

const-string v1 "https://@.staging.kaodim.com"

const-string v5 "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."

const-string v7 "https://support.kaodim.sg/hc/en-us/articles/360004166952-Why-communicate-through-Kaodim-directly-"

DRIVE_APPS = "https://www.googleapis.com/auth/drive.apps"

MY_ZENDESK_URL = "https://kaodim.zendesk.com"

const-string v3 "https://www.example.com"

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

const-string v6 "http://api.mixpanel.com/engage"

FITNESS_OXYGEN_SATURATION_READ = "https://www.googleapis.com/auth/fitness.oxygen_saturation.read"

const-string v1 "https://docs.branch.io/pages/dashboard/integrate/#android"

const-string v0 "http://dashboard.beres.id/reset-password"

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

const-string v0 "https://twitter.com/GawinPH"

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

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

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."

const-string v1 "https://docs.branch.io/pages/apps/android/#load-branch"

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

const-string p1 "https://%s/%s"

PLUS_SETTINGS = "https://www.googleapis.com/auth/plus.settings"

PLUS_STREAM_WRITE = "https://www.googleapis.com/auth/plus.stream.write"

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

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

CONTENT_PROVIDER_NOT_FOUND_REASON = "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."

const-string v0 "https://kaodim.zendesk.com"

FITNESS_BLOOD_PRESSURE_READ = "https://www.googleapis.com/auth/fitness.blood_pressure.read"

FIREBASE_AUTH_DEFAULT_API_HOST = "https://auth.firebase.com/"

const-string v9 "https://my."

const-string v1 "https://docs.branch.io/pages/apps/android/#configure-app"

const-string v0 "http://dashboard.kaodim.sg/reset-password"

const-string v3 "Some required attributes were missing. Forcing a Zendesk theme. Please read https://developer.zendesk.com/embeddables/docs/android/customize_the_look#use-or-extend-an-sdk-theme"

const-string v2 "https://www.kaodim.com/privacy"

BASE_URL_CRAMER = "https://@.cs.staging.kaodim.com"

TEST_URL = "https://www.example.com"

const-string v1 "This app relies on Crashlytics. Please sign up for access at https://fabric.io/sign_up, install an Android build tool and ask a team member to invite you to this app's organization."

const-string v2 "https://docs.branch.io/pages/dashboard/integrate/#android"

PLUSONE_SERVICE = "https://www.googleapis.com/auth/pos"

const-string v0 "https://androidquery.appspot.com"

const-string v1 "https://bnc.lt/a/"

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

const-string v1 "https://onelink.%s/shortlink-sdk/v1"

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

const-string v0 "https://gawin.zendesk.com"

const-string v0 "https://@.staging.kaodim.com"

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

FITNESS_BLOOD_PRESSURE_READ_WRITE = "https://www.googleapis.com/auth/fitness.blood_pressure.write"

FITNESS_REPRODUCTIVE_HEALTH_READ_WRITE = "https://www.googleapis.com/auth/fitness.reproductive_health.write"

PLUS_PROFILE_READ = "https://www.googleapis.com/auth/plus.profiles.read"

const-string v2 "https://www.kaodim.com/terms"

const-string v2 "https://www.kaodim.com/privacy"

const-string v6 "====================== FileProvider failed to retrieve file uri. There might be an issue with the FileProvider Please make sure that manifest-merger is working, and that you have defined the applicationId (package name) in the build.gradle Manifest merger: http://tools.android.com/tech-docs/new-build-system/user-guide/manifest-merger If your are not able to use gradle or the manifest merger, please add the following to your AndroidManifest.xml: <provider android:name="com.zendesk.belvedere.BelvedereFileProvider" android:authorities="${applicationId}${belvedereFileProviderAuthoritySuffix}" android:exported="false" android:grantUriPermissions="true"> <meta-data android:name="android.support.FILE_PROVIDER_PATHS" android:resource="@xml/belvedere_attachment_storage" /> </provider> ==========="

const-string v1 "https://@.staging.kaodim.com"

const-string v1 "http://10.0.2.2:8080/logserver/log"

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

const-string v8 "http://decide.mixpanel.com/decide"

BASE_URL = "https://dashboard.zopim.com/bin/"

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

ID_ZENDESK_URL = "https://beres.zendesk.com"

const-string v1 "https://@.cs.staging.kaodim.com"

const-string v0 "https://vm-mpayment.cloudapp.net:8243/PaymentGateway/RHX"

BASE_URL_APP_APPSFLYER_COM = "https://app.%s"

const-string v5 "https://api.mixpanel.com/engage"

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

const-string v1 "http://play.google.com/store/apps/details?id=com.facebook.orca"

const-string v9 "https://sg."

