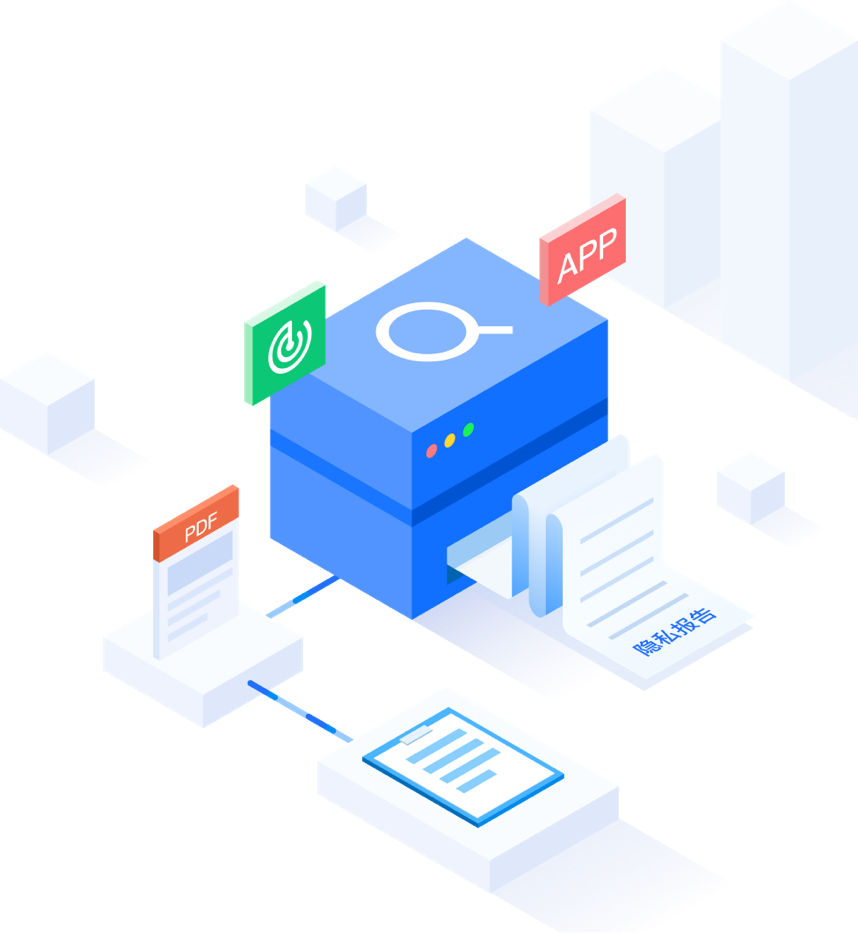
小米移动应用隐私

合规检测报告



目录

[1 评估总体情况 3](#_Toc256000001)

[1.1 检测依据 3](#_Toc256000002)

[1.2 应用基本信息 3](#_Toc256000003)

[1.3 检测环境 4](#_Toc256000004)

[1.4 总体评估结论 4](#_Toc256000005)

[2 《关于开展纵深推进APP侵害用户权益专项整治行动的通知》（164号文）检测 5](#_Toc256000006)

[2.1 评估结论 5](#_Toc256000007)

[2.2 评估明细 6](#_Toc256000008)

[2.2.1 违规收集个人信息（存在风险） 6](#_Toc256000009)

[3 检测详情 18](#_Toc256000010)

[3.1 权限使用情况 18](#_Toc256000011)

[3.1.1 声明权限 18](#_Toc256000012)

[3.1.2 尝试使用未声明权限 22](#_Toc256000013)

[3.1.3 权限过度申请 22](#_Toc256000014)

[3.2 应用行为分析 26](#_Toc256000015)

[3.3 通信行为分析 27](#_Toc256000016)

[3.4 传输个人信息 33](#_Toc256000017)

[3.5 存储个人信息 33](#_Toc256000018)

[3.6 个人信息风险漏洞 33](#_Toc256000019)

[3.6.1 Java代码反编译风险检测 34](#_Toc256000020)

[3.6.2 资源文件泄露风险检测 34](#_Toc256000021)

[3.6.3 访问境外服务器风险检测 42](#_Toc256000022)

[3.6.4 SSL证书有效性风险检测 43](#_Toc256000023)

[3.6.5 HTTP传输通道风险检测 44](#_Toc256000024)

[3.6.6 启用VPN服务检测 45](#_Toc256000025)

[3.6.7 密钥硬编码风险检测 46](#_Toc256000026)

[3.6.8 WebView明文存储密码风险检测 46](#_Toc256000027)

[3.6.9 输入监听风险检测 47](#_Toc256000028)

[附件一：Android涉及个人信息权限 48](#_Toc256000029)

[附件二：个人信息 55](#_Toc256000030)

[附件三：个人敏感信息 57](#_Toc256000031)

# 评估总体情况

## 检测依据

1、全国人大常委会《中华人民共和国网络安全法》

2、全国人大常委会《个人信息保护法》

3、全国信息安全标准化技术委员会《网络安全标准实践指南—移动互联网应用程序（App）个人信息保护常见问题及处置指南》

4、全国信息安全标准化技术委员会《移动互联网应用程序（APP）系统权限申请使用指南》

5、APP专项治理工作组《App申请安卓系统权限机制分析与建议》

6、工业和信息化部《关于开展纵深推进APP侵害用户权益专项整治行动的通知》（工信部信管函〔2020〕164号）

7、四部委《App违法违规收集使用个人信息行为认定方法》（国信办秘字〔2019〕191号）

## **应用基本信息**

|  |  |
| --- | --- |
| **APP名称** | 酒仙 |
| **版本号** | 9.1.19 |
| **文件大小** | 125.93MB |
| **包名** | com.jiuxianapk.ui |
| **文件MD5** | 0B66B5FEFAB1009D610CA3C732CBBDCF |
| **签名证书** | 所有者:CN=jiuxian, OU=jiuxian, O=jiuxian, L=beijing, ST=beijing, C=china 发布者:CN=jiuxian, OU=jiuxian, O=jiuxian, L=beijing, ST=beijing, C=china |
| **minSdkVersion** | 21 |
| **targetSdkVersion** | 30 |
| **是否加固** | 否 |
| **评估单位** | 小米安全、爱加密联合评估 |
| **评估时间** | 2024-01-11 14:37:23 |
| **检测时长** | 26分0秒 |

## **检测环境**

|  |  |
| --- | --- |
| **测试手机品牌** | - |
| **测试手机型号** | - |
| **测试手机操作系统版本** | Android8.1 |

## 总体评估结论

|  |  |  |  |
| --- | --- | --- | --- |
| **检测内容** | **总体结论** | **发现风险项** | **未发现风险项** |
| 工业和信息化部《关于开展纵深推进APP侵害用户权益专项整治行动的通知》下文简称（工信部信管函〔2020〕164号） | **存在风险** | **2** | 0 |

# 《关于开展纵深推进APP侵害用户权益专项整治行动的通知》（164号文）检测

## 评估结论

根据《工业和信息化部关于开展纵深推进APP侵害用户权益专项整治行动的通知》（《工信部信管函[2020]164号》）中3大项检测项，30个检测细项进行评估，其中评估未发现风险0项，评估发现风险2项。自行评估检测项为2大项。

