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

**小果视界（ 1.2.9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 | 小果视界 |
| 版本 | 1.2.9 |
| 包名 | com.lizhi.xiaoguoshijie |
| 域名线索 | 35条 |
| URL线索 | 27条 |
| APP图标 |  |
| 分析日期 | 2025年7月21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 | 6F45CA8DF73A4661802A342F041BF88B.apk |
| 文件大小 | 21.64MB |
| MD5值 | bf91ba94a798ed943563c8f3b6024676 |
| SHA1值 | 2e01f496b3d2858e7e3544d5a98d044de0605511 |
| SHA256值 | 719c7e6a7b86a6816812f3611f487ac345b78e0357ce8dca212177680a8677e7 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 小果视界 |
| 包名 | com.lizhi.xiaoguoshijie |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 1.2.9 |
| 安卓版本 | 129 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| npms.io | IP: 104.21.4.104 所属国家: United States of America 地区: California 城市: San Francisco  |
| openjsf.org | IP: 23.185.0.1 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.google.com | IP: 199.59.148.247 所属国家: United States of America 地区: California 城市: San Francisco  |
| stream.dcloud.net.cn | IP: 47.99.97.167 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| ask.dcloud.net.cn | IP: 36.102.212.39 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| 192.168.50.105 | IP: 192.168.50.105 所属国家: - 地区: - 城市: -  |
| at.alicdn.com | IP: 111.225.210.163 所属国家: China 地区: Hebei 城市: Langfang  |
| er.dcloud.net.cn | IP: 47.97.228.179 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| koc-img.lizhibj.cn | IP: 220.181.158.230 所属国家: China 地区: Beijing 城市: Beijing  |
| lame.sf.net | IP: 104.18.26.198 所属国家: United States of America 地区: California 城市: San Francisco  |
| mp-281e3ee8-3380-4740-9b6e-11eac5254879.cdn.bspapp.com | IP: 106.39.240.36 所属国家: China 地区: Beijing 城市: Beijing  |
| www.mescroll.com | IP: 106.39.240.48 所属国家: China 地区: Beijing 城市: Beijing  |
| apis.map.qq.com | IP: 109.244.244.223 所属国家: China 地区: Beijing 城市: Beijing  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| feross.org | IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont  |
| er.dcloud.io | 没有服务器地理信息.  |
| lodash.com | IP: 52.74.166.77 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| mths.be | IP: 83.137.145.144 所属国家: Netherlands 地区: Groningen 城市: Groningen  |
| cdn.uviewui.com | IP: 36.103.176.220 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| crbug.com | IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View  |
| service.dcloud.net.cn | IP: 121.41.10.27 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| stream.mobihtml5.com | IP: 23.27.132.60 所属国家: United States of America 地区: California 城市: Santa Clara  |
| ns.adobe.com | 没有服务器地理信息.  |
| www.tuixiaoguo.com | IP: 39.107.209.219 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| xgsj.lizhibj.cn | IP: 39.107.209.219 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| m3w.cn | IP: 36.102.212.34 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| underscorejs.org | IP: 104.21.25.112 所属国家: United States of America 地区: California 城市: San Francisco  |
| github.com | IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond  |
| quilljs.com | IP: 216.24.57.253 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.iconfont.cn | IP: 59.82.23.172 所属国家: China 地区: Beijing 城市: Beijing  |
| schemas.android.com | 没有服务器地理信息.  |
| help.aliyun.com | IP: 203.119.144.7 所属国家: China 地区: Beijing 城市: Beijing  |
| example.com | IP: 93.184.216.34 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| open.douyin.com | IP: 42.185.153.125 所属国家: China 地区: Heilongjiang 城市: Harbin  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://ask.dcloud.net.cn/article/35058  | io/dcloud/feature/audio/AudioRecorderMgr.java  |
| https://er.dcloud.io/sc  | io/dcloud/feature/gg/dcloud/ADHandler.java  |
| https://er.dcloud.net.cn/sc  | io/dcloud/feature/gg/dcloud/ADHandler.java  |
| http://ask.dcloud.net.cn/article/283  | io/dcloud/feature/utsplugin/ProxyModule.java  |
| https://ask.dcloud.net.cn/article/287  | io/dcloud/share/IFShareApi.java  |