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

const-string p3 "https://%s/%s"

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

const-string v2 "https://www.kaodim.com/privacy"

[Medium] Secret key hard coded 32 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.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.kaodim.kaodimuserapp.general.SharedData.ID_ZENDESK_APP_ID
ID_ZENDESK_APP_ID = "3d5ab24af967befabe5fcc6efd88ca268077f85280ea1eca"

com.kaodim.kaodimuserapp.SharedData.ID_ZENDESK_APP_ID
ID_ZENDESK_APP_ID = "3d5ab24af967befabe5fcc6efd88ca268077f85280ea1eca"

io.fabric.sdk.android.BuildConfig.DEVELOPER_TOKEN
DEVELOPER_TOKEN = "470fa2b4ae81cd56ecbcda9735803434cec591fa"

com.kaodim.kaodimuserapp.general.SharedData.SG_ZENDESK_APP_ID
SG_ZENDESK_APP_ID = "dad75a09508a0aa74eec059b253f304bf5c61341849dbbce"

com.kaodim.kaodimuserapp.SharedData.SG_ZENDESK_APP_ID
SG_ZENDESK_APP_ID = "dad75a09508a0aa74eec059b253f304bf5c61341849dbbce"

com.kaodim.kaodimuserapp.general.SharedData.PH_ZENDESK_APP_ID
PH_ZENDESK_APP_ID = "0a4b9298d563734cf9fcf0743b2793f1847fbbc2809091e7"

com.kaodim.kaodimuserapp.SharedData.PH_ZENDESK_APP_ID
PH_ZENDESK_APP_ID = "0a4b9298d563734cf9fcf0743b2793f1847fbbc2809091e7"

io.fabric.sdk.android.services.common.AbstractSpiCall.CLS_ANDROID_SDK_DEVELOPER_TOKEN
CLS_ANDROID_SDK_DEVELOPER_TOKEN = "470fa2b4ae81cd56ecbcda9735803434cec591fa"

com.facebook.internal.FacebookSignatureValidator.MSR_HASH
MSR_HASH = "9b8f518b086098de3d77736f9458a3d2f6f95a37"

com.kaodim.kaodimuserapp.SharedData.MY_ZENDESK_APP_ID
MY_ZENDESK_APP_ID = "79ea1211d28e479075349d68dabe8da086d09cea5979e078"

com.kaodim.kaodimuserapp.general.SharedData.MY_ZENDESK_APP_ID
MY_ZENDESK_APP_ID = "79ea1211d28e479075349d68dabe8da086d09cea5979e078"

com.kaodim.kaodimuserapp.SharedData.setCountryPH : 113
const-string v0 "0a4b9298d563734cf9fcf0743b2793f1847fbbc2809091e7"

com.kaodim.kaodimuserapp.general.SharedData.setCountryPH : 147
const-string v0 "0a4b9298d563734cf9fcf0743b2793f1847fbbc2809091e7"

com.kaodim.kaodimuserapp.general.SharedData.setCountryIndonesia : 166
const-string v0 "3d5ab24af967befabe5fcc6efd88ca268077f85280ea1eca"

com.kaodim.kaodimuserapp.SharedData.setCountryIndonesia : 127
const-string v0 "3d5ab24af967befabe5fcc6efd88ca268077f85280ea1eca"

com.kaodim.kaodimuserapp.SharedData.setCountryMY : 83
const-string v0 "79ea1211d28e479075349d68dabe8da086d09cea5979e078"

com.kaodim.kaodimuserapp.general.SharedData.setCountryMY : 107
const-string v0 "79ea1211d28e479075349d68dabe8da086d09cea5979e078"

com.kaodim.kaodimuserapp.SharedData.setCountrySG : 98
const-string v0 "dad75a09508a0aa74eec059b253f304bf5c61341849dbbce"

com.kaodim.kaodimuserapp.general.SharedData.setCountrySG : 127
const-string v0 "dad75a09508a0aa74eec059b253f304bf5c61341849dbbce"

com.facebook.internal.FacebookSignatureValidator.buildAppSignatureHashes : 53
const-string v1 "5e8f16062ea3cd2c4a0d547876baa6f38cabf625"

com.facebook.internal.FacebookSignatureValidator.buildAppSignatureHashes : 50
const-string v1 "8a3c4b262d721acd49a4bf97d5213199c86fa2b9"

com.facebook.internal.FacebookSignatureValidator.buildAppSignatureHashes : 55
const-string v1 "9b8f518b086098de3d77736f9458a3d2f6f95a37"

