MoGua

快云影音 1.5.5.APK 分析报告

APP名称: 快云影音

包名:	com.rx.rongxingnaozhong
域名线索:	0条
URL线索:	0条
邮箱线索:	1条
分析日期:	2025年9月16日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: kyyy1.5.5.apk
文件大小: 32.51MB
MD5值: 50a61f913a4ef4c49256acc6b54a7aa5
SHA1值: 013bb571a8feb6282e87ced0d78d9fca3ca83d8d
SHA256值: cb974653205f863e1ff9b7386fb25580b637d0b5f1540ce6f0f336b0b2bbfb06

APP 信息

App名称: 快云影音
包名: com.rx.rongxingnaozhong
主活动Activity: com.rx.rongxingnaozhong.SplashActivity
安卓版本名称: 1.5.5
安卓版本: 65

域名线索

URL线索

邮箱线索

邮箱地址	所在文件
邮件至tuiguangvip2021_3@163.com 邮箱tuiguangvip2021_3@163.com	Mogua Engine V1

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=20000, ST=henansheng, L=henansheng, O=kuaiyun, OU=kuaiyun, CN=kuaiyun
签名算法: rsassa_pkcs1v15
有效期自: 2021-10-20 07:54:40+00:00
有效期至: 2046-10-14 07:54:40+00:00
发行人: C=20000, ST=henansheng, L=henansheng, O=kuaiyun, OU=kuaiyun, CN=kuaiyun
序列号: 0x77745891
哈希算法: sha256
md5值: 8afc2c4511f554bc083ecd017fd9eb21
sha1值: 86d6ced3f70e7130f07580fa86a7402ba517c904
sha256值: bc3d9d19377435252305f7490776983ea2f3411c1cd80fb5cc53315f13510cd0
sha512值: 2335b3d0ec85a1f0d741f8ea9a9d90c77255688e7c8bb1ef49eca09ed9b20e72cd7eec59206a3eb8e2018441efef860e716b76791e06456a03bd4f32976413e7
公钥算法: rsa
密钥长度: 2048
指纹: 3df3c997841bbc74194f8e899d1b77c615962def833fea7e9d94ff37600bb0d2

硬编码敏感信息

可能的敏感信息
"forget_pwd" : "找回密码"
"pwd_sure" : "确定"

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.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.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.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_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
com.rx.rongxingnaozhong.openadsdk.permission.TT_PANGOLIN	未知	Unknown permission	Unknown permission from android reference
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
		检索正在运行	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

android.permission.GET_TASKS	危险	的应用程序	发现有关其他应用程序的私人信息
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.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.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
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.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.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。
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.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.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.REPLACE_EXISTING_PACKAGE	未知	Unknown permission	Unknown permission from android reference

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
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.ACTIVITY_RECOGNITION	危险	允许应用程序识别身体活动	允许应用程序识别身体活动
com.asus.msa.SupplementaryDID.ACCESS	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.EXPAND_STATUS_BAR	正常	展开/折叠状态栏	允许应用程序展开或折叠状态栏

应用内通信

报告由 **摸瓜**APK**反编译平台** 自动生成，并非包含所有检测结果，有疑问请联系管理员。