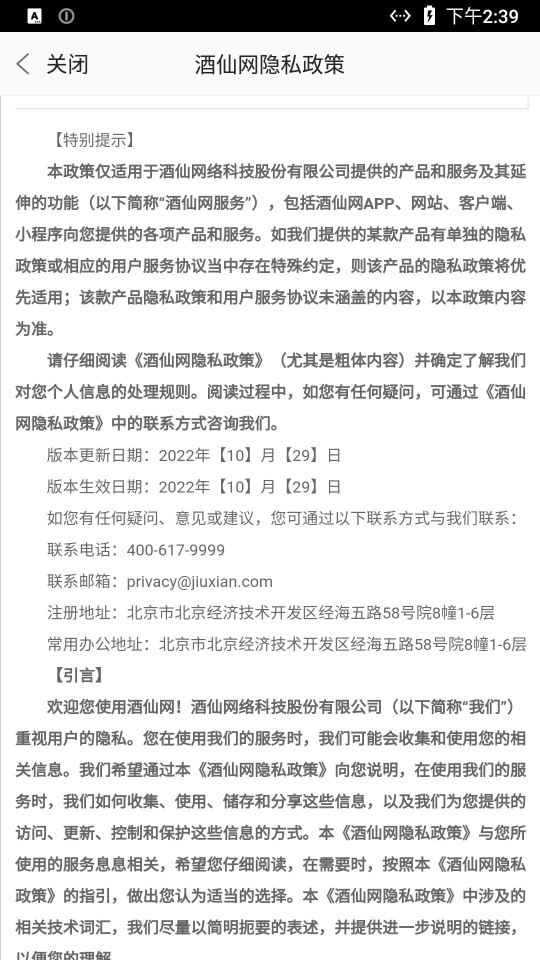
|  |  |  |
| --- | --- | --- |
| **序号** | **应用问题** | **问题描述** |
| 1 | [违规收集个人信息。重点整治APP、SDK未告知用户收集个人信息的目的、方式、范围且未经用户同意，私自收集用户个人信息的行为。](#_违规收集个人信息（存在风险）) | 1、APP以隐私政策弹窗的形式向用户明示收集使用规则，但未见清晰明示APP收集SD卡数据等的目的方式范围，用户同意隐私政策后，存在收集SD卡数据的行为。  2、APP向用户明示SDK的收集使用规则，但未见清晰明示腾讯SDK获取SD卡数据、腾讯Web浏览器框架,腾讯TBS浏览服务获取SD卡数据等的目的方式范围，用户同意隐私政策后，SDK存在腾讯SDK获取SD卡数据、腾讯Web浏览器框架,腾讯TBS浏览服务获取SD卡数据的行为。 |

## 评估明细

### 违规收集个人信息（存在风险）

#### 场景1：APP以隐私政策弹窗的形式向用户明示收集使用规则，但未见清晰明示APP收集SD卡数据等的目的方式范围，用户同意隐私政策后，存在收集SD卡数据的行为。（存在风险）

**截图凭证：**



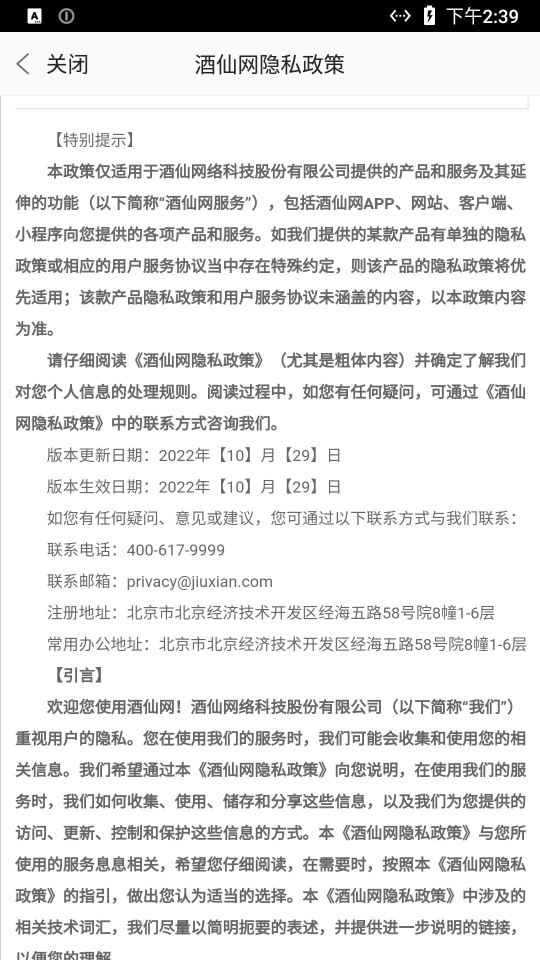
**整改建议：**建议在隐私政策中清晰明示APP收集设备MAC地址、软件安装列表等的目的方式范围，不要使用“等”等模糊或者有多意性的表述。

**个人信息行为**：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **行为阶段** | **主体类型** | **主体名称** | **行为名称** | **权限名称** | **触发频次（次/秒）** | **是否有相关隐私文本** |
| 前台行为 | SDK | 腾讯Web浏览器框架,腾讯TBS浏览服务 | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **8** | 否 |
| 前台行为 | SDK | 腾讯Web浏览器框架,腾讯TBS浏览服务 | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **1** | 否 |
| 前台行为 | SDK | 腾讯Web浏览器框架,腾讯TBS浏览服务 | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **2** | 否 |
| 前台行为 | SDK | 腾讯Web浏览器框架,腾讯TBS浏览服务 | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **16** | 否 |
| 前台行为 | SDK | 腾讯Web浏览器框架,腾讯TBS浏览服务 | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **8** | 否 |
| 前台行为 | SDK | 腾讯Web浏览器框架,腾讯TBS浏览服务 | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **1** | 否 |
| 前台行为 | SDK | 腾讯Web浏览器框架,腾讯TBS浏览服务 | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **2** | 否 |
| 前台行为 | SDK | 腾讯Web浏览器框架,腾讯TBS浏览服务 | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **1** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **4** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **2** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **2** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **2** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **2** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **2** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **1** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **1** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **1** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **1** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **1** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **1** | 否 |

#### 场景2：APP向用户明示SDK的收集使用规则，但未见清晰明示腾讯SDK获取SD卡数据、腾讯Web浏览器框架,腾讯TBS浏览服务获取SD卡数据等的目的方式范围，用户同意隐私政策后，SDK存在腾讯SDK获取SD卡数据、腾讯Web浏览器框架,腾讯TBS浏览服务获取SD卡数据的行为。（存在风险）

**截图凭证：**



**整改建议：**建议在隐私政策中清晰明示各个SDK收集设备MAC地址、软件安装列表等的目的方式范围。不要使用“等”等模糊或者有多意性的表述

**个人信息行为**：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **行为阶段** | **主体类型** | **主体名称** | **行为名称** | **权限名称** | **触发频次（次/秒）** | **是否有相关隐私文本** |
| 前台行为 | SDK | 腾讯Web浏览器框架,腾讯TBS浏览服务 | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **8** | 否 |
| 前台行为 | SDK | 腾讯Web浏览器框架,腾讯TBS浏览服务 | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **1** | 否 |
| 前台行为 | SDK | 腾讯Web浏览器框架,腾讯TBS浏览服务 | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **2** | 否 |
| 前台行为 | SDK | 腾讯Web浏览器框架,腾讯TBS浏览服务 | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **16** | 否 |
| 前台行为 | SDK | 腾讯Web浏览器框架,腾讯TBS浏览服务 | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **8** | 否 |
| 前台行为 | SDK | 腾讯Web浏览器框架,腾讯TBS浏览服务 | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **1** | 否 |
| 前台行为 | SDK | 腾讯Web浏览器框架,腾讯TBS浏览服务 | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **2** | 否 |
| 前台行为 | SDK | 腾讯Web浏览器框架,腾讯TBS浏览服务 | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **1** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **4** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **2** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **2** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **2** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **2** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **2** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **1** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **1** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **1** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **1** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **1** | 否 |
| 前台行为 | SDK | 腾讯SDK | 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **1** | 否 |

