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

**福满花牌（ 1.0.0060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 | 福满花牌 |
| 版本 | 1.0.0060 |
| 包名 | com.yoomeentbase.centerplldd |
| 域名线索 | 14条 |
| URL线索 | 17条 |
| APP图标 |  |
| 分析日期 | 2025年6月18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 | apply1747282272435.apk |
| 文件大小 | 76.36MB |
| MD5值 | 65867be7d8bc2f305ffdf95525400583 |
| SHA1值 | 8cbaeeaba175f653b0cd20c431406731a70f8a47 |
| SHA256值 | 5183d3f342010e947dc188f058ee43500680542f9c2ce38cbc65e2d2c38fcbd8 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 福满花牌 |
| 包名 | com.yoomeentbase.centerplldd |
| 主活动Activity | com.yoomeentbase.centerplldd.AppActivity |
| 安卓版本名称 | 1.0.0060 |
| 安卓版本 | 3 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| lbs.amap.com | IP: 110.253.189.212 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| abroad.apilocate.amap.com | IP: 59.82.44.11 所属国家: China 地区: Shanghai 城市: Shanghai  |
| dualstack-arestapi.amap.com | IP: 203.119.169.174 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| cgicol.amap.com | IP: 110.253.188.148 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| apilocate.amap.com | IP: 59.82.31.183 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| open.weixin.qq.com | IP: 116.128.171.214 所属国家: China 地区: Shanghai 城市: Shanghai  |
| long.open.weixin.qq.com | IP: 112.65.193.170 所属国家: China 地区: Shanghai 城市: Shanghai  |
| dualstack-a.apilocate.amap.com | IP: 59.82.31.183 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.apple.com | IP: 221.194.154.187 所属国家: China 地区: Hebei 城市: Langfang  |
| www.openssl.org | IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View  |
| adiu.amap.com | IP: 110.253.188.148 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| restapi.amap.com | IP: 203.119.169.174 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| restsdk.amap.com | IP: 106.11.43.113 所属国家: China 地区: Beijing 城市: Beijing  |
| mp.weixin.qq.com | IP: 140.207.121.14 所属国家: China 地区: Shanghai 城市: Shanghai  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://mp.weixin.qq.com/publicpoc/opensdkconf?action=GetShareConf&appid=%s&sdkVersion=%s&buffer=%s  | com/tencent/mm/opensdk/openapi/WXAPiSecurityHelper.java  |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s  | com/tencent/mm/opensdk/diffdev/a/c.java  |
| https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s  | com/tencent/mm/opensdk/diffdev/a/b.java  |
| http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&  | com/loc/dd.java  |
| https://adiu.amap.com/ws/device/adius  | com/loc/bn.java  |
| http://apilocate.amap.com/mobile/binary  | com/loc/fr.java  |
| http://dualstack-a.apilocate.amap.com/mobile/binary  | com/loc/fr.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/loc/fr.java  |
| https://restapi.amap.com/rest/aaid/get  | com/loc/af.java  |
| http://restapi.amap.com/rest/aaid/get  | com/loc/af.java  |
| http://restsdk.amap.com  | com/loc/v.java  |
| https://restsdk.amap.com/sdk/compliance/params  | com/loc/ax.java  |
| http://restsdk.amap.com/sdk/compliance/params  | com/loc/ax.java  |
| https://restsdk.amap.com/v3/iasdkauth  | com/loc/m.java  |
| https://dualstack-arestapi.amap.com/v3/iasdkauth  | com/loc/m.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/loc/fw.java  |
| http://dualstack-arestapi.amap.com/v3/geocode/regeo  | com/loc/fm.java  |
| http://restsdk.amap.com/v3/geocode/regeo  | com/loc/fm.java  |
| http://restsdk.amap.com/v3/place/text?  | com/loc/a.java  |
| http://restsdk.amap.com/v3/config/district?  | com/loc/a.java  |
| http://restsdk.amap.com/v3/place/around?  | com/loc/a.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/loc/fk.java  |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/  | com/amap/api/location/AMapLocation.java  |
| http://www.apple.com/DTDs/PropertyList-1.0.dtd  | lib/arm64-v8a/libcocos2dlua.so  |
| https://www.openssl.org/docs/faq.html  | lib/arm64-v8a/libcocos2dlua.so  |
| http://www.apple.com/DTDs/PropertyList-1.0.dtd  | lib/armeabi-v7a/libcocos2dlua.so  |
| https://www.openssl.org/docs/faq.html  | lib/armeabi-v7a/libcocos2dlua.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| cocos@cocoss-macbook-pro.local  | lib/arm64-v8a/libcocos2dlua.so  |
| cocos@cocoss-macbook-pro.local  | lib/armeabi-v7a/libcocos2dlua.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 14222222222  | com/loc/m.java  |

## **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=CH, ST=CH, L=CH, O=HH, OU=GG, CN=FF 签名算法: rsassa\_pkcs1v15 有效期自: 2023-06-09 02:48:02+00:00 有效期至: 2050-10-25 02:48:02+00:00 发行人: C=CH, ST=CH, L=CH, O=HH, OU=GG, CN=FF 序列号: 0x4d702c0b 哈希算法: sha256 md5值: a7d73c97a2c4ad424c663b142dafe831 sha1值: 1447fd7435d93840f7c6ba98065ebb29f48bd756 sha256值: fea6bfe66640b6ea84363cb8bb643a6957ff5de8ebe61c033df517e50f43efcc sha512值: 2858384b2b134defb7dae65290dc345ce8ce33b10fc92e268c824a162fefe7e6ca261b6da9507f749a6a6c481389ed2c9451a32d8caae1590bde70004f1f6c34 公钥算法: rsa 密钥长度: 4096 指纹: 1de929137f9d56cd4cf57d5480992560486e84ab0c8badf5287327d3546c167a**

## **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.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\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.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\_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\_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.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\_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\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 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。**