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

**升辉APP（ 2.0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 | 升辉APP |
| 版本 | 2.0 |
| 包名 | com.auI8b1fpti67wlfns0i049d1q |
| 域名线索 | 18条 |
| URL线索 | 23条 |
| APP图标 |  |
| 分析日期 | 2025年6月17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 | 升辉[1].apk |
| 文件大小 | 10.09MB |
| MD5值 | 330954b84cc6369e524261836d627c77 |
| SHA1值 | f7165c97db140c74017ce482a262b9761aa42c5b |
| SHA256值 | e15f0721c4ff996771ddcd64308490fac40863f8ca90ae0ff02088d460f39fac |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 升辉APP |
| 包名 | com.auI8b1fpti67wlfns0i049d1q |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 2.0 |
| 安卓版本 | 20250605 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| mclient.alipay.com | IP: 124.95.172.71  所属国家: China  地区: Liaoning  城市: Shenyang |
| er.dcloud.io | 没有服务器地理信息. |
| mobilegw.alipaydev.com | IP: 110.75.132.131  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| er.dcloud.net.cn | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| stream.mobihtml5.com | 没有服务器地理信息. |
| mobilegw.alipay.com | IP: 203.209.243.27  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| m3w.cn | IP: 116.196.150.254  所属国家: China  地区: Zhejiang  城市: Jinhua |
| stream.dcloud.net.cn | IP: 121.4.116.110  所属国家: China  地区: Beijing  城市: Beijing |
| mobilegwpre.alipay.com | IP: 110.75.138.35  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ask.dcloud.net.cn | IP: 124.163.195.89  所属国家: China  地区: Shanxi  城市: Taiyuan |
| mcgw.alipay.com | IP: 111.202.5.209  所属国家: China  地区: Beijing  城市: Beijing |
| render.alipay.com | IP: 124.95.153.222  所属国家: China  地区: Liaoning  城市: Shenyang |
| dev.dcloud.net.cn | IP: 123.12.235.54  所属国家: China  地区: Henan  城市: Hebi |
| ns.adobe.com | 没有服务器地理信息. |
| schemas.android.com | 没有服务器地理信息. |
| loggw-exsdk.alipay.com | IP: 110.76.6.82  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| h5.m.taobao.com | IP: 125.39.155.59  所属国家: China  地区: Tianjin  城市: Tianjin |
| wappaygw.alipay.com | IP: 111.202.5.210  所属国家: China  地区: Beijing  城市: Beijing |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://mobilegwpre.alipay.com/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| https://mobilegw.alipay.com/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| https://mobilegw.alipay.com/mgw.htm | com/alipay/sdk/m/l/a.java |
| https://mobilegw.alipaydev.com/mgw.htm | com/alipay/sdk/m/l/a.java |
| https://mcgw.alipay.com/sdklog.do | com/alipay/sdk/m/l/a.java |
| https://loggw-exsdk.alipay.com/loggw/logUpload.do | com/alipay/sdk/m/l/a.java |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/m/l/a.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/m/l/a.java |
| https://h5.m.taobao.com/mlapp/olist.html | com/alipay/sdk/m/m/a.java |
| https://render.alipay.com/p/s/i?scheme=%s | com/alipay/sdk/app/OpenAuthTask.java |
| https://wappaygw.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| http://wappaygw.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| http://mclient.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm | com/alipay/sdk/app/PayTask.java |
| http://mclient.alipay.com/home/exterfaceAssign.htm | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/cashier/mobilepay.htm | com/alipay/sdk/app/PayTask.java |
| http://mclient.alipay.com/cashier/mobilepay.htm | com/alipay/sdk/app/PayTask.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://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 |
| 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 |
| 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 |
| http://ask.dcloud.net.cn/article/283 | io/dcloud/g/b.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 |
| https://ask.dcloud.net.cn/article/36199 | 摸瓜V1引擎 |
| http://dev.dcloud.net.cn/mui) | 摸瓜V2引擎 |
| http://a'); | 摸瓜V2引擎 |

### **4.3 邮箱线索**

### **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: False 找到 1 个唯一证书 主题: C=(ENY), ST=(Vt), L=(kRuxwWgSzTevcS), O=(camLmhYuyoIz), OU=(djZXPzsGXKrm), CN=(lZUdF) 签名算法: rsassa\_pkcs1v15 有效期自: 2025-06-16 02:49:04+00:00 有效期至: 2035-06-14 02:49:04+00:00 发行人: C=(ENY), ST=(Vt), L=(kRuxwWgSzTevcS), O=(camLmhYuyoIz), OU=(djZXPzsGXKrm), CN=(lZUdF) 序列号: 0x28b1e857 哈希算法: sha256 md5值: 0d452077695a3b1517c2482513bbdf7e sha1值: f6a63f8f58d219b81a6113faa639c25f2b0c2665 sha256值: a0447394157795beeec434a259d910693de0a1c246fcf5264e00025cdf4bc224 sha512值: cb64b31d3644542c17d843fcf58181f2f77a5105f29a2cc023c155189f0bafc1244b745bd9d19117f62995a3df14d2a2abda8169029d8c0dce80b4289db0d81d 公钥算法: rsa 密钥长度: 4096 指纹: e369e8e01c465780d120e819e17c5cc3ed5a6d9a4fe7cefc101fe45852d6cb18**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "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.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.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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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 |
| 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 |
| 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 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| io.dcloud.PandoraEntry | **Schemes**: h5f8c3dc7://, |

**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。**