# **检测详情**

## 权限使用情况

### 声明权限

本应用共声明了以下45项权限，其中敏感等级为敏感的权限有25项，与个人信息相关的权限有10项，在前台运行行为阶段过程中，已使用的权限有3项：

注：如需查看其他行为阶段的详细数据，请下载《酒仙\_9.1.19\_行为数据》文档。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **权限名称** | **权限描述** | **Protection Level** | **敏感等级** | **个人信息相关系统权限** | **是否使用** |
| WRITE\_EXTERNAL\_STORAGE | 写入外部存储 | dangerous | 敏感 | 是 | 是 |
| READ\_PHONE\_STATE | 读取手机状态 | dangerous | 敏感 | 是 | 是 |
| READ\_CONTACTS | 读取通讯录 | dangerous | 敏感 | 是 | 否 |
| GET\_ACCOUNTS | 访问账户服务中的账户列表 | dangerous | 敏感 | 是 | 否 |
| ACCESS\_FINE\_LOCATION | 获取精确位置 | dangerous | 敏感 | 是 | 否 |
| ACCESS\_COARSE\_LOCATION | 访问近似位置 | dangerous | 敏感 | 是 | 否 |
| RECORD\_AUDIO | 录音 | dangerous | 敏感 | 是 | 否 |
| GET\_TASKS | 获取任务信息 | -- | 敏感 | 是 | 否 |
| CAMERA | 使用照相设备 | dangerous | 敏感 | 是 | 否 |
| READ\_EXTERNAL\_STORAGE | 读取外部存储 | dangerous | 敏感 | 是 | 否 |
| READ\_LOGS | 读取系统日志 | 不允许第三方应用使用 | 敏感 | 否 | 否 |
| AD\_ID | 自定义权限 |  | 敏感 | 否 | 否 |
| SYSTEM\_ALERT\_WINDOW | 显示系统窗口 | signature|preinstalled|appop|pre23|development | 敏感 | 否 | 否 |
| BADGE\_ICON | 自定义权限 |  | 敏感 | 否 | 否 |
| POST\_NOTIFICATIONS | 自定义权限 |  | 敏感 | 否 | 否 |
| READ\_SETTINGS | 自定义权限 |  | 敏感 | 否 | 否 |
| QUERY\_ALL\_PACKAGES | 自定义权限 |  | 敏感 | 否 | 否 |
| CHANGE\_BADGE | 华为自定义权限 |  | 敏感 | 否 | 否 |
| SMARTCARD | 自定义权限 |  | 敏感 | 否 | 否 |
| REQUEST\_INSTALL\_PACKAGES | 安装应用程序 | signature | 敏感 | 否 | 否 |
| KILL\_BACKGROUND\_PROCESSES | 结束后台进程 | normal | 敏感 | 否 | 否 |
| RESTART\_PACKAGES | 重新启动其他程序 | -- | 敏感 | 否 | 否 |
| CHANGE\_WIFI\_STATE | 改变WiFi连接状态 | normal | 敏感 | 否 | 否 |
| BLUETOOTH | 使用蓝牙 | normal | 敏感 | 否 | 否 |
| WRITE\_SETTINGS | 读写系统设置 | signature|preinstalled|appop|pre23 | 敏感 | 否 | 否 |
| ACCESS\_WIFI\_STATE | 访问Wi-Fi网络信息 | normal | 正常 | 否 | 是 |
| FLASHLIGHT | 使用闪光灯 |  | 正常 | 否 | 否 |
| BROADCAST\_PACKAGE\_CHANGED | 接收apk包改变的广播 |  | 正常 | 否 | 否 |
| BROADCAST\_PACKAGE\_INSTALL | 接收apk包安装的广播 |  | 正常 | 否 | 否 |
| FOREGROUND\_SERVICE | 常规应用使用前台服务 | normal | 正常 | 否 | 否 |
| RECEIVE\_USER\_PRESENT | 接收当用户出现即屏幕点亮的广播 |  | 正常 | 否 | 否 |
| RECEIVE\_BOOT\_COMPLETED | 接收开机完成事件 | normal | 正常 | 否 | 否 |
| NFC | 允许NFC通讯 | normal | 正常 | 否 | 否 |
| ACCESS\_NOTIFICATION\_POLICY | 访问通知策略 | normal | 正常 | 否 | 否 |
| ACCESS\_NETWORK\_STATE | 访问网络信息 | normal | 正常 | 否 | 否 |
| WAKE\_LOCK | 唤醒锁定 | normal | 正常 | 否 | 否 |
| VIBRATE | 访问振动设备 | normal | 正常 | 否 | 否 |
| BROADCAST\_PACKAGE\_REPLACED | 接收apk包替换的广播 |  | 正常 | 否 | 否 |
| REORDER\_TASKS | 排序系统任务 | normal | 正常 | 否 | 否 |
| MOUNT\_UNMOUNT\_FILESYSTEMS | 挂载或者反挂载外置sdcard的文件系统 | 不允许第三方应用使用 | 正常 | 否 | 否 |
| BROADCAST\_PACKAGE\_ADDED | 接收apk包增加的广播 |  | 正常 | 否 | 否 |
| INTERNET | 访问网络 | normal | 正常 | 否 | 否 |
| CHANGE\_NETWORK\_STATE | 改变网络状态 | normal | 正常 | 否 | 否 |
| MODIFY\_AUDIO\_SETTINGS | 修改音频设置 | normal | 正常 | 否 | 否 |
| ACCESS\_LOCATION\_EXTRA\_COMMANDS | 访问额外的定位服务 | normal | 正常 | 否 | 否 |