| http://ask.dcloud.net.cn/article/283  | io/dcloud/g/b.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | io/dcloud/common/util/ExifInterface.java  |
| http://m3w.cn/s/  | io/dcloud/common/util/ShortCutUtil.java  |
| https://stream.mobihtml5.com/  | io/dcloud/common/constant/StringConst.java  |
| https://stream.dcloud.net.cn/  | io/dcloud/common/constant/StringConst.java  |
| http://ask.dcloud.net.cn/article/282  | io/dcloud/common/constant/DOMException.java  |
| https://er.dcloud.io/rv  | io/dcloud/e/c/h/b.java  |
| https://er.dcloud.net.cn/rv  | io/dcloud/e/c/h/b.java  |
| https://ask.dcloud.net.cn/article/35627  | io/dcloud/e/b/a.java  |
| https://ask.dcloud.net.cn/article/35877  | io/dcloud/e/b/a.java  |
| http://schemas.android.com/apk/res/android  | pl/droidsonroids/gif/GifTextView.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  |
| https://ask.dcloud.net.cn/article/36199  | Mogua Engine V1  |
| https://apis.map.qq.com/jsapi?qt=translate&type=1&points=  | Mogua Engine V2  |
| https://koc-img.lizhibj.cn/XGSJ/prospect\_applet.jpg);background-size:100%  | Mogua Engine V2  |
| https://www.iconfont.cn/manage  | Mogua Engine V2  |
| https://koc-img.lizhibj.cn/applet/mini-program.png?t=2  | Mogua Engine V2  |
| https://at.alicdn.com/t/c/font\_1387774\_eggbzxwk9lj.woff2?t=1681875309878)  | Mogua Engine V2  |
| https://at.alicdn.com/t/c/font\_1387774\_eggbzxwk9lj.woff?t=1681875309878)  | Mogua Engine V2  |
| https://at.alicdn.com/t/c/font\_1387774\_eggbzxwk9lj.ttf?t=1681875309878)  | Mogua Engine V2  |
| https://at.alicdn.com/t/font\_2225171\_8kdcwk4po24.ttf)  | Mogua Engine V2  |
| https://service.dcloud.net.cn/uniapp/feedback.html  | Mogua Engine V2  |
| http://www.w3.org/1999/xlink  | Mogua Engine V2  |
| http://www.w3.org/2000/svg  | Mogua Engine V2  |
| http://www.w3.org/1998/Math/MathML  | Mogua Engine V2  |
| https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=  | Mogua Engine V2  |
| https://www.google.com/maps/?daddr=  | Mogua Engine V2  |
| https://www.google.com/maps/  | Mogua Engine V2  |
| http://koc-img.lizhibj.cn/manage/litui5bi4.jpg?t=jdjejkde  | Mogua Engine V2  |
| https://koc-img.lizhibj.cn/manage/ltui1bi1.jpg?t=jdjejkde  | Mogua Engine V2  |
| https://koc-img.lizhibj.cn/applet/mini-program.png?t=2  | Mogua Engine V2  |
| https://koc-img.lizhibj.cn/  | Mogua Engine V2  |
| https://github.com/crypto-browserify/crypto-browserify  | Mogua Engine V2  |
| https://github.com/indutny/elliptic/issues  | Mogua Engine V2  |
| https://github.com/indutny/elliptic  | Mogua Engine V2  |
| https://lodash.com/>  | Mogua Engine V2  |
| https://openjsf.org/>  | Mogua Engine V2  |
| https://lodash.com/license>  | Mogua Engine V2  |
| http://underscorejs.org/LICENSE>  | Mogua Engine V2  |
| https://npms.io/search?q=ponyfill.  | Mogua Engine V2  |
| https://open.douyin.com/platform/oauth/connect?response\_type=code&client\_key=awuk8wnz3cwv3ppy&scope=  | Mogua Engine V2  |
| https://xgsj.lizhibj.cn/api/public/callback/douyin/  | Mogua Engine V2  |
| https://cdn.uviewui.com/uview/album/1.jpg  | Mogua Engine V2  |
| http://www.w3.org/2000/svg  | Mogua Engine V2  |
| http://www.w3.org/2000/svg'/>  | Mogua Engine V2  |
| https://koc-img.lizhibj.cn/applet/wx\_browser.png  | Mogua Engine V2  |
| https://help.aliyun.com/document\_detail/32077.html  | Mogua Engine V2  |
| https://help.aliyun.com/document\_detail/32069.html  | Mogua Engine V2  |
| http://feross.org>  | Mogua Engine V2  |
| https://github.com/ded/bowser  | Mogua Engine V2  |
| https://feross.org/opensource>  | Mogua Engine V2  |
| https://feross.org>  | Mogua Engine V2  |
| http://mths.be/fromcodepoint  | Mogua Engine V2  |
| http://www.w3.org/XML/1998/namespace  | Mogua Engine V2  |
| http://www.w3.org/2000/xmlns/  | Mogua Engine V2  |
| http://www.w3.org/2000/xmlns/\nActual:  | Mogua Engine V2  |
| http://github.com/dominictarr/crypto-browserify  | Mogua Engine V2  |
| https://example.com  | Mogua Engine V2  |
