MoGua

华数TV 5.0.0.119.APK 分析报告

APP名称: 华数TV

包名:	cn.com.wasu.main
域名线索:	17条
URL线索:	18条
邮箱线索:	0条
分析日期:	2025年6月18日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: WasuTV5.0_unicom_shanxi_5.0.0.119_202406121634.apk
文件大小: 17.46MB
MD5值: 1724c0a57aabb8a607ace0d16c134b0f
SHA1值: db6455af58dfc155ed46c2493a1428d8624f768d
SHA256值: 3d585c9129b40a37c1a8b34eb1c1ca3d9695956c2794395af2ef5a61bdca1297

APP 信息

App名称: 华数TV
包名: cn.com.wasu.main
主活动Activity: cn.com.wasu.main.page.start.WelcomeActivity
安卓版本名称: 5.0.0.119
安卓版本: 50000119

域名线索

域名	服务器信息
delivery.wasu.cn	**IP**: 47.96.193.68 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
itf.upm.wasu.tv	**IP**: 47.96.193.116 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
schemas.android.com	没有服务器地理信息.

itf-zw.upm.wasu.tv	**IP:** 101.37.45.139 **所属国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161583
schemas.microsoft.com	**IP:** 13.107.246.73 **所属国家:** United States of America **地区:** Washington **城市:** Redmond **纬度:** 47.682899 **经度:** -122.120903
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
pr.expressplay.cn	没有服务器地理信息.
api.ipify.org	**IP:** 104.26.13.205 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203
202.99.114.14	**IP:** 202.99.114.14 **所属国家:** China **地区:** Tianjin **城市:** Tianjin **纬度:** 39.142181 **经度:** 117.176102
	IP: 121.43.183.80 **所属国家:** China

update-new.wasu.tv	**地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
time.wasu.tv	IP: 124.95.150.71 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
61.160.200.252	IP: 61.160.200.252 **所属国家**: China **地区**: Jiangsu **城市**: Changzhou **纬度**: 31.783331 **经度**: 119.966667
www.baidu.com	IP: 110.242.70.57 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
127.0.0.1	IP: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
android-update.wasu.tv	IP: 121.196.207.154 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583

adash.man.aliyuncs.com	**IP**: 59.82.40.77 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
m.wasu	没有服务器地理信息.

URL线索

URL**信息**	Url**所在文件**
http://itf.upm.wasu.tv/um	cn/com/wasu/main/TVApp.java
http://itf.upm.wasu.tv/p	cn/com/wasu/main/TVApp.java
http://itf.upm.wasu.tv/pay	cn/com/wasu/main/TVApp.java
http://m.wasu	cn/com/wasu/main/oem/IAuthCallback.java
https://www.baidu.com	cn/com/wasu/main/page/NetworkCheckActivity.java
http://delivery.wasu.cn/d/vmap/1.0?prd=	cn/com/wasu/main/etc/property/a.java
http://schemas.android.com/apk/res/android	com/flyco/banner/widget/Banner/base/BaseBanner.java
https://api.ipify.org?format=text	com/wasu/log_service_base/model/LogStatisticConfig.java
http://61.160.200.252	com/wasu/model/wasuwebview/WasuWebView.java
http://202.99.114.14:35820/ACS/vas/serviceorder	com/wasu/oem/OEMInVokeImpl.java

https://itf-zw.upm.wasu.tv/upm-ip/getIP	com/wasu/oem/OEMInVokeImpl.java
http://itf-zw.upm.wasu.tv/otn/plan/auth/getAuthResult	com/wasu/oem/pay/UPMUtil.java
https://time.wasu.tv/getJsonTime	com/wasu/decode/WatchDog.java
https://adash.man.aliyuncs.com/man/api	com/wasu/statistics/restful/a.java
http://adash.man.aliyuncs.com:80/man/api	com/wasu/statistics/restful/a.java
http://android-update.wasu.tv/allinone/action.do	com/wasu/update/action/g.java
http://update-new.wasu.tv/LauncherZhilinkServiceV2/action.do	com/wasu/update/action/h.java
http://update-new.wasu.tv/LauncherZhilinkServiceV2/action.do	com/wasu/update/action/i.java
http://127.0.0.1	com/media/MediaUtil.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	com/media/a/a.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	com/media/exoplayer/f.java
http://pr.expressplay.cn/playready/RightsManager.asmx	com/media/exoplayer/f.java
https://github.com/yyued/SVGAPlayer-Android	com/opensource/svgaplayer/SVGAParser.java

邮箱线索

手机线索

手机号	所在文件

15552000000	cn/com/wasu/main/TVApp.java

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=zh, ST=zj, L=hz, O=wasu, OU=wasu, CN=wasu
签名算法: rsassa_pkcs1v15
有效期自: 2012-03-06 02:41:33+00:00
有效期至: 2285-12-20 02:41:33+00:00
发行人: C=zh, ST=zj, L=hz, O=wasu, OU=wasu, CN=wasu
序列号: 0x4f55795d
哈希算法: sha1
md5值: 610c75bea660ee26b52ab8f6ec28073d
sha1值: 792baef4176c74b8772347a00c200b57eea11554
sha256值: 479e6b31e49686d33157f544065f56c6a36d4ffffab331959618102706a60275
sha512值: 762da25c3396d26f0078f0f3f4303a98a83a7c75b1ab2f72dbef8537dc2c5311ffaec6c5de209b6686135aa0d9fc7f151abf6eb07fd4ce31c2327cf7e7e436fa
公钥算法: rsa
密钥长度: 1024
指纹: d44fecbc4bd4c5f2b17f6b160275fc81beb434832dca7a88ff4cc966c7080f4f

硬编码敏感信息

可能的敏感信息
"key" : "键"

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.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.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.CHANGE_WIFI_MULTICAST_STATE	正常	允许Wi-Fi多播	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

		接收	有用。它比非多播模式使用更多的功率
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_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.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.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.RAISED_THREAD_PRIORITY	未知	Unknown permission	Unknown permission from android reference
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.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
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.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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。

应用内通信
