



# MoGua

## 美视 null.APK 分析报告



APP名称:

美视

包名:	wmp.jfohva.dksbsjx
域名线索:	6条
URL线索:	17条
邮箱线索:	0条
分析日期:	2025年7月16日
分析平台:	<a href="#">摸瓜APK反编译平台</a>

文件名: 美视 (视频库).apk

文件大小: 27.79MB

MD5值: f3c557d553c82bc0e80b5130301a8d83

SHA1值: aacb7e6e1d6fd45bf2223ff3fc4e773b25069c90

SHA256值: 9f3942771eaf2d6cde04ce90e6e7ba79a10061b9eb02b1de7b9d2acbc05341fd

## i APP 信息

App名称: 美视

包名: wmp.jfohva.dksbsjx

主活动Activity: io.dcloud.PandoraEntry

安卓版本名称: null

安卓版本:

## 🔍 域名线索

域名	服务器信息
er.dcloud.io	没有服务器地理信息.
ns.adobe.com	没有服务器地理信息.
m3w.cn	IP: 42.231.138.188 所属国家: China 地区: Henan 城市: Nanyang 纬度: 32.994720 经度: 112.532784
ask.dcloud.net.cn	IP: 123.125.244.31 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

schemas.android.com	没有服务器地理信息.
er.dcloud.net.cn	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000

## URL线索

URL信息	Url所在文件
<a href="http://schemas.android.com/apk/res/android">http://schemas.android.com/apk/res/android</a>	com/hjq/permissions/AndroidManifestParser.java
<a href="http://ns.adobe.com/xap/1.0/\u0000">http://ns.adobe.com/xap/1.0/\u0000</a>	io/dcloud/common/util/ExifInterface.java
<a href="https://m3w.cn/s/">https://m3w.cn/s/</a>	io/dcloud/common/util/ShortCutUtil.java
<a href="https://ask.dcloud.net.cn/article/282">https://ask.dcloud.net.cn/article/282</a>	io/dcloud/common/constant/DOMException.java
<a href="https://ask.dcloud.net.cn/article/35058">https://ask.dcloud.net.cn/article/35058</a>	io/dcloud/feature/audio/AudioRecorderMgr.java
<a href="https://ask.dcloud.net.cn/article/283">https://ask.dcloud.net.cn/article/283</a>	io/dcloud/feature/utsplugin/ProxyModule.java
<a href="https://er.dcloud.io/sc">https://er.dcloud.io/sc</a>	io/dcloud/feature/gg/dcloud/ADHandler.java
<a href="https://er.dcloud.net.cn/sc">https://er.dcloud.net.cn/sc</a>	io/dcloud/feature/gg/dcloud/ADHandler.java
<a href="https://ask.dcloud.net.cn/article/35627">https://ask.dcloud.net.cn/article/35627</a>	io/dcloud/p/r.java
<a href="https://ask.dcloud.net.cn/article/35877">https://ask.dcloud.net.cn/article/35877</a>	io/dcloud/p/r.java

https://ask.dcloud.net.cn/article/283	io/dcloud/p/h1.java
https://er.dcloud.io/rv	io/dcloud/p/d0.java
https://er.dcloud.net.cn/rv	io/dcloud/p/d0.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java

## 邮箱线索

## 手机线索

## 签名证书

APK已签名

v1 签名: False

v2 签名: True

v3 签名: False

找到 1 个唯一证书

主题: C=hunxquwhbggebhx, ST=fnxymvnhfabgpq, L=brjkojdmjmvkhjn, O=ekk1751941866388, OU=fuc1751941866388, CN=Xhjt1751941866388

签名算法: rsassa\_pkcs1v15

有效期自: 2025-07-08 02:31:06+00:00

有效期至: 2075-06-26 02:31:06+00:00

发行人: C=hunxquwhbggebhx, ST=fnxymvnhfabgpq, L=brjkojdmjmvkhjn, O=ekk1751941866388, OU=fuc1751941866388, CN=Xhjt1751941866388

序列号: 0x40b4bfc

哈希算法: sha1

md5值: 94d46305c6ff7ab398f7606fc5e02221

sha1值: 67475a5c6c6b082a1e78b8ddbe6b31c5399b015e

sha256值: 6546f764cb72afe2908cc1a13f92c8d8029742dc84e4da558c1225e738f00604

sha512值: cd66410717f4b26047327bfc1dec9791fba22de1bbff6c8f942cb8619123a1603ead758b98f792b399a13e91cb3c80edd1a056af9136af2d9a0c5e5c5c87ebc2

公钥算法: rsa

密钥长度: 1024

指纹: 144cd8755331ecee6c9b770431275d8c7e6b96a37a398afd66e5cbbcb550f51a

## 硬编码敏感信息

## 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

	是否		

向手机申请的权限	危险	类型	详细情况
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_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.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.READ_MEDIA_IMAGES	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.READ_MEDIA_VISUAL_USER_SELECTED	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.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.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。
wmp.jfohva.dksbsjx_com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
	未知	Unknown	

wmp.jfohva.dksbsjx_com.asus.msa.SupplementaryDID.ACCESS	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
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
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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.WRITE_CONTACTS	危险	写入联系人数据	允许应用程序修改您手机上存储的联系人 (地址) 数据。恶意应用程序可以使用它来删除或修改您的联系人数据
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表

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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.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

## 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。