com.facebook.internal.FacebookSignatureValidator.buildAppSignatureHashes : 52
const-string v1 "a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc"

com.facebook.internal.FacebookSignatureValidator.buildAppSignatureHashes : 51
const-string v1 "cc2751449a350f668590264ed76692694a80308a"

com.facebook.internal.FacebookSignatureValidator.buildAppSignatureHashes : 54
const-string v1 "df6b721c8b4d3b6eb44c861d4415007e5a35fc95"

com.crashlytics.android.beta.CheckForUpdatesRequest.applyHeadersTo : 76
const-string v2 "470fa2b4ae81cd56ecbcda9735803434cec591fa"

io.fabric.sdk.android.services.common.AbstractSpiCall.getHttpRequest : 141
const-string v3 "470fa2b4ae81cd56ecbcda9735803434cec591fa"

— [Low] **PendingIntent hijacking** 2 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:

androidx.browser.browseractions.BrowserActionsIntent$Builder.build : 261

invoke-static {v0 v2 v1 v2} Landroid/app/PendingIntent; getActivity (Landroid/content/Context; I Landroid/content/Intent; I)Landroid/app/PendingIntent;

com.mixpanel.android.mpmetrics.MixpanelAPI$PeopleImpl.registerForPushIdAPI19AndOlder : 1753

invoke-static {v2 v4 v3 v4} Landroid/app/PendingIntent; getBroadcast (Landroid/content/Context; I Landroid/content/Intent; I)Landroid/app/PendingIntent;

— [Low] **Uncompressed & unencrypted JS Code** 4 risks

Risk Details: There is the risk of leaking important information such as program logic when there is unobfuscated JavaScript code in the APP.

Repair Suggestions: JavaScript code to be obfuscated.

File Path:

/assets/html/js/preview.js

/assets/html/js/highlight.pack.js

/assets/html/js/jquery-2.1.4.min.js

/assets/html/js/marked.js

Encryption Security

— [Medium] **Insecure hash algorithm** 12 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.zzbv.zzd

invoke-static {v1} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;

v1 = "MD5"

com.mixpanel.android.java_websocket.drafts.Draft_10.generateFinalKey : 183

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

v2 = "SHA1"

com.squareup.okhttp.internal.Util.md5Hex : 177

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

v0 = "MD5"

com.google.firebase.iid.zzah.zza

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

v0 = "SHA1"

com.appsflyer.q.´ : 63
invoke-static {v0} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;
v0 = "MD5"

com.google.android.gms.iid.InstanceID.zzd
invoke-static {v0} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;
v0 = "SHA1"

com.androidquery.util.AQUtility.getMD5 : 375
invoke-static {v1} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;
v1 = "MD5"

io.fabric.sdk.android.services.network.PinningTrustManager.isValidPin : 116
invoke-static {v0} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;
v0 = "SHA1"

com.facebook.appevents.AppEvent.md5Checksum : 266
invoke-static {v0} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;
v0 = "MD5"

com.mixpanel.android.util.ImageStore.<init> : 46
invoke-static {v0} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;
v0 = "SHA1"

io.branch.indexing.ContentDiscoverer$HashHelper.<init> : 380
invoke-static {p1} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;
p1 = "MD5"

com.mixpanel.android.java_websocket.drafts.Draft_76.createChallenge : 60
invoke-static {v3} Ljava/security/MessageDigest; getInstance (Ljava/lang/String;)Ljava/security/MessageDigest;
v3 = "MD5"

Code Security

— **[Medium] WebView same origin policy bypass** 1 risks

Risk Details: There is a risk of information leakage when the APP's WebView loads local resource files and enables JavaScript.

Repair Suggestions: Avoid using both the File protocol and JavaScript.

Risk Code: **com.mukesh.MarkdownView.initialize : 85**
invoke-virtual {v0 v1} Landroid/webkit/WebSettings; setAllowUniversalAccessFromFileURLs (Z)V
v1 = 0x1