### 尝试使用未声明权限

本应用在前台运行行为阶段过程中，尝试使用未声明了以下0项权限，其中敏感等级为敏感的权限有0项，与个人信息相关的权限有0项：

注：如需查看其他行为阶段的详细数据，请下载《酒仙\_9.1.19\_行为数据》文档。

### 权限过度申请

本应用权限过度申请了以下45项权限，其中敏感等级为敏感的权限有25项，与个人信息相关的权限有10项，在前台运行行为阶段过程中，已使用的权限有3项：

注：如需查看其他行为阶段的详细数据，请下载《酒仙\_9.1.19\_行为数据》文档。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **权限名称** | **权限描述** | **敏感等级** | **个人信息相关系统权限** | **APP次数** | **SDK次数** |
| READ\_CONTACTS | 读取通讯录 | 敏感 | 是 | 未使用 | 未使用 |
| READ\_LOGS | 读取系统日志 | 敏感 | 否 | 未使用 | 未使用 |
| AD\_ID | 自定义权限 | 敏感 | 否 | 未使用 | 未使用 |
| GET\_ACCOUNTS | 访问账户服务中的账户列表 | 敏感 | 是 | 未使用 | 未使用 |
| FLASHLIGHT | 使用闪光灯 | 正常 | 否 | 未使用 | 未使用 |
| BROADCAST\_PACKAGE\_CHANGED | 接收apk包改变的广播 | 正常 | 否 | 未使用 | 未使用 |
| BROADCAST\_PACKAGE\_INSTALL | 接收apk包安装的广播 | 正常 | 否 | 未使用 | 未使用 |
| FOREGROUND\_SERVICE | 常规应用使用前台服务 | 正常 | 否 | 未使用 | 未使用 |
| RECEIVE\_USER\_PRESENT | 接收当用户出现即屏幕点亮的广播 | 正常 | 否 | 未使用 | 未使用 |
| SYSTEM\_ALERT\_WINDOW | 显示系统窗口 | 敏感 | 否 | 未使用 | 未使用 |
| RECEIVE\_BOOT\_COMPLETED | 接收开机完成事件 | 正常 | 否 | 未使用 | 未使用 |
| NFC | 允许NFC通讯 | 正常 | 否 | 未使用 | 未使用 |
| WRITE\_EXTERNAL\_STORAGE | 写入外部存储 | 敏感 | 是 | 未使用 | 59 |
| ACCESS\_FINE\_LOCATION | 获取精确位置 | 敏感 | 是 | 未使用 | 未使用 |
| ACCESS\_NOTIFICATION\_POLICY | 访问通知策略 | 正常 | 否 | 未使用 | 未使用 |
| ACCESS\_COARSE\_LOCATION | 访问近似位置 | 敏感 | 是 | 未使用 | 未使用 |
| BADGE\_ICON | 自定义权限 | 敏感 | 否 | 未使用 | 未使用 |
| ACCESS\_NETWORK\_STATE | 访问网络信息 | 正常 | 否 | 未使用 | 未使用 |
| WAKE\_LOCK | 唤醒锁定 | 正常 | 否 | 未使用 | 未使用 |
| ACCESS\_WIFI\_STATE | 访问Wi-Fi网络信息 | 正常 | 否 | 2 | 7 |
| POST\_NOTIFICATIONS | 自定义权限 | 敏感 | 否 | 未使用 | 未使用 |
| READ\_SETTINGS | 自定义权限 | 敏感 | 否 | 未使用 | 未使用 |
| QUERY\_ALL\_PACKAGES | 自定义权限 | 敏感 | 否 | 未使用 | 未使用 |
| VIBRATE | 访问振动设备 | 正常 | 否 | 未使用 | 未使用 |
| BROADCAST\_PACKAGE\_REPLACED | 接收apk包替换的广播 | 正常 | 否 | 未使用 | 未使用 |
| REORDER\_TASKS | 排序系统任务 | 正常 | 否 | 未使用 | 未使用 |
| CHANGE\_BADGE | 华为自定义权限 | 敏感 | 否 | 未使用 | 未使用 |
| SMARTCARD | 自定义权限 | 敏感 | 否 | 未使用 | 未使用 |
| MOUNT\_UNMOUNT\_FILESYSTEMS | 挂载或者反挂载外置sdcard的文件系统 | 正常 | 否 | 未使用 | 未使用 |
| RECORD\_AUDIO | 录音 | 敏感 | 是 | 未使用 | 未使用 |
| REQUEST\_INSTALL\_PACKAGES | 安装应用程序 | 敏感 | 否 | 未使用 | 未使用 |
| BROADCAST\_PACKAGE\_ADDED | 接收apk包增加的广播 | 正常 | 否 | 未使用 | 未使用 |
| KILL\_BACKGROUND\_PROCESSES | 结束后台进程 | 敏感 | 否 | 未使用 | 未使用 |
| RESTART\_PACKAGES | 重新启动其他程序 | 敏感 | 否 | 未使用 | 未使用 |
| CHANGE\_WIFI\_STATE | 改变WiFi连接状态 | 敏感 | 否 | 未使用 | 未使用 |
| INTERNET | 访问网络 | 正常 | 否 | 未使用 | 未使用 |
| GET\_TASKS | 获取任务信息 | 敏感 | 是 | 未使用 | 未使用 |
| CHANGE\_NETWORK\_STATE | 改变网络状态 | 正常 | 否 | 未使用 | 未使用 |
| CAMERA | 使用照相设备 | 敏感 | 是 | 未使用 | 未使用 |
| MODIFY\_AUDIO\_SETTINGS | 修改音频设置 | 正常 | 否 | 未使用 | 未使用 |
| READ\_EXTERNAL\_STORAGE | 读取外部存储 | 敏感 | 是 | 未使用 | 未使用 |
| BLUETOOTH | 使用蓝牙 | 敏感 | 否 | 未使用 | 未使用 |
| READ\_PHONE\_STATE | 读取手机状态 | 敏感 | 是 | 未使用 | 26 |
| WRITE\_SETTINGS | 读写系统设置 | 敏感 | 否 | 未使用 | 未使用 |
| ACCESS\_LOCATION\_EXTRA\_COMMANDS | 访问额外的定位服务 | 正常 | 否 | 未使用 | 未使用 |

## 应用行为分析

本应用在运行过程中，隐私政策授权前行为出现0种行为，前台运行行为出现10种行为，后台运行行为出现0种行为，应用退出行为出现0种行为：

注：如需查看详细行为数据，请下载《酒仙\_9.1.19\_行为数据》文档。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **行为描述** | **行为权限** | **个人信息相关行为** | **APP次数** | **SDK次数** |
| **隐私政策授权前行为** | | | | |
| 暂无数据 | | | | |
| **前台运行行为** | | | | |
| 获取设备IMEI | READ\_PHONE\_STATE | **是** | 未使用 | 20 |
| 获取设备IMSI | READ\_PHONE\_STATE | **是** | 未使用 | 6 |
| 获取SIM服务商信息 |  | **是** | 未使用 | 68 |
| 获取设备传感器 |  | **否** | 未使用 | 1 |
| 获取MAC地址 |  | **是** | 未使用 | 5 |
| 获取WIFI名称 | ACCESS\_WIFI\_STATE | **否** | 2 | 4 |
| 尝试获取BSSID(WIFI的MAC地址) | ACCESS\_WIFI\_STATE | **否** | 未使用 | 3 |
| 获取AndroidID |  | **是** | 未使用 | 6 |
| 获取已安装的应用 |  | **是** | 未使用 | 1 |
| 尝试写入SDCard数据(创建) | WRITE\_EXTERNAL\_STORAGE | **是** | 未使用 | 59 |
| **后台运行行为** | | | | |
| 暂无数据 | | | | |
| **应用退出行为** | | | | |
| 暂无数据 | | | | |

