MoGua

九色™视频 1.1.6.APK 分析报告

APP名称:	九色™视频

包名:	com.jiuse.androidwebview
域名线索:	10条
URL线索:	14条
邮箱线索:	0条
分析日期:	2025年7月18日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: JS_V1.1.6_6_20221022_2358.apk
文件大小: 7.37MB
MD5值: b2fbfbb9d0996e91c0f570be18e83d1f
SHA1值: af5efd9843a4114661400b04bccdb69409955f63
SHA256值: d965278135c2578c692f65dd3101f7799a961102575cb2f5b25a407d7e52e9e8

APP 信息

App名称: 九色™视频
包名: com.jiuse.androidwebview
主活动Activity: com.jiuse.androidwebview.main.WelcomeActivity
安卓版本名称: 1.1.6
安卓版本: 6

域名线索

域名	服务器信息
vbi2.qiyuewuyi.xyz	**IP**: 23.224.48.29 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052231 **经度**: -118.243683
xml.apache.org	**IP**: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
jstv888.xyz	**IP**: 104.21.9.155 **所属国家**: United States of America **地区**: California

	城市: San Francisco **纬度**: 37.775700 **经度**: -122.395203
jstv666.xyz	IP: 23.224.48.20 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052231 **经度**: -118.243683
vbi1.qiyuewuyi.xyz	IP: 23.224.48.2 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052231 **经度**: -118.243683
vbi3.qiyuewuyi.xyz	IP: 23.224.48.22 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052231 **经度**: -118.243683
jstv777.xyz	IP: 172.67.204.48 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
vipmedia-20b07.firebaseio.com	IP: 34.120.160.131 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
	IP: 20.205.243.166

github.com	**所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
aria.laoyuyu.me	IP: 118.24.25.24 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232

URL线索

URL信息	Url所在文件
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/rxjava3/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Observable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Flowable.java
http://xml.apache.org/xslt	com/blankj/utilcode/util/LogUtils.java
https://vbi3.qiyuewuyi.xyz/app/startup	com/jiuse/androidwebview/Constant.java

https://vbi1.qiyuewuyi.xyz	com/jiuse/androidwebview/Constant.java
https://vbi2.qiyuewuyi.xyz	com/jiuse/androidwebview/Constant.java
https://vbi3.qiyuewuyi.xyz	com/jiuse/androidwebview/Constant.java
https://jstv666.xyz	com/jiuse/androidwebview/Constant.java
https://jstv777.xyz	com/jiuse/androidwebview/Constant.java
https://jstv888.xyz	com/jiuse/androidwebview/Constant.java
https://vbi2.qiyuewuyi.xyz/app/domains	com/jiuse/androidwebview/Constant.java
https://vbi1.qiyuewuyi.xyz/app/update	com/jiuse/androidwebview/Constant.java
https://aria.laoyuyu.me/aria_doc/create/any_java.html	com/arialyy/aria/core/Aria.java
https://aria.laoyuyu.me/aria_doc/other/annotaion_invalid.html	com/arialyy/aria/core/download/DownloadReceiver.java
https://github.com/AriaLyy/Aria/issues/597	com/arialyy/aria/core/download/m3u8/M3U8Option.java
https://aria.laoyuyu.me/aria_doc/other/annotaion_invalid.html	com/arialyy/aria/core/upload/UploadReceiver.java
https://vipmedia-20b07.firebaseio.com	Mogua Engine V1

邮箱线索

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: O=JiuSe, OU=JS
签名算法: rsassa_pkcs1v15
有效期自: 2022-03-21 11:24:39+00:00
有效期至: 2047-03-15 11:24:39+00:00
发行人: O=JiuSe, OU=JS
序列号: 0x8ed61b3
哈希算法: sha256
md5值: 91b47a563c6297b319ec2b13fb064434
sha1值: f75dcd3df5b96e05d5412fa64c1414e9e5aea3b8
sha256值: 591c8653f5977d9325431be2efc8344d6bb8913ee74e7a21ea3f8ea876e15f05
sha512值: 9b06603ebb784fb0ad7df0ea2bdde204887f72d53db3327c302fb3f6b4c52a941979d5e31f89c460cb84c827fbcf0cfd0cd6ed96c61025f5be318eb764fee2a4
公钥算法: rsa
密钥长度: 2048
指纹: 71c04815f6ef43fd22923745052f7a20ef4617ba0318377d1559cd649b277989

硬编码敏感信息

可能的敏感信息
"firebase_database_url" : "https://vipmedia-20b07.firebaseio.com"
"google_api_key" : "AIzaSyAZ7q467qAf-vZkm42Swc8EkdGnZ39wSwU"
"google_crash_reporting_api_key" : "AIzaSyAZ7q467qAf-vZkm42Swc8EkdGnZ39wSwU"

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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
		读取/修改/	

android.permission.WRITE_EXTERNAL_STORAGE	危险	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.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_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.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.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	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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价
android.permission.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
android.permission.READ_CALENDAR	危险	读取日历事件	允许应用程序读取您手机上存储的所有日历事件。恶意应用程序可以借此将您的日历事件发送给其他人
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.MODIFY_PHONE_STATE	系统需要	修改电话状态	允许应用程序控制设备的电话功能。具有此权限的应用程序可以切换网络,打开和关闭电话收音机等,而无需通知您
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.FLASHLIGHT	正	控制手电筒	允许应用程序控制手电筒

	常		
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
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.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。
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

---