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

**花儿直播（ 1.0.8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 | 花儿直播 |
| 版本 | 1.0.8 |
| 包名 | com.d7fe2km.g2vq1mb2o |
| 域名线索 | 8条 |
| URL线索 | 9条 |
| APP图标 |  |
| 分析日期 | 2025年7月1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 | 1.apk |
| 文件大小 | 48.71MB |
| MD5值 | 7deafd6c10f4038139a0c50ae85e4427 |
| SHA1值 | 16da1e90cf6cbff1e1193e316230d71d30e43ba9 |
| SHA256值 | 86dad4299a9d08101d9d032a44ac89ab34bbb3580fd9baaf88af0e3c59c81181 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 花儿直播 |
| 包名 | com.d7fe2km.g2vq1mb2o |
| 主活动Activity | com.example.flutter\_live\_new.MainActivity |
| 安卓版本名称 | 1.0.8 |
| 安卓版本 | 2022120716 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| astat.bugly.cros.wr.pvp.net | IP: 170.106.135.32 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.jsdelivr.com | IP: 216.24.57.3 所属国家: United States of America 地区: California 城市: San Francisco  |
| astat.bugly.qcloud.com | IP: 150.109.27.253 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| developer.android.com | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| journeyapps.com | IP: 18.65.168.3 所属国家: United States of America 地区: Washington 城市: Seattle  |
| developer.mozilla.org | IP: 99.84.50.5 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| github.com | IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond  |
| android.bugly.qq.com | IP: 109.244.244.137 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://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/PlatformPlugin.java  |
| https://developer.android.com/reference/javax/net/ssl/SSLSocket  | io/flutter/plugins/videoplayer/VideoPlayerPlugin.java  |
| http://%s:%s  | com/ql/shield/ql\_shield\_plugin/QlShieldPlugin.java  |
| https://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| https://astat.bugly.qcloud.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/c.java  |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async  | com/tencent/bugly/crashreport/common/strategy/c.java  |
| https://journeyapps.com/  | Mogua Engine V1  |
| https://github.com/journeyapps/zxing-android-embedded  | Mogua Engine V1  |
| https://www.jsdelivr.com/using-sri-with-dynamic-files  | Mogua Engine V2  |
| https://github.com/apvarun/toastify-js  | Mogua Engine V2  |
| https://github.com/richtr/NoSleep.js/issues/15  | Mogua Engine V2  |
| https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)  | Mogua Engine V2  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| egw@3x.webp egx@3x.webp egy@3x.webp egz@3x.webp eh0@3x.webp eh1@3x.webp eh2@3x.webp eh3@3x.webp eh4@3x.webp eh5@3x.webp eh6@3x.webp eh7@3x.webp eh8@3x.webp eh9@3x.webp eh\_@3x.webp eha@3x.webp ehb@3x.webp ehc@3x.webp ehd@3x.webp ehe@3x.webp ehf@3x.webp ehg@3x.webp ehh@3x.webp ehi@3x.webp ehj@3x.webp ehk@3x.webp ehl@3x.webp ehm@3x.webp ehn@3x.webp eho@3x.webp ehp@3x.webp ehq@3x.webp ehr@3x.webp ehs@3x.webp eht@3x.webp ehu@3x.webp ehv@3x.webp ehw@3x.webp ehx@3x.webp ehy@3x.webp ehz@3x.webp ei0@3x.webp ei1@3x.webp ei2@3x.webp ei3@3x.webp ei4@3x.webp ei5@3x.webp ei6@3x.webp ei7@3x.webp ei8@3x.webp ei9@3x.webp ei\_@3x.webp eia@3x.webp eib@3x.webp eic@3x.webp eid@3x.webp eie@3x.webp eif@3x.webp eig@3x.webp eih@3x.webp eii@3x.webp eij@3x.webp eik@3x.webp eil@3x.webp eim@3x.webp ein@3x.webp eio@3x.webp eip@3x.webp eiq@3x.webp eir@3x.webp eis@3x.webp eit@3x.webp eiu@3x.webp eiv@3x.webp eiw@3x.webp eix@3x.webp eiy@3x.webp eiz@3x.webp ej0@3x.webp ej1@3x.webp ej2@3x.webp ej3@3x.webp ej4@3x.webp ej5@3x.webp ej6@3x.webp ej7@3x.webp ej8@3x.webp ej9@3x.webp ej\_@3x.webp eja@3x.webp ejb@3x.webp ejc@3x.webp ejd@3x.webp eje@3x.webp ejf@3x.webp ejg@3x.webp ejh@3x.webp eji@3x.webp ejj@3x.webp ejk@3x.webp ejl@3x.webp ejm@3x.webp ejn@3x.webp ejo@3x.webp ejp@3x.webp ejq@3x.webp ejr@3x.webp ejs@3x.webp ejt@3x.webp eju@3x.webp ejv@3x.webp ejw@3x.webp ejx@3x.webp ejy@3x.webp ejz@3x.webp ek0@3x.webp ek1@3x.webp ek2@3x.webp ek3@3x.webp ek4@3x.webp ek5@3x.webp ek6@3x.webp ek7@3x.webp ek8@3x.webp ek9@3x.webp ek\_@3x.webp eka@3x.webp ekb@3x.webp ekc@3x.webp ekd@3x.webp eke@3x.webp ekf@3x.webp ekg@3x.webp ekh@3x.webp eki@3x.webp ekj@3x.webp ekk@3x.webp ekl@3x.webp ekm@3x.webp ekn@3x.webp eko@3x.webp ekp@3x.webp fb9@3x.webp g\_9@3x.webp  | Mogua Engine V2  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.java  |

## **5. 签名证书**

**APK is signed v1 signature: True v2 signature: False v3 signature: False Found 1 unique certificates Subject: CN=xx.com, OU=dev, O=vihoo, L=SZ, ST=GD, C=CN Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2022-12-01 09:28:08+00:00 Valid To: 2050-04-18 09:28:08+00:00 Issuer: CN=xx.com, OU=dev, O=vihoo, L=SZ, ST=GD, C=CN Serial Number: 0x5c306e1c Hash Algorithm: sha256 md5: 9f2981df2d40f7aaba5ba67418016cb1 sha1: 935928edbebc021496162127a3f89d050a4b812a sha256: fd921809f37a1ec565bc4b615a2c774096a70aa8ca1816f596656bb972b8fff0 sha512: fb68a1d90de26c94b9c343e69b596b04a45c3a858177277c3d7d142c4d8ad030eb9c6275d49879f1fd595f9c4ccd698eed6637a0ca2df9d0147ba4695157c55d**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "library\_zxingandroidembedded\_author" : "JourneyApps"  |
| "library\_zxingandroidembedded\_authorWebsite" : "https://journeyapps.com/"  |

## **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.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.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.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\_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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.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.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.example.flutter\_live\_new.MainActivity | **Schemes**: rdmzgd9o://,  |

**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。**