## 通信行为分析

本应用在前台运行行为阶段过程中，访问了以下56个IP地址，其中境外IP有0个，境内IP有56个：

注：如需查看其他行为阶段的详细数据，请下载《酒仙\_9.1.19\_行为数据》文档。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **境外IP** | | | | |
| **序号** | **IP** | **域名** | **地址** | **通信次数** |
| 暂无数据 | | | | |
| **境内IP** | | | | |
| **序号** | **IP** | **域名** | **地址** | **通信次数** |
| 1 | 61.180.32.155 | img09.jiuxian.com | 中国 江西省 景德镇市 电信 | 56 |
| 2 | 101.36.158.20 | shu.jiuxian.com | 中国 北京 北京市 电信 | 50 |
| 3 | 101.36.158.20 | pintuan.jiuxian.com | 中国 北京 北京市 电信 | 40 |
| 4 | 49.71.75.195 | img07.jiuxian.com | 中国 江苏省 扬州市 电信 | 22 |
| 5 | 49.71.75.195 | img10.jiuxian.com | 中国 江苏省 扬州市 电信 | 22 |
| 6 | 59.63.81.65 | misc.jiuxian.com | 中国 江西省 景德镇市 电信 | 19 |
| 7 | 101.36.158.20 | newapphome.jiuxian.com | 中国 北京 北京市 电信 | 18 |
| 8 | 113.219.132.16 | img08.jiuxian.com | 中国 湖南省 衡阳市 电信 | 14 |
| 9 | 61.147.210.155 | m.jiuxian.com | 中国 江苏省 南通市 电信 | 13 |
| 10 | 49.71.75.195 | misc.jiuxian.com | 中国 江苏省 扬州市 电信 | 7 |
| 11 | 101.36.158.56 | dljx.jxwmanage.com | 中国 北京 北京市 电信 | 7 |
| 12 | 115.227.12.25 | log.tbs.qq.com | 中国 浙江省 杭州市 电信 | 7 |
| 13 | 223.109.148.178 | ulogs.umeng.com | 中国 江苏省 移动 | 7 |
| 14 | 223.109.148.141 | ulogs.umeng.com | 中国 江苏省 移动 | 6 |
| 15 | 47.102.14.9 | s.oadz.com | 中国 上海 上海市 阿里云 | 5 |
| 16 | 113.219.132.16 | img06.jiuxian.com | 中国 湖南省 衡阳市 电信 | 5 |
| 17 | 113.219.132.24 | img09.jiuxian.com | 中国 湖南省 衡阳市 电信 | 5 |
| 18 | 49.71.75.195 | img08.jiuxian.com | 中国 江苏省 扬州市 电信 | 4 |
| 19 | 58.49.216.78 | -- | 中国 湖北省 武汉市 电信 | 4 |
| 20 | 101.36.158.20 | newappuser.jiuxian.com | 中国 北京 北京市 电信 | 4 |
| 21 | 101.36.158.56 | trailjx.jxwmanage.com | 中国 北京 北京市 电信 | 4 |
| 22 | 58.49.216.170 | log.tbs.qq.com | 中国 湖北省 武汉市 电信 | 4 |
| 23 | 58.220.63.20 | img06.jiuxian.com | 中国 江苏省 扬州市 电信 | 3 |
| 24 | 59.82.112.112 | log.umsns.com | 中国 北京 北京市 阿里巴巴 | 3 |
| 25 | 59.82.121.179 | eco.taobao.com | 中国 北京 北京市 阿里巴巴 | 3 |
| 26 | 111.170.15.148 | m.jiuxian.com | 中国 湖北省 襄阳 电信 | 3 |
| 27 | 113.219.132.24 | shop.jiuxian.com | 中国 湖南省 衡阳市 电信 | 3 |
| 28 | 113.219.132.24 | img07.jiuxian.com | 中国 湖南省 衡阳市 电信 | 3 |
| 29 | 110.253.189.208 | -- | 中国 河北省 张家口市 联通 | 3 |
| 30 | 223.109.148.177 | ulogs.umeng.com | 中国 江苏省 移动 | 3 |
| 31 | 42.81.219.31 | newappproduct.jiuxian.com | 中国 天津 天津市 电信 | 2 |
| 32 | 59.63.226.81 | newapprproduct.jiuxian.com | 中国 江西省 南昌市 电信 | 2 |
| 33 | 218.91.197.67 | utoken.umeng.com | 中国 江苏省 南通市 电信 | 2 |
| 34 | 42.81.183.202 | cfg.imtt.qq.com | 中国 天津 天津市 电信 | 2 |
| 35 | 113.219.132.16 | shop.jiuxian.com | 中国 湖南省 衡阳市 电信 | 2 |
| 36 | 113.219.132.24 | img10.jiuxian.com | 中国 湖南省 衡阳市 电信 | 2 |
| 37 | 36.143.252.112 | -- | 中国 移动 | 2 |
| 38 | 59.82.31.92 | offmsg.umeng.com | 中国 北京 北京市 阿里巴巴 | 1 |
| 39 | 36.99.183.90 | tbs.sjy.tcdnos.com | 中国 河南省 郑州市 电信 | 1 |
| 40 | 42.81.178.46 | cgi.connect.qq.com | 中国 天津 天津市 电信 | 1 |
| 41 | 42.81.219.80 | newapprproduct.jiuxian.com | 中国 天津 天津市 电信 | 1 |
| 42 | 59.82.31.154 | offmsg.umeng.com | 中国 北京 北京市 阿里巴巴 | 1 |
| 43 | 59.82.31.160 | deeplink.umeng.com | 中国 北京 北京市 阿里巴巴 | 1 |
| 44 | 59.82.31.210 | log.umsns.com | 中国 北京 北京市 阿里巴巴 | 1 |
| 45 | 101.36.158.20 | newappcart.jiuxian.com | 中国 北京 北京市 电信 | 1 |
| 46 | 101.36.158.56 | downtjx.jxwmanage.com | 中国 北京 北京市 电信 | 1 |
| 47 | 106.11.61.137 | -- | 中国 上海 上海市 阿里巴巴 | 1 |
| 48 | 110.242.48.56 | misc-pili-qos-report.qiniuapi.com | 中国 河北省 保定市 联通 | 1 |
| 49 | 180.102.49.73 | pingma.qq.com:80 | 中国 江苏省 南京市 电信 | 1 |
| 50 | 36.143.252.40 | audid.umeng.com | 中国 移动 | 1 |
| 51 | 58.49.216.113 | android.bugly.qq.com | 中国 湖北省 武汉市 电信 | 1 |
| 52 | 111.170.15.148 | img10.jiuxian.com | 中国 湖北省 襄阳 电信 | 1 |
| 53 | 115.231.143.71 | tbs.imtt.qq.com | 中国 浙江省 衢州市 电信 | 1 |
| 54 | 202.107.192.66 | shortvideo.qiniuapi.com | 中国 浙江省 杭州市 电信 | 1 |
| 55 | 110.253.189.200 | ccs.umeng.com | 中国 河北省 张家口市 联通 | 1 |
| 56 | 116.211.155.211 | newappproduct.jiuxian.com | 中国 湖北省 武汉市 电信 | 1 |

## 传输个人信息

本应用在前台运行行为阶段过程中，抓取到0次传输个人信息行为其中应用0次，第三方SDK0次：

注：如需查看其他行为阶段的详细数据，请下载《酒仙\_9.1.19\_行为数据》文档。

## 存储个人信息

本应用在前台运行行为阶段过程中，存储了0次个人信息数据，其中应用0次，第三方SDK0次：

注：如需查看其他行为阶段的详细数据，请下载《酒仙\_9.1.19\_行为数据》文档。

## 个人信息风险漏洞

### Java代码反编译风险检测

|  |  |
| --- | --- |
| **检测目的** | 检测应用是否存在被反编译后泄露源代码的风险。 |
| **风险等级** | 高 |
| **威胁描述** | Android应用如果未采用有效的保护措施，可能面临被反编译的风险。反编译是将二进制程序转换成人们易读的一种描述语言的形式，是逆向工程中的常见手段。反编译的结果是易读的应用程序代码，这样就暴露了Android应用客户端的所有逻辑，比如与服务端的通讯方式、加解密算法、密钥、转账业务流程、软键盘技术实现等等。攻击者可以利用这些信息窃取客户端的敏感数据，包括手机号、密码；绕过业务安全认证流程，直接篡改用户账号信息等。 |
| **检测结果** | 安全 |
| **结果描述** | 该应用的Java代码已被加壳保护。 |
| **出现次数** | 0次 |
| **检测详情** | N/A |
| **解决方案** | 建议使用专业应用安全加固方案，对APK包中的classes.dex文件进行保护，防止应用被反编译。 |