| https://github.com/facebook/regenerator/blob/main/LICENSE  | Mogua Engine V2  |
| https://koc-img.lizhibj.cn/XGSJ/xgsj\_bg.jpg  | Mogua Engine V2  |
| https://koc-img.lizhibj.cn/wechat\_material  | Mogua Engine V2  |
| https://xgsj.lizhibj.cn/h5/pageStatic/mount/mount?token=  | Mogua Engine V2  |
| https://www.mescroll.com/img/mescroll-totop.png  | Mogua Engine V2  |
| https://www.mescroll.com/img/mescroll-empty.png  | Mogua Engine V2  |
| https://mp-281e3ee8-3380-4740-9b6e-11eac5254879.cdn.bspapp.com/cloudstorage/cd703d88-ece5-4823-b922-dfe8b6c7b48c.apk  | Mogua Engine V2  |
| https://koc-img.lizhibj.cn/applet/  | Mogua Engine V2  |
| http://127.0.0.1:3016/api  | Mogua Engine V2  |
| http://192.168.50.105:3016/api  | Mogua Engine V2  |
| https://xgsj.lizhibj.cn/api  | Mogua Engine V2  |
| https://www.tuixiaoguo.com  | Mogua Engine V2  |
| https://quilljs.com/  | Mogua Engine V2  |
| https://quilljs.com  | Mogua Engine V2  |
| http://www.w3.org/1999/xlink  | Mogua Engine V2  |
| http://www.w3.org/2000/svg  | Mogua Engine V2  |
| http://www.w3.org/1998/Math/MathML  | Mogua Engine V2  |
| https://crbug.com/v8/8520  | lib/arm64-v8a/libweexjss.so  |
| http://lame.sf.net  | lib/arm64-v8a/liblamemp3.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| git@github.com fedor@indutny.com feross@feross.org dead\_horse@qq.com  | Mogua Engine V2  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 19919152923  | Mogua Engine V2  |

## **5. 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=CN, ST=Beijing, L=Beijing, O=Lizhi, OU=Lizhi, CN=Liuyi 签名算法: rsassa\_pkcs1v15 有效期自: 2023-03-02 01:55:12+00:00 有效期至: 2048-02-24 01:55:12+00:00 发行人: C=CN, ST=Beijing, L=Beijing, O=Lizhi, OU=Lizhi, CN=Liuyi 序列号: 0x2897b550 哈希算法: sha256 md5值: a4e5a45063473c9656ff73a709ab6373 sha1值: 405979d0c71a10cb27086f5d0cc19e7629936fa1 sha256值: 6c0fd2018349ff0760609a78635ad6e4712c43d4a126e7bd9f5bd88fbca59f3e sha512值: c0b928352bd14444e33ff639b7559ba1a790ec7d541a958b00f27122e84579e992be10d8ab18a770fdeb0662309625a9a12aa0fb94b893a54cf9ad8f0647fd4b 公钥算法: rsa 密钥长度: 2048 指纹: c3c048ec9c24f1fae8b7cdac5e78a5261dd14fa5df1bb95db7b1868efc2230b7**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "aweme\_open\_auth\_title" : "抖音登录授权"  |
| "aweme\_open\_web\_auth\_cancel" : "返回"  |
| "dcloud\_common\_user\_refuse\_api" : "the user denies access to the API"  |
| "dcloud\_io\_without\_authorization" : "not authorized"  |
| "dcloud\_oauth\_authentication\_failed" : "failed to obtain authorization to log in to the authentication service"  |
| "dcloud\_oauth\_empower\_failed" : "the Authentication Service operation to obtain authorized logon failed"  |
| "dcloud\_oauth\_logout\_tips" : "not logged in or logged out"  |
| "dcloud\_oauth\_oauth\_not\_empower" : "oAuth authorization has not been obtained"  |
| "dcloud\_oauth\_token\_failed" : "failed to get token"  |
| "dcloud\_permissions\_reauthorization" : "reauthorize"  |
| "dcloud\_common\_user\_refuse\_api" : "用户拒绝该API访问"  |
| "dcloud\_io\_without\_authorization" : "没有获得授权"  |
| "dcloud\_oauth\_authentication\_failed" : "获取授权登录认证服务操作失败"  |
| "dcloud\_oauth\_empower\_failed" : "获取授权登录认证服务操作失败"  |
| "dcloud\_oauth\_logout\_tips" : "未登录或登录已注销"  |
| "dcloud\_oauth\_oauth\_not\_empower" : "尚未获取oauth授权"  |
| "dcloud\_oauth\_token\_failed" : "获取token失败"  |
| "dcloud\_permissions\_reauthorization" : "重新授权"  |

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.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.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.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.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.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\_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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| 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。 |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |

## **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。**