— **[Low] Sensitive function calls** 9 risks

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:

com.amplitude.api.Amplitude.getDeviceId : 245
invoke-virtual {v0} Lcom/amplitude/api/AmplitudeClient; getDeviceId ()Ljava/lang/String;

com.kaodim.kaodimuserapp.activities.IPay88CustomActivity.setupPaymentViews : 141
invoke-virtual {v6} Landroid/telephony/TelephonyManager; getDeviceId ()Ljava/lang/String;

com.ipay.IPayIHActivity.setupPaymentViews : 128
invoke-virtual {v6} Landroid/telephony/TelephonyManager; getDeviceId ()Ljava/lang/String;

com.kaodim.kaodimuserapp.firebase.RegistrationIntentService.sendRegistrationToServer : 57
invoke-direct {p0 v0} Lcom/kaodim/kaodimuserapp/firebase/RegistrationIntentService; getDeviceId (Landroid/content/Context;)Ljava/lang/String;

com.mixpanel.android.mpmetrics.SystemInformation.getPhoneRadioType : 91
invoke-virtual {v1} Landroid/telephony/TelephonyManager; getPhoneType ()I

com.appsflyer.j.´ : 96
invoke-virtual {p0} Landroid/telephony/TelephonyManager; getPhoneType ()I

com.amplitude.api.DeviceInfo$CachedInfo.getCountryFromNetwork : 168
invoke-virtual {v0} Landroid/telephony/TelephonyManager; getPhoneType ()I

com.ipay.IPayIHActivity.setupPaymentViews : 134
invoke-virtual {v6} Landroid/telephony/TelephonyManager; getSubscriberId ()Ljava/lang/String;

com.kaodim.kaodimuserapp.activities.IPay88CustomActivity.setupPaymentViews : 142
invoke-virtual {v6} Landroid/telephony/TelephonyManager; getSubscriberId ()Ljava/lang/String;

Component Security

— **[Medium] Activity component exposure** 2 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:

Componet Type: Activity
Component Name: com.facebook.CustomTabActivity
Reason for Export: android:exported=true

Componet Type: Activity
Component Name: com.zopim.android.sdk.prechat.ZopimChatActivity
Reason for Export: intent-filter

— **[Medium] Broadcast component exposure** 9 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:

Componet Type: Broadcast Receiver
Component Name: com.appsflyer.MultipleInstallBroadcastReceiver
Reason for Export: android:exported=true

Componet Type: Broadcast Receiver
Component Name: com.appsflyer.SingleInstallBroadcastReceiver
Reason for Export: android:exported=true

Componet Type: Broadcast Receiver
Component Name: com.google.android.gms.analytics.CampaignTrackingReceiver
Reason for Export: android:exported=true

Componet Type: Broadcast Receiver
Component Name: com.kaodim.kaodimuserapp.firebase.QuotesReceiver
Reason for Export: android:exported=true

Componet Type: Broadcast Receiver
Component Name: com.kaodim.messenger.tools.NetworkStateReceiver
Reason for Export: intent-filter

Componet Type: Broadcast Receiver
Component Name: com.zendesk.sdk.power.BatteryStateBroadcastReceiver
Reason for Export: intent-filter

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

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

Componet Type: Broadcast Receiver
Component Name: com.zopim.android.sdk.api.ZopimChatApi$ChatTimeoutReceiver
Reason for Export: intent-filter

[Medium] Service component exposure — 4 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:

Componet Type: Service
Component Name: com.kaodim.kaodimuserapp.firebase.MyFirebaseMessagingService
Reason for Export: intent-filter

Componet Type: Service
Component Name: com.kaodim.kaodimuserapp.firebase.MyFirebaseInstanceIdService
Reason for Export: intent-filter

Componet Type: Service
Component Name: com.google.firebase.messaging.FirebaseMessagingService
Reason for Export: android:exported=true

Componet Type: Service
Component Name: com.google.firebase.iid.FirebaseInstanceIdService
Reason for Export: android:exported=true

Configuration Security

[High] Backup mode not turned off 1 risks

Risk Details: When APP turns on data backup and restore capabilities, it can back up data through the ADB, with the risk of information leakage.

Repair Suggestions: Set the configuration to 'android:allowbackup=false' in the AndroidManifest.xml file.

[High] Debug mode is not turned off 1 risks

Risk Details: When APP turns on dynamic debugging, it is possible to debug and tamper with execution logic, with the risk of execution logic leakage.

Repair Suggestions: Set the configuration to 'android:debuggable=false' in the AndroidManifest.xml file.

[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.

[Low] Unnecessary runtime permissions 3 risks

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

Repair Suggestions: Remove the unnecessary permissions.

Request Permission: Accessing Phone Status and Identity Automatically Making Phone Calls Displaying System Alarm

Communication Security

[High] Server-side certificate weak validation 3 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: com.ipay.IPayIHSelectionActivity$MySSLSocketFactory$1.checkServerTrusted

com.ipay.log.LoggingTask$MySSLSocketFactory$1.checkServerTrusted

com.google.android.gms.common.net.zza.checkServerTrusted

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

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