### 资源文件泄露风险检测

|  |  |
| --- | --- |
| **检测目的** | 检测应用中的资源文件是否存在被查看分析风险。 |
| **风险等级** | 中 |
| **威胁描述** | 程序在未进行资源文件加密时，直接把APK解压缩或者反编译会造成APK 的资源文件被窃取、查看分析的风险。 |
| **检测结果** | 存在风险 |
| **结果描述** | 该应用存在资源文件泄露风险。检测文件总数1565个，检测出1564处风险。 |
| **出现次数** | 1564次 |
| **检测详情** | 1．使用静态检测引擎对APK进行反编译。 2．扫描反编译后的代码文件，发现可以获取源代码。 第1处： 文件： res/layout/layout\_o2o\_product\_detail\_content.xml 第2处： 文件： res/layout/item\_near\_store.xml 第3处： 文件： res/layout/item\_o2o\_cart\_gift.xml 第4处： 文件： res/layout/activity\_my\_userinfo.xml 第5处： 文件： res/layout/address\_selector.xml 第6处： 文件： res/layout/test\_address\_activity.xml 第7处： 文件： res/layout/common\_up\_slide\_dialog\_layout.xml 第8处： 文件： res/layout/item\_recommend.xml 第9处： 文件： res/layout/community\_circle.xml 第10处： 文件： res/layout/pop\_personal\_center\_report.xml 第11处： 文件： res/layout/activity\_jzk\_address\_select.xml 第12处： 文件： res/layout/activity\_user\_privacy.xml 第13处： 文件： res/layout/item\_service\_detail.xml 第14处： 文件： res/layout/activity\_capture\_wine\_wiki.xml 第15处： 文件： res/layout/b2c\_pop\_composite.xml 第16处： 文件： res/layout/activity\_o2o\_orderdetail\_layout.xml 第17处： 文件： res/layout/shifting\_bottom\_navigation\_item.xml 第18处： 文件： res/layout/pop\_phone\_vip\_tab.xml 第19处： 文件： res/layout/collect\_tem\_recommend.xml 第20处： 文件： res/layout/design\_layout\_snackbar.xml 第21处： 文件： res/layout/activity\_choose\_shop.xml 第22处： 文件： res/layout/o2o\_part\_item\_quickenter.xml 第23处： 文件： res/layout/o2o\_fragment\_mainhome.xml 第24处： 文件： res/layout/part\_item\_ad\_storey\_1\_1\_2.xml 第25处： 文件： res/layout/part\_item\_ad\_two\_list.xml 第26处： 文件： res/layout/item\_mainhome\_topic.xml 第27处： 文件： res/layout/activity\_collect.xml 第28处： 文件： res/layout/product\_switch\_tag.xml 第29处： 文件： res/layout/pop\_bottom\_btn.xml 第30处： 文件： res/layout/activity\_o2o\_append\_comment.xml 第31处： 文件： res/layout/b2c\_shop\_list\_second\_layout.xml 第32处： 文件： res/layout/status.xml 第33处： 文件： res/layout/item\_o2o\_fragment\_main\_mine\_hor\_wine.xml 第34处： 文件： res/layout/chat\_input.xml 第35处： 文件： res/layout/horizontal\_winelist\_gallery\_layout.xml 第36处： 文件： res/layout/abc\_activity\_chooser\_view.xml 第37处： 文件： res/layout/design\_navigation\_menu.xml 第38处： 文件： res/layout/o2o\_item\_homelist\_with\_head.xml 第39处： 文件： res/layout/item\_o2o\_cart\_change\_buy\_product\_view.xml 第40处： 文件： res/layout/item\_change\_shop\_active.xml 第41处： 文件： res/layout/account\_safe\_activity.xml 第42处： 文件： res/layout/activity\_message\_setting.xml 第43处： 文件： res/layout/xn\_dialog\_myvioce.xml 第44处： 文件： res/layout/b2c\_o2o\_activity\_main\_header.xml 第45处： 文件： res/layout/item\_icart\_coudan\_recommend.xml 第46处： 文件： res/layout/item\_condition.xml 第47处： 文件： res/layout/dialog\_pre\_sell\_rule.xml 第48处： 文件： res/layout/item\_phone\_vip\_product.xml 第49处： 文件： res/layout/fragment\_o2o\_order\_list.xml 第50处： 文件： res/layout/community\_homepage.xml |
| **解决方案** | 使用专业的安全加固方案，对资源文件进行加密处理，保证文件在存储过程中为密文。 |

### 访问境外服务器风险检测

|  |  |
| --- | --- |
| **检测目的** | 检测应用中ip、域名是否访问境外服务器。 |
| **风险等级** | 高 |
| **威胁描述** | 应用程序访问境外服务器造成网络请求延迟、卡顿，被防火墙屏蔽网络请求出现访问无响应。 |
| **检测结果** | 安全 |
| **结果描述** | 该应用不存在境外IP地址。 |
| **出现次数** | 0次 |
| **检测详情** | N/A |
| **解决方案** | 建议开发者对应用中的 ip 、域名使用境内服务器 |

### SSL证书有效性风险检测

|  |  |
| --- | --- |
| **检测目的** | 检测应用是否对客户端和服务端证书进行有效性校验。 |
| **风险等级** | 中 |
| **威胁描述** | 使用HTTPS协议时，客户端必须对服务器证书进行完整性校验，以验证服务器的合法性。如果未校验，客户端可能与仿冒的服务器建立通信链接，同时服务端也可能与仿冒的客户端建立通信链接，即“中间人攻击”。Android允许开发者重定义证书验证方法，使用X509TrustManager类检查证书是否合法并且是否过期。如果重写X509TrustManager时，checkServerTrusted()方法对证书校验结果未做任何处理，即在证书验证失败时，仍然与服务器建立通信链接，存在发生“中间人攻击”的风险。当发生中间人攻击时，仿冒的中间人可以冒充服务器与客户端进行交互，同时冒充客户端与服务器进行交互，在充当中间人转发信息的时候，窃取手机号码、账号、密码等敏感信息，甚至可能对通信内容进行篡改。 |
| **检测结果** | 安全 |
| **结果描述** | 该应用不存在SSL证书有效性校验风险。 |
| **出现次数** | 0次 |
| **检测详情** | N/A |
| **解决方案** | 建议开发者自查，在使用HTTPS协议时应对证书的合法性进行校验，校验失败时应进行正确处理。<w:br/>修复代码示例如下：<w:br/> @Override<w:br/> public void checkServerTrusted(X509Certificate[] X509Certificates, String s) throws CertificateException {<w:br/> if(x509Certificates == null) {<w:br/> throws new IllegalArgumentException("Check Server x509Certificates is null");<w:br/> }<w:br/> <w:br/> if(x509Certificates.length &lt; 0 ){<w:br/> throws new IllegalArgumentException("Check Server x509Certificates is empty");<w:br/> }<w:br/> <w:br/>for(x509Certificates cert : x509Certificates){<w:br/> //检查服务端证书是否过期<w:br/> cert.checkValidity();<w:br/>try{<w:br/> cert.verify(serverCert.getPublicKey());<w:br/>}catch (NoSuchAlgorithmException e) {<w:br/> e.printStackTrace();<w:br/> }catch (InvalidKeyException e) {<w:br/> e.printStackTrace();<w:br/> }catch (NoSuchProviderException e) {<w:br/> e.printStackTrace();<w:br/> }catch (SignatureException e) {<w:br/> e.printStackTrace();<w:br/> }<w:br/>} |

