



MoGua

咪咕快游 6.9.2.0.APK 分析报告



APP名称:

咪咕快游

包名: com.cmgame.gamehalltv

域名线索: 8条

URL线索: 3条

邮箱线索: 2条

分析日期: 2025年8月2日

分析平台: [摸瓜APK反编译平台](#)

文件名: mgjy_111212.apk
文件大小: 52.03MB
MD5值: 867c39cc03daad46b97d149ffafa1b91
SHA1值: 511fea6f633c4a19ffe6694bfa8564f9489f9ec6
SHA256值: 453425cc596d0fe4437d29db80a1561a5a3e9b6ff22abbea0cc102e93ca29f20

i APP 信息

App名称: 咪咕快游
包名: com.cmgame.gamehalltv
主活动Activity: com.cmgame.gamehalltv.WelcomeActivity
安卓版本名称: 6.9.2.0
安卓版本: 6920

🔍 域名线索

域名	服务器信息
mb.knowyou.com.cn	IP: 112.50.250.146 所属国家: China 地区: Fujian 城市: Nanping 纬度: 26.645119 经度: 118.173515
www.openssl.org	IP: 34.36.58.177 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
120.202.254.225	IP: 120.202.254.225 所属国家: China 地区: Hubei

	城市: Wuhan 纬度: 30.583330 经度: 114.266853
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
120.202.254.226	IP: 120.202.254.226 所属国家: China 地区: Hubei 城市: Wuhan 纬度: 30.583330 经度: 114.266853
172.16.1.132	IP: 172.16.1.132 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
218.206.26.77	IP: 218.206.26.77 所属国家: China 地区: Chongqing 城市: Chongqing 纬度: 29.562780 经度: 106.553101
218.206.26.78	IP: 218.206.26.78 所属国家: China 地区: Chongqing 城市: Chongqing 纬度: 29.562780 经度: 106.553101

URL线索

URL信息	Url所在文件
https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection	org/java_websocket/AbstractWebSocket.java
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libijkffmpeg.so
http://172.16.1.132:8081/MobileBoxWebService/index	lib/armeabi-v7a/libkysdk.so
http://mb.knowyou.com.cn:18090/BlktvWebService/index	lib/armeabi-v7a/libkysdk.so
http://218.206.26.77:6869/MobileBoxWebService/index	lib/armeabi-v7a/libkysdk.so
http://218.206.26.78:6869/MobileBoxWebService/index	lib/armeabi-v7a/libkysdk.so
http://120.202.254.225:18080/MobileBoxWebService/index	lib/armeabi-v7a/libkysdk.so
http://120.202.254.226:18080/MobileBoxWebService/index	lib/armeabi-v7a/libkysdk.so

邮箱线索

邮箱地址	所在文件
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so
ftp@example.com	lib/armeabi-v7a/libkysdk.so

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=CN, ST=Jiangsu, L=Nanjing, O=Emagsoftware, OU=Tian, CN=Lu
签名算法: rsassa_pkcs1v15
有效期自: 2010-09-21 06:12:28+00:00
有效期至: 2038-02-06 06:12:28+00:00
发行人: C=CN, ST=Jiangsu, L=Nanjing, O=Emagsoftware, OU=Tian, CN=Lu
序列号: 0x4c984ccc
哈希算法: sha1
md5值: 09897a6d2602fc7e81d14df20188cc3d
sha1值: 0310a60fabdb768472452708b9a51f61cc7a4592
sha256值: d347f0607b0fbdb4e6b942f95c64205f7bc781b13fba90df43ea3b92d4d96955
sha512值: f5e36cb21f07af03f2333435c07354b649c5c0aa079ec14c291143c6e95b4987c8cf14f0c856fb8bc11e81d8add6117df3623f5bf5e28b6e52bb42be9584bbae
公钥算法: rsa
密钥长度: 1024
指纹: ad97c2d3e3b3a950cb8549c92246d41867ced1326abfa2a2873f835fcb623b35

硬编码敏感信息

可能的敏感信息
"DANGBEI_APPKEY" : "b6c0bd7986dc0d1944004ea9046329e7"
"DANGBEI_PAY_APPKEY" : "9a52a7af80fc16dd21ae1a48"
"Le_AppKey" : "ef7fe7d8a294c098c5115c1d0b4eb8a5"

"Le_EncryptionKey" : "rcpbq6ehgtfjaayqa9mvrtdt0fhh6gvdt"
"child_password" : "您的儿童锁密码为： "
"home_str_find_password" : "重置密码"
"home_str_forget_pwd" : "忘记密码？ "
"home_str_private" : "《隐私政策》 "
"migu_secret_policy" : "您可以在系统设置中找到“咪咕快游”查看或修改授权，但可能会影响部分功能的使用。其它有关本产品的用户个人信息保护和隐私政策的详细内容，可见《咪咕隐私权政策》及《咪咕用户服务协议》 。 进入App，您可在【我的】>【隐私政策】 查看咪咕快游TV版隐私政策及相关信息，在【我的】>【版本信息】 查看《咪咕用户服务协议》 。 "
"sso_str_manual_unlock_pwd" : "移动号码用户可编辑短信“JS”发送至"
"sso_str_up_pwd_err1" : "密码错误，您还有1次机会"
"sso_str_up_pwd_err2" : "密码错误，您还有2次机会"
"sso_str_up_pwd_err_limit" : "密码错误次数已达上限，建议重置密码或24小时后再试"
"token_over_time" : "服务器连接失败， 请重试"

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
com.aspire.hbhdc.permission.PAY_SERVICE	未知	Unknown permission	Unknown permission from android reference
com.aspire.jshdc.permission.PAY_SERVICE	未知	Unknown permission	Unknown permission from android reference
com.cmhi.softmbh.provider.READ	未知	Unknown permission	Unknown permission from android reference
com.cmhi.softmbh.contentprovider.READ	未知	Unknown permission	Unknown permission from android reference
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
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.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.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_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.WRITE_OWNER_DATA	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_OWNER_DATA	未知	Unknown permission	Unknown permission from android reference
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.USB	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.KILL_BACKGROUND_PROCESSES	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.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
com.chinamobile.middleware.auth.contentprovider.READ	未知	Unknown permission	Unknown permission from android reference
iflytek.permission.OPEN_PLATFORM	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。
com.xiaomi.permission.AUTH_SERVICE	未知	Unknown permission	Unknown permission from android reference

		permission	
com.cmgame.gamehalltv.PLUGIN_SERVICE	未知	Unknown permission	Unknown permission from android reference
com.cmgame.gamehalltv.TVGAMESERVICE	未知	Unknown permission	Unknown permission from android reference
android.permission.PACKAGE_USAGE_STATS	合法	更新组件使用统计	允许修改收集的组件使用统计。不供普通应用程序使用
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
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.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
android.permission.CHANGE_WIFI_MULTICAST_STATE	正常	允许Wi-Fi多播接收	允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.cmgame.gamehalltv.WelcomeActivity	Schemes: cmgamehalltv://, Hosts: epq,