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

**聚疆共创（ 2.3.2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 | 聚疆共创 |
| 版本 | 2.3.2 |
| 包名 | com.eipp.cuya.jxgcwin |
| 域名线索 | 0条 |
| URL线索 | 0条 |
| APP图标 |  |
| 分析日期 | 2025年6月25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 | JJGC\_20241003\_2.3.2.apk |
| 文件大小 | 43.77MB |
| MD5值 | 778130b0aca0c0e0e1af76cfe6506f8b |
| SHA1值 | 8ed0c5a79cb124aab69aad2bbd0df0f5594d4484 |
| SHA256值 | 6f276be076d3ad2c3da32cff9debf89cd9a9440940a12f670baf8044a7dc7327 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 聚疆共创 |
| 包名 | com.eipp.cuya.jxgcwin |
| 主活动Activity | com.poui.vctyp.newpack.ui.activity.SplashActivity |
| 安卓版本名称 | 2.3.2 |
| 安卓版本 | 52 |

## **4. 线索情况**

### **4.1 域名线索**

### **4.2 URL线索**

### **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=china, ST=xinjiang, L=wlmq, O=nodf, OU=jltec, CN=xj 签名算法: rsassa\_pkcs1v15 有效期自: 2024-08-31 10:58:59+00:00 有效期至: 2049-08-25 10:58:59+00:00 发行人: C=china, ST=xinjiang, L=wlmq, O=nodf, OU=jltec, CN=xj 序列号: 0x175244dc 哈希算法: sha256 md5值: bf69a8de9d3171aed53d372f5cf8828b sha1值: e9e13b7236f050b6f09a9b1fda81fc5bccb20d69 sha256值: 41410b51c85460ae1b6bfb78b28a3775148b672294fb3e05c68cad9dcc9f32fe sha512值: 31d42e8bea1e3bd73445ea5155a21fb98915aad5e779bf5aab9603b41207db54d775e0d96b16f32418801adc56197768699c69b4ab383edbeda09525b0b8fac3 公钥算法: rsa 密钥长度: 2048 指纹: 63d3c9f7380cfc554e4060f8174784623da91823e80136eb0b696594787ff543**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "anythink\_myoffer\_feedback\_violation\_of\_laws" : "Illegal"  |
| "kt\_auth" : "%1$s授权"  |
| "kt\_auth\_desc" : "完成%1$s授权后，购买或分享%1$s商品才可获得返佣"  |
| "kt\_desc\_auth\_account" : "点此授权账号"  |
| "kt\_please\_agree\_authentication\_agreement" : "请阅读并同意协议"  |
| "kt\_real\_name\_authentication\_agreement" : "我已阅读并同意《共享经济合作伙伴协议》"  |
| "kt\_sale\_goods\_user" : "带货用户"  |
| "kt\_share\_order\_password" : "【下单口令】"  |
| "kt\_tips\_authorize" : "点此授权账号"  |
| "kt\_to\_auth" : "前往%1$s授权"  |
| "anythink\_myoffer\_feedback\_violation\_of\_laws" : "违规违法"  |

## **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.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.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| 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.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\_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.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.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.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.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.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.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |
| com.eipp.cuya.jxgcwin.openadsdk.permission.TT\_PANGOLIN | 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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |

## **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。**