### HTTP传输通道风险检测

|  |  |
| --- | --- |
| **检测目的** | 检测应用是否使用HTTPS协议对传输通道进行加密。 |
| **风险等级** | 低 |
| **威胁描述** | 由于HTTP数据传输是明文传输的，导致HTTP数据容易被抓取、篡改，泄露用户的敏感数据，如账号、密码等。甚至通过中间人劫持将原有信息替换成恶意链接或恶意代码程序，以达到远程控制、恶意扣费等攻击意图。 |
| **检测结果** | 安全 |
| **结果描述** | 该应用没有使用HTTP协议进行数据传输。 |
| **出现次数** | 0次 |
| **检测详情** | N/A |
| **解决方案** | 建议开发者对应用中的重要数据使用HTTPS协议传输。 |

### 启用VPN服务检测

|  |  |
| --- | --- |
| **检测目的** | 检测应用是否启动了VPN服务。 |
| **风险等级** | 低 |
| **威胁描述** | VPN（虚拟专用网络）的功能是在公用网络上建立专用网络，进行加密通讯。VPN网关通过对数据包的加密和数据包目标地址的转换实现远程访问。翻墙，指绕过相应的IP封锁、内容过滤、域名劫持、流量限制等，实现对海外敏感网站或邮件的访问。提供“翻墙”服务的VPN软件又叫“翻墙”软件，提供“翻墙”服务属于违法行为。同时使用恶意VPN联网时，通过网络请求的数据容易被劫持，造成用户敏感信息泄露。 |
| **检测结果** | 安全 |
| **结果描述** | 该应用未使用VPN。 |
| **出现次数** | 0次 |
| **检测详情** | N/A |
| **解决方案** | 建议开发者自查，应用中不要启动VPN服务。 |

### 密钥硬编码风险检测

|  |  |
| --- | --- |
| **检测目的** | 检测应用是否存在密钥硬编码风险。 |
| **风险等级** | 高 |
| **威胁描述** | 密钥硬编码是指在代码中直接将加密算法的密钥设置为一个固定值。加密算法本身都是公开的，加密内容的安全主要依赖于加密密钥。当密钥被硬编码在代码中时，攻击者可以通过反编译得到密钥，从而破解加密数据，获取加密前的明文信息。密钥硬编码，可直接造成加密数据被破解，客户端与服务器之间的通信内容被破解，导致应用内的加密文件被破解，或是用户的敏感信息泄露。 |
| **检测结果** | 安全 |
| **结果描述** | 该应用不存在密钥硬编码漏洞。 |
| **出现次数** | 0次 |
| **检测详情** | N/A |
| **解决方案** | 1. 使用算法生成密钥。<w:br/> 2. 若不使用算法生成密钥，则使用参数的形式传递密钥，使密钥与加密算法不在同一函数中。 |

### WebView明文存储密码风险检测

|  |  |
| --- | --- |
| **检测目的** | 检测应用的WebView组件中是否使用明文保存用户名及密码。 |
| **风险等级** | 高 |
| **威胁描述** | WebView组件默认开启了密码保存功能，会提示用户是否保存密码，当用户选择保存在WebView中输入的用户名和密码，则会被明文保存到应用数据目录的databases/webview.db中。攻击者可能通过root的方式访问该应用的WebView数据库，从而窃取本地明文存储的用户名和密码。 |
| **检测结果** | 安全 |
| **结果描述** | 该应用不存在明文存储密码漏洞。 |
| **出现次数** | 0次 |
| **检测详情** | N/A |
| **解决方案** | 建议开发者通过WebView.getSettings().setSavePassword(false)来关闭WebView组件的密码保存功能。 |

### 输入监听风险检测

|  |  |
| --- | --- |
| **检测目的** | 检测应用在敏感数据输入时是否使用不安全的系统键盘。 |
| **风险等级** | 中 |
| **威胁描述** | 客户端的敏感界面如登录界面、注册界面、支付界面等，用户在输入敏感信息与显示（输出）时，如果未使用安全键盘，而使用第三方未知键盘或系统键盘的话可能存在数据被拦截与监听的风险，导致账号、密码等敏感数据泄露。 |
| **检测结果** | 安全 |
| **结果描述** | 该应用不存在系统键盘使用风险。 |
| **出现次数** | 0次 |
| **检测详情** | N/A |
| **解决方案** | 在敏感数据输入时使用专业的安全键盘，可以有效防止输入敏感内容时被监听。 |

