



MoGua

同城聊欢 5.10.4.APK 分析报告



APP名称:

同城聊欢

包名:	com.sh.shuihulu.kiwi
域名线索:	28条
URL线索:	6条
邮箱线索:	1条
分析日期:	2025年4月27日
分析平台:	摸瓜APK反编译平台

文件名: 同城聊欢.apk
文件大小: 119.85MB
MD5值: 67eab5fb2074c4f969eb1c13cbc51b55
SHA1值: 28135c66723bfa82edacab21635151e54d0035c2
SHA256值: 1a6f82f4e239310171aac828ee51543ddfbe98fdf7fc6695b377e3bcbcd200d

i APP 信息

App名称: 同城聊欢
包名: com.sh.shuihulu.kiwi
主活动Activity: com.yicheng.assemble.activity.LauncherActivity
安卓版本名称: 5.10.4
安卓版本: 231103103

🔍 域名线索

域名	服务器信息
grs.dbankcloud.com	IP: 113.201.107.90 所属国家: China 地区: Shaanxi 城市: Baoji 纬度: 34.353611 经度: 107.375275
metrics-dra.dt.hicloud.com	IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
v.map.baidu.com	IP: 111.206.209.185 所属国家: China 地区: Beijing

	城市: Beijing 纬度: 39.907501 经度: 116.397102
argus.agoralab.co	IP: 39.107.118.231 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
newvector.map.baidu.com	IP: 111.206.209.177 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
vectormap0.bdimg.com	IP: 60.6.196.35 所属国家: China 地区: Hebei 城市: Xingtai 纬度: 37.062309 经度: 114.494209
itsmap3.baidu.com	IP: 153.3.237.86 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
sv.map.baidu.com	IP: 111.206.209.186 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

data-dra.push.dbankcloud.com	IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
metrics5.dt.dbankcloud.ru	IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
client.map.baidu.com	IP: 111.206.209.120 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
grs.dbankcloud.asia	IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
grs.dbankcloud.cn	IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361

	经度: 113.264572
metrics2.data.hicloud.com	IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel 纬度: 54.321358 经度: 10.134532
data-drru.push.dbankcloud.com	IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
mapoffdownload.bdstatic.com	IP: 119.167.139.36 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
map.baidu.com	IP: 111.206.208.32 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
metrics1-drcn.dt.dbankcloud.cn	IP: 111.202.17.12 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
	IP: 119.249.50.35 所属国家: China

offmap2.baidu.com	地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
data-drcn.push.dbankcloud.com	IP: 49.4.40.58 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
grs.platform.dbankcloud.ru	没有服务器地理信息.
indoorsearch.map.baidu.com	IP: 111.206.209.201 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
data-dre.push.dbankcloud.com	IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel 纬度: 54.321358 经度: 10.134532
metrics5.data.hicloud.com	IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
newclient.map.baidu.com	IP: 111.206.209.170 所属国家: China 地区: Beijing 城市: Beijing

	纬度: 39.907501 经度: 116.397102
api.map.baidu.com	IP: 111.206.208.72 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
grs.dbankcloud.eu	没有服务器地理信息.

 URL线索

URL信息	Url所在文件
https://github.com/vinc3m1	Mogua Engine V1
https://github.com/vinc3m1/RoundedImageView	Mogua Engine V1
https://github.com/vinc3m1/RoundedImageView.git	Mogua Engine V1
https://data-drcn.push.dbankcloud.com	Mogua Engine V2
https://data-dra.push.dbankcloud.com	Mogua Engine V2
https://data-dre.push.dbankcloud.com	Mogua Engine V2
https://data-drru.push.dbankcloud.com	Mogua Engine V2
https://metrics1-drcn.dt.dbankcloud.cn:443	Mogua Engine V2
https://metrics-dra.dt.hicloud.com:6447	Mogua Engine V2

https://metrics2.data.hicloud.com:6447	Mogua Engine V2
https://metrics5.data.hicloud.com:6447	Mogua Engine V2
https://metrics5.dt.dbankcloud.ru:6447	Mogua Engine V2
https://grs.dbankcloud.com	Mogua Engine V2
https://grs.dbankcloud.cn	Mogua Engine V2
https://grs.dbankcloud.asia	Mogua Engine V2
https://grs.platform.dbankcloud.ru	Mogua Engine V2
https://grs.dbankcloud.eu	Mogua Engine V2
https://indoorsearch.map.baidu.com/is/	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
http://map.baidu.com/zt/y2015/taohuayuan/	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://sv.map.baidu.com/	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://v.map.baidu.com/high/	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://client.map.baidu.com/imap/sdk/tj?qt=vmap	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://client.map.baidu.com/heatmap/client?	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://newclient.map.baidu.com/client/	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
http://map.baidu.com/zt/y2016/fudai/mobile/	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://newclient.map.baidu.com/pic/newvector/	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://newvector.map.baidu.com/	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so

https://vectormap0.bdimg.com/vecdata/	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://api.map.baidu.com/api_olog/v1/up	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://client.map.baidu.com/	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://sv.map.baidu.com	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://newclient.map.baidu.com/its/	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://newvector.map.baidu.com/grid_vc/	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://v.map.baidu.com/low/	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://v.map.baidu.com/indoorinside/	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://api.map.baidu.com/api_olog/v1/control?	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://newvector.map.baidu.com/travel_vc/	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
http://client.map.baidu.com/?qt=rg&mmproxyver=1&url=	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://newvector.map.baidu.com/starpic/	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://offmap2.baidu.com/offline-search/?	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://newclient.map.baidu.com/pic/newvector/topic_map/	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://mapoffdownload.bdstatic.com/	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://client.map.baidu.com/offline-search/?	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
https://api.map.baidu.com/sdkproxy/lbs_androidsdk/statistics/v1/	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so

https://itsmap3.baidu.com/	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so
http://argus.agoralab.co/vosdk/public/report?speaker=%u&listener=%u&venderID=%s&channelName=%s	lib/arm64-v8a/libagora-rtc-sdk.so
http://argus.agoralab.co/vosdk/public/report?listener=%u&venderID=%s&channelName=%s	lib/arm64-v8a/libagora-rtc-sdk.so
http://s	lib/arm64-v8a/libagora-rtc-sdk.so

