Evaluation Warning: The document was created with Spire.Doc for Python.

**昆明有线（ 2.0.0-20240912173002版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 昆明有线 |
| 版本 | 2.0.0-20240912173002 |
| 包名 | com.ipanel.join.homed.stb |
| 域名线索 | 6条 |
| URL线索 | 5条 |
| APP图标 |  |
| 分析日期 | 2025年7月5日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | kunming\_mini-release-v1.1.732(1).apk |
| 文件大小 | 0.19MB |
| MD5值 | bda1105fc8a176c938344aa0d0edea68 |
| SHA1值 | d66c1d554e3243a7f89bbec61e30eeabeda93984 |
| SHA256值 | ac02983daa32d2b00178065691486d728be90eaa6abb3ae962becb8c040e0c18 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 昆明有线 |
| 包名 | com.ipanel.join.homed.stb |
| 主活动Activity | com.ipanel.join.homed.stb.HostLaunchActivity |
| 安卓版本名称 | 2.0.0-20240912173002 |
| 安卓版本 | 205 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| cloudupgrade.96599.cn | IP: 39.129.78.132 所属国家: China 地区: Yunnan 城市: Kunming  |
| slave.s | 没有服务器地理信息.  |
| access.s | 没有服务器地理信息.  |
| ipanellog.homed.tv | IP: 113.98.233.203 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| git.ipanel.cn | IP: 58.251.130.218 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| collect.s | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://access.%s  | com/ipanel/join/homed/stb/BuildConfig.java  |
| http://collect.%s/collect/resource  | com/ipanel/join/homed/stb/BuildConfig.java  |
| http://slave.%s  | com/ipanel/join/homed/stb/BuildConfig.java  |
| https://cloudupgrade.96599.cn:50443  | com/ipanel/join/homed/stb/BuildConfig.java  |
| http://git.ipanel.cn/project/820037/mini\_apk.release.git  | com/ipanel/join/homed/stb/BuildConfig.java  |
| http://%s:%s/router/vgater/device/action?cmd=get\_info  | com/ipanel/join/homed/stb/OooOOO0.java  |
| https://cloudupgrade.96599.cn:50443/s/todolist  | com/ipanel/join/homed/stb/DexManager.java  |
| https://cloudupgrade.96599.cn:50443/s/todolist/tvmiddleware/v1/apkdownload  | com/ipanel/join/homed/stb/DexManager.java  |
| https://cloudupgrade.96599.cn:50443/s/todolist/tvmiddleware/v1/guideapkdownload  | com/ipanel/join/homed/stb/DexManager.java  |
| https://cloudupgrade.96599.cn:50443/s/todolist/tvmiddleware/v1/gettvid  | com/ipanel/join/homed/stb/DexManager.java  |
| https://cloudupgrade.96599.cn:50443/s/todolist/tvmiddleware/v1/get3rdapkindex  | com/ipanel/join/homed/stb/DexManager.java  |
| https://cloudupgrade.96599.cn:50443/s/todolist/tv/qrcode1/  | com/ipanel/join/homed/stb/OooO0o.java  |
| http://ipanellog.homed.tv/ipanelcloudlog/\_bulk/  | com/ipanel/join/homed/stb/mini\_patch/OooO0OO.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| ipanel2021@homed.tv  | com/ipanel/join/homed/stb/mini\_patch/OooO0OO.java  |

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: True 找到 1 个唯一证书 主题: C=CN, ST=GuangDong, L=ShenZhen, O=ipanel, OU=ipanel, CN=ipanel, E=ipanel@ipanel.cn 签名算法: rsassa\_pkcs1v15 有效期自: 2022-02-16 02:07:28+00:00 有效期至: 2122-01-23 02:07:28+00:00 发行人: C=CN, ST=GuangDong, L=ShenZhen, O=ipanel, OU=ipanel, CN=ipanel, E=ipanel@ipanel.cn 序列号: 0xc50bd215f833dd37 哈希算法: sha1 md5值: 96de99e7b4170652e08ff20d7a868438 sha1值: bdb290986b201c6d5eb5433a6a73b8447a35f995 sha256值: 316e5f4c7d37055d917ef3e070deccb719fd6d1cd02da1d1f18d45df537009fe sha512值: 1185ed1b569926b2607f3d3c2d18de9b74e1de2bb473ddd42a487781abcc619ab3609ec9679055b2fbdc8abb0be84f588411177c913e2846120df06af80234a8 公钥算法: rsa 密钥长度: 2048 指纹: e578a08b724d6d42dd6f39d1ba8d1c3d2a1aef1c4de7d2efe2bafad2410e204e**

## **6. 硬编码敏感信息**

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 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.INJECT\_EVENTS | 合法 | 按键和控制按钮 | 允许应用程序将其自己的输入事件（按键等）传递给其他应用程序。恶意应用程序可以利用它来接管电话 |
| com.mitv.tvhome.permission.HOME\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.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.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.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\_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\_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\_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.DISABLE\_KEYGUARD | 正常 |  | 如果键盘不安全,允许应用程序禁用它。 |
| android.permission.BROADCAST\_STICKY | 正常 | 发送粘性广播 | 允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定 |
| 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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.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.CAPTURE\_VIDEO\_OUTPUT | 正常 |  | 允许应用程序捕获视频输出 |
| android.permission.CAPTURE\_SECURE\_VIDEO\_OUTPUT | 正常 |  | 允许应用程序捕获安全视频输出 |
| android.permission.RETRIEVE\_WINDOW\_CONTENT | 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。  |
| 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 |

## **10. 应用内通信**

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**