**附件一：Android涉及个人信息权限**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **权限分组** | **权限名** | **功能描述** | **可访问的个人信息** | **业务功能示例** |
| 1 | CAENDAR日历 | READ\_CALENDAR读取日历 | 允许App读取用户日历数据 | 系统日历中的日程安排、备忘、行程等信息 | 例如日程规划、事件提醒、票务预订等 |
| 2 | WRITE\_CALENDAR编辑日历 | 允许App写入用户日历数据 |
| 3 | CALL\_LOG通话记录 | READ\_CALL\_LOG读取通话记录 | 允许App读取用户通话记录 | 用户通话记录 | 例如通话记录管理、备份与恢复，骚扰截、SOS紧急求助等 |
| 4 | WRITE\_CALL\_LOG编辑通话记录 | 允许App写入用户通话记录 |
| 5 | PROCESS\_OUTGOING\_CALLS监听呼出电话 | 允许App查看正在拨打的号码，并监听、控制或终止呼出电话 | 用户呼出的电话号码、呼叫状态等信息 | 例如呼出电话监控场景、儿童手表、骚扰拦截等 |
| 6 | CAMERA相机 | CAMERA拍摄 | 允许App使用摄像头 | 照片或视频信息 | 例如拍摄照片视频、扫描二维码/条形码、人脸识别等 |
| 7 | CONTACTS通讯录 | READ\_CONTACTS读取通讯录 | 允许App读取用户通讯录 | 联系人数据 | 例如通讯录管理与备份、添加联系人等 |
| 8 | WRITE\_CONTACTS编辑通讯录 | 允许App写入用户通讯录 |
| 9 | GET\_ACCOUNTS获取App账户 | 允许App从账户务中获取App账户列表 | 账户服务中的App账户列表 | 账号登录场景等 |
| 10 | LOCATION位置 | ACCESS\_FINE\_LOCATION访问精准定位 | 允许App获取基于GPS等的精准地理位置 | 精准地理位置信息 | 例如定位当用户位置、拍照记录照片拍摄位置、社交分享位置、O2O上门服务定位用户位置等需要用户精准位置的场景 |
| 11 | ACCESS\_COARSE\_LOCATION访问粗略位置 | 允许App获取基于基站、IP等粗略的地理位置 | 粗略地理位置信息 | 例如外卖、本地生活服务等分区域信息推荐、基于城市或地域进行新闻推送等基于粗略用户地理置的场景 |
| 12 | ACCESS\_BACKGROUND\_LOCATION支持后台访问位置 | 允许App在后台运行时使用位置信息（需要App获得访问粗略位置或访问精准位置权限） | 实时地理位置信息、行踪轨迹 | 例如地图导航、网络约车、运动健身等场景 |
| 13 | MICROPHONE麦克风 | RECORD\_AUDIO录音 | 允许App使用麦克风进行录音 | 录音内容 | 例如语音即时通信、语音识别、音视频录制、直播等语音输入场景 |
| 14 | PHONE电话 | READ\_PHONE\_STATE读取电话状态 | App可通过此权限获取设备IMSI（国际移动用户识别码）、IMEI（国际移动设备识别码）等设备唯一标识信息，以及手机通话状态等 | 设备唯一标识信息（如IMEI、设备序列号） | 进行用户常用设备的标识，可用于监测App账户异常登录、关联用户行为 |
| 15 | READ\_PHONE\_NUMBERS读取本机电话号码 | 允许App读取用户的本机电话号码 | 手机号码 | 读取本机号码场景 |
| 16 | CALL\_PHONE拨打电话 | 允许App直接拨打电话 | 实时通话行为 | 例如在App内直接拨打商家、快递员、客服电话等 |
| 17 | ANSWER\_PHONE\_CALLS接听电话 | 允许App接听拨入的电话 | 例如在驾驶模式下直接接听来电等 |
| 18 | ADD\_VOICEMAIL添加语音邮件 | 允许App向邮件中添加语音附件 | 语音邮件内容 |  |
| 19 | USE\_SIP使用网络电话 | 允许App拨打/接听SIP网络电话 | 实时网络通话行为 | 例如接听、拨打网络电话等 |
| 20 | ACCEPT\_HANDOVER继续进行来自其他App的通话 | 允许App继续进行在其他App中发起的通话 | 实时网络通话行为 |  |
| 21 | BODY\_SENSORS身体传感器 | BODY\_SENSORS获取身体传感器信息 | 允许App访问身体内部状况相关的传感器数据，一般特指心率传感器数据 | 心率等身体传感器数据 | 例如运动健身、健康类App及可穿戴设备显示心率等状况 |
| 22 | SMS短信 | SEND\_SMS发送短信 | 允许App发送短信 | 短信 | 例如短信管理、短信备份恢复、手机号码注册或登录时的验证码场景、SOS紧急求助等 |
| 23 | RECEIVE\_SMS接收短信 | 允许App接收短信 |
| 24 | READ\_SMS读取文字讯息（短信或彩信） | 允许App读取短信或彩信 | 短信、彩信内容 |
| 25 | RECEIVE\_WAP\_PUSH接收WAP推送 | 允许App接收WAP推送信息 | WAP推送消息 | 例如短信管理、WAP消息推送场景等 |
| 26 | RECEIVE\_MMS接收彩信 | 允许App接收彩信 | 彩信 | 例如短信管理、接收彩信场景等 |
| 27 | STORAGE存储 | READ\_EXTERNAL\_STORAGE读取外置存储器 | 允许App读取外置存储器 | 外置存储器存储的个人数据 | 例如文件管理、阅读器等打开本地文件的场景等 |
| 28 | WRITE\_EXTERNAL\_STORAGE写入外置存储器 | 允许App写入外置存储器 | 例如存储拍摄的照片和视频，及下载文件、需要下载大量资源的游戏场景等 |
| 29 | ACCESS\_MEDIA\_LOCATION读取照片位置信息 | 允许App读取照片文件中包含的拍摄地点信息 | 照片拍摄地点信息 | 例如展示照片拍摄地点的场景等 |
| 30 | ACTIVITY\_RECOGNITION身体活动 | ACTIVITY\_RECOGNITION识别身体活动 | 允许App识别身体活动 | 特定身体活动变化信息（如未移动、步行、跑步、骑车、坐车等） | 例如追踪用户步数及卡路里消耗、需要对用户的身体活动进行分类的场景等 |
| 31 |  | PACKAGE\_USAGE\_STATS读取应用使用情况 | 允许App获取其他App的使用统计数据 |  | 例如使用频率，使用时长，以及语言设置等使用记录 |
| 32 |  | BIND\_DEVICE\_ADMIN设备管理器 | 允许App激活使用设备管理器 |  |  |
| 33 |  | BIND\_ACCESSIBILITY\_SERVICE辅助模式 | 允许App通过屏幕取词、模拟用户点击等方式，方便用户操作 |  | 也称无障碍功能 |
| 34 |  | BIND\_NOTIFICATION\_LISTENER\_SERVICE监听通知栏 | 允许App监听其他App通知栏显示的内容 |  |  |
| 35 |  | SYSTEM\_ALERT\_WINDOW悬浮窗 | 允许App在其他App上覆盖显示 |  |  |
| 36 |  | CHANGE\_WIFI\_STATE改变WLAN状态的开关 | 允许App打开或关闭Wi-Fi | 网络配置信息 |  |
| 37 |  | BLUETOOTH\_ADMIN打开蓝牙 | 允许App打开或关闭蓝牙 | 蓝牙上传/下载信息 |  |
| 38 | 工信部 | GET\_TASKS允许程序获取当前或最近运行的应用 | 允许APP获取当前或最近运行的应用 | 当前或最近运行的应用 |  |
| 39 | 工信部 | PackageManager.getInstalledPackages() | 允许APP获取当前已安装应用软件列表 | 已安装应用软件列表 |  |

**附件二：个人信息**

个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，如姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

判定某项信息是否属于个人信息，应考虑以下两条路径：一是识别，即从信息到个人，由信息本身的特殊性识别出特定自然人，个人信息应有助于识别出特定个人。二是关联，即从个人到信息，如已知特定自然人，由该特定自然人在其活动中产生的信息（如个人位置信息、个人通话记录、个人浏览记录等）即为个人信息。符合上述两种情形之一的信息，均应判定为个人信息。

表A.1给出了个人信息举例。

表A.1 个人信息举例

|  |  |
| --- | --- |
| **个人基本资料** | 个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等 |
| **个人身份信息** | 身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等 |
| **个人生物识别信息** | 个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等 |
| **网络身份标识信息** | 个人信息主体账号、IP 地址、个人数字证书等 |
| **个人健康生理信息** | 个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况相关的信息，如体重、身高、肺活量等 |
| **个人教育工作信息** | 个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等 |
| **个人财产信息** | 银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息 |
| **个人通信信息** | 通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据（通常称为元数据）等 |
| **联系人信息** | 通讯录、好友列表、群列表、电子邮件地址列表等 |
| **个人上网记录** | 指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等 |
| **个人常用设备信息** | 指包括硬件序列号、设备 MAC 地址、软件列表、唯一设备识别码（如IMEI/Android ID/IDFA/OpenUDID/GUID/SIM 卡 IMSI 信息等）等在内的描述个人常用设备基本情况的信息 |
| **个人位置信息** | 包括行踪轨迹、精准定位信息、住宿信息、经纬度等 |
| **其他信息** | 婚史、宗教信仰、性取向、未公开的违法犯罪记录等 |

**附件三：个人敏感信息**

个人敏感信息是指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。通常情况下，14岁以下（含） 儿童的个人信息和涉及自然人隐私的信息属于个人敏感信息。可从以下角度判定是否属于个人敏感信息：

泄露：个人信息一旦泄露，将导致个人信息主体及收集、使用个人信息的组织和机构丧失对个人信息的控制能力，造成个人信息扩散范围和用途的不可控。某些个人信息在泄漏后，被以违背个人信息主体意愿的方式直接使用或与其他信息进行关联分析，可能对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，个人信息主体的身份证复印件被他人用于手机号卡实名登记、银行账户开户办卡等。

非法提供：某些个人信息仅因在个人信息主体授权同意范围外扩散，即可对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，性取向、存款信息、传染病史等。

滥用：某些个人信息在被超出授权合理界限时使用（如变更处理目的、扩大处理范围等），可能对个人信息主体权益带来重大风险，应判定为个人敏感信息。例如，在未取得个人信息主体授权时，将健康信息用于保险公司营销和确定个体保费高低。

表B.1给出了个人敏感信息举例。

表B.1 个人敏感信息举例

|  |  |
| --- | --- |
| **个人财产信息** | 银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息 |
| **个人健康生理信息** | 个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等 |
| **个人生物识别信息** | 个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等 |
| **个人身份信息** | 身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等 |
| **其他信息** | 性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等 |