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

**汇德民生（ 1.1.3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 | 汇德民生 |
| 版本 | 1.1.3 |
| 包名 | lxpebnzln.dngysdq.octrsykxh |
| 域名线索 | 22条 |
| URL线索 | 19条 |
| APP图标 |  |
| 分析日期 | 2025年5月28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 | 汇德.apk |
| 文件大小 | 5.12MB |
| MD5值 | 0cf348cfce365f3ef961ccaebcea76d8 |
| SHA1值 | 1d7711d7f6c99dff1ebf298248ec54c442389ca1 |
| SHA256值 | 2697c6a579373d9ffe084312d32ddb6a363bb9956541912da22a73472a145970 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 汇德民生 |
| 包名 | lxpebnzln.dngysdq.octrsykxh |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 1.1.3 |
| 安卓版本 | 100 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| m3w.cn | IP: 116.196.151.14 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| bugs.webkit.org | IP: 17.33.194.218 所属国家: United States of America 地区: California 城市: Cupertino  |
| dev.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| jquery.org | IP: 104.17.176.200 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| bugzilla.mozilla.org | IP: 34.110.178.183 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| bugs.jquery.com | IP: 104.131.8.164 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| schemas.android.com | 没有服务器地理信息.  |
| ask.dcloud.net.cn | IP: 101.72.254.86 所属国家: China 地区: Hebei 城市: Langfang  |
| jquery.com | IP: 104.18.155.119 所属国家: United States of America 地区: California 城市: San Francisco  |
| ns.adobe.com | 没有服务器地理信息.  |
| sizzlejs.com | IP: 104.17.99.190 所属国家: United States of America 地区: California 城市: San Francisco  |
| er.dcloud.net.cn | IP: 43.142.57.168 所属国家: China 地区: Beijing 城市: Beijing  |
| jsperf.com | IP: 104.16.228.18 所属国家: United States of America 地区: California 城市: San Francisco  |
| er.dcloud.io | 没有服务器地理信息.  |
| dev.dcloud.net.cn | IP: 124.163.195.89 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| m.chinaz.com | IP: 111.161.122.153 所属国家: China 地区: Tianjin 城市: Tianjin  |
| msdn.microsoft.com | IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond  |
| db.panzh.icu | IP: 0.0.0.0 所属国家: - 地区: - 城市: -  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| blindsignals.com | IP: 103.224.182.247 所属国家: Australia 地区: Victoria 城市: Beaumaris  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://ns.adobe.com/xap/1.0/\u0000  | io/dcloud/common/util/ExifInterface.java  |
| https://m3w.cn/s/  | io/dcloud/common/util/ShortCutUtil.java  |
| https://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/p/r.java  |
| https://ask.dcloud.net.cn/article/35877  | io/dcloud/p/r.java  |
| https://ask.dcloud.net.cn/article/283  | io/dcloud/p/h1.java  |
| https://er.dcloud.io/rv  | io/dcloud/p/d0.java  |
| https://er.dcloud.net.cn/rv  | io/dcloud/p/d0.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://db.panzh.icu/zyd  | 摸瓜V2引擎  |
| http://jquery.com/  | 摸瓜V2引擎  |
| http://sizzlejs.com/  | 摸瓜V2引擎  |
| http://jquery.org/license  | 摸瓜V2引擎  |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=814622  | 摸瓜V2引擎  |
| http://bugs.jquery.com/ticket/13378  | 摸瓜V2引擎  |
| http://bugs.jquery.com/ticket/12359  | 摸瓜V2引擎  |
| https://github.com/jquery/sizzle/pull/225  | 摸瓜V2引擎  |
| http://msdn.microsoft.com/en-us/library/ms536429%28VS.85%29.aspx  | 摸瓜V2引擎  |
| http://bugs.jquery.com/ticket/12282  | 摸瓜V2引擎  |
| http://jsperf.com/getall-vs-sizzle/2  | 摸瓜V2引擎  |
| https://developer.mozilla.org/en-US/docs/CSS/display  | 摸瓜V2引擎  |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=649285  | 摸瓜V2引擎  |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=491668  | 摸瓜V2引擎  |
| http://blindsignals.com/index.php/2009/07/jquery-delay/  | 摸瓜V2引擎  |
| https://bugs.webkit.org/show\_bug.cgi?id=29084  | 摸瓜V2引擎  |
| https://github.com/jquery/jquery/pull/764  | 摸瓜V2引擎  |
| https://github.com/jquery/jquery/pull/557)  | 摸瓜V2引擎  |
| http://dev.dcloud.net.cn/mui)  | 摸瓜V2引擎  |
| https://m.chinaz.com/  | 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: True 找到 1 个唯一证书 主题: C=beijing, ST=beijing, L=beijing, O=li1743562220267, OU=xs1743562220267, CN=rryf 签名算法: rsassa\_pkcs1v15 有效期自: 2025-04-02 02:50:25+00:00 有效期至: 2075-03-21 02:50:25+00:00 发行人: C=beijing, ST=beijing, L=beijing, O=li1743562220267, OU=xs1743562220267, CN=rryf 序列号: 0x402e0194 哈希算法: sha512 md5值: 6e4dc3a9790fe0d72d83174d5ccd340f sha1值: f2adbafe75665a24a354cb3a118fa187e90ecb48 sha256值: 08d445595aecadf45c7dd4198cdfcfe017512f59cb027590dc48e752d64430e2 sha512值: 3aed5ea55933c614cd916aba43fe68ae2710217df11b2cf25517f8c0ae8efa4a3c29a361b81dbf2cb34bf63e361927ac6827e401d606d90740b3b4f7ce10157c 公钥算法: rsa 密钥长度: 4096 指纹: 43149c80221d5a85f278b6bf5345da9bce575e27ede9feeb4e1044916cc969dd**

## **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\_feature\_confusion\_exception\_no\_private\_key\_input" : "no private key input"  |
| "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\_tips\_certificate" : "certificate"  |
| "dcloud\_common\_user\_refuse\_api" : "用户拒绝该API访问"  |
| "dcloud\_feature\_confusion\_exception\_no\_private\_key\_input" : "私钥数据为空"  |
| "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"  |
| "dcloud\_tips\_certificate" : "证书"  |

## **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.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\_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 |
| 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.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 |
| 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。 |
| lxpebnzln.dngysdq.octrsykxh\_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 |
| 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 |
| lxpebnzln.dngysdq.octrsykxh\_com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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.MODIFY\_AUDIO\_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| 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.READ\_LOGS | 危险 | 读取敏感日志数据 | 允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.RECEIVE\_SMS | 危险 | 接收短信 | 允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示 |
| android.permission.SEND\_SMS | 危险 | 发送短信 | 允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价 |
| android.permission.WRITE\_SMS | 危险 | 编辑短信或彩信 | 允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息 |
| android.permission.READ\_SMS | 危险 | 阅读短信或彩信 | 允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| io.dcloud.PandoraEntry | **Schemes**: h517d660f://,  |

**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。**