 邮箱线索

邮箱地址	所在文件
appro@openssl.org	lib/arm64-v8a/libBaiduMapSDK_map_v7_5_7.so

 手机线索

 签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=gnwgh, ST=jhpyxmh, L=mklqxq, O=xyoaujog, OU=dgtqcwzc, CN=guujtq
签名算法: rsassa_pkcs1v15
有效期自: 2020-07-24 01:57:10+00:00
有效期至: 2075-04-27 01:57:10+00:00
发行人: C=gnwgh, ST=jhpyxmh, L=mklqxq, O=xyoaujog, OU=dgtqcwzc, CN=guujtq
序列号: 0x5f1a3ff6
哈希算法: sha1
md5值: 21a0331dcdb529683104c63b30a6d45d

sha1值: 9f3b25ec2523dd71af25fa2d580e40b6f0a9a2ce
sha256值: ab8aa429aba2f7faf901de9db7fa748d8543c1e5e4ef3b4a29594c8727cae410
sha512值: 11fc4f288a20c8b5778343f0b497c1d3ad71a22dc59f9eb0068614345d26bfb9845a7f9b8101f5b70d924f0289c84fd06d5f74e7f27bbd7531185b71ea3e883b
公钥算法: rsa
密钥长度: 1024
指纹: ff7420e960af8d3750fa59d2e1fd83b94f21a278b3c05d684d01d57685bdc73c

硬编码敏感信息

可能的敏感信息
"had_problem_to_auth" : "实名认证不了怎么办? "
"idcard_auth_tmyh" : "您已实名认证通过"
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"manager_auth" : "管理员审核"
"need_complete_anchor_authentication" : "使用该功能，需完成实名认证。"
"phone_authentication" : "手机认证"
"please_select_identity_authentication_avatar" : "请上传身份证人像面照片"
"please_select_user" : "请选择用户"
"private_chat" : "私聊"
"real_name_authentication" : "实名认证"
"start_notification_authority" : "咱们的App没有通知栏权限，请您先开启"

"ta_authentication" : "Ta的认证"
"teenagers_input_closepwd" : "请输入密码关闭青少年模式"
"teenagers_input_nowpwd" : "请输入当前密码"
"teenagers_input_pwd" : "请输入4位数字密码"
"teenagers_pwd_edit" : "设置密码"
"teenagers_pwd_forget_tip" : "如果忘记密码，可以卸载重装退出青少年模式"
"teenagers_pwd_input" : "输入密码"
"teenagers_pwd_please_input" : "请输入新密码"
"teenagers_pwd_set" : "设置密码"
"start_notification_authority" : "咱们的App没有通知栏权限，请您先开启"

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

--	--	--

名称	分类	URL链接
登陆摸瓜网站后查看		

☰ 此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.ACCESS_WIFI_STATE	正常	查看Wi-Fi状态	允许应用程序查看有关 Wi-Fi 状态的信息
android.permission.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取

android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
com.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
android.permission.CAMERA2	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
android.permission.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
android.permission.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
		Unknown	

android.permission.INTERACT_ACROSS_USERS_FULL	未知	permission	Unknown permission from android reference
android.permission.GET_TOP_ACTIVITY_INFO	未知	Unknown permission	Unknown permission from android reference
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.ACCESS_FINE_LOCATION	危险	精细定位 (GPS)	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.BROADCAST_PACKAGE_ADDED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_CHANGED	未知	Unknown permission	Unknown permission from android reference

android.permission.BROADCAST_PACKAGE_INSTALL	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_REPLACED	未知	Unknown permission	Unknown permission from android reference
android.permission.RESTART_PACKAGES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
com.sh.shuihulu.kiwi.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.sh.shuihulu.kiwi.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.BLUETOOTH_CONNECT	未知	Unknown permission	Unknown permission from android reference
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
android.permission.NETWORK_PROVIDER	未知	Unknown permission	Unknown permission from android reference
com.heytao.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.sh.shuihulu.kiwi.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference

com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.sh.shuihulu.kiwi.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.sec.android.provider.badge.permission.READ	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或徽章
com.majeur.launcher.permission.UPDATE_BADGE	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或标记为固体。
com.huawei.android.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章
com.huawei.android.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章

com.hihonor.android.launcher.permission.CHANGE_BADGE	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_APP_BADGE	正常	显示应用程序通知	允许应用程序显示应用程序图标徽章
com.oppo.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	未知	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	Unknown permission	Unknown permission from android reference
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa.SECURITY_ACCESS	未知	Unknown permission	Unknown permission from android reference
com.sh.shuihulu.kiwi.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.permission.PUSH	未知	Unknown	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.yicheng.assemble.activity.LauncherActivity	Schemes: kiwi://,
com.tencent.tauth.AuthActivity	Schemes: \ 1110653580://,
k.i.w.i.m.assemble.activity.KiwiAliRealNameAuthActivity	Schemes: kiwialpverify://, Hosts: result,