南明离火
移动应用检测平台

# ANDROID 静态分析报告

test • v1.0



分析日期: 2025-05-16 07:47:35

# 应用概览

| | |
|---|---|
| 文件名称: | test.apk |
| 文件大小: | 1.11MB |
| 应用名称: | test |
| 软件包名: | com.lawivehelowu.vezino |
| 主活动: | com.lawivehelowu.vezino.muyaxoheyafe |
| 版本号: | 1.0 |
| 最小SDK: | 27 |
| 目标SDK: | 28 |
| 加固信息: | 未加壳 |
| 开发框架: | Java/Kotlin |
| 应用程序安全分数: | 36/100 (高风险) |
| 杀软检测: | 28 个杀毒软件报毒 |
| MD5: | e380822a814c12db6f82f705298f44fb |
| SHA1: | 6a281f0d17b9260cd4060bc39a6d498b489d3e6c |
| SHA256: | 14686cea935b7ac1dbcf314a574f50f2569d08d2d59b9baaae5857041295d954 |

# 分析结果严重性分布

| 高危 | 中危 | 信息 | 安全 | 关注 |
|---|---|---|---|---|
| 19 | 41 | 2 | 2 | 0 |

# 四大组件导出状态统计

| |
|---|
| Activity组件：11个，其中export的有：8个 |
| Service组件：11个，其中export的有：8个 |
| Receiver组件：13个，其中export的有：6个 |
| Provider组件：1个，其中export的有：0个 |

# 应用签名证书信息

APK已签名
v1 签名: False

v2 签名: True
v3 签名: False
v4 签名: False
主题: C=US, O=naji, CN=fudadako
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-06 01:15:42+00:00
有效期至: 2027-12-31 01:15:42+00:00
发行人: C=US, O=naji, CN=fudadako
序列号: 0x2be4509d
哈希算法: sha256
证书MD5: df4076a712c46df3c2c8779546e92fac
证书SHA1: 3e9d21e07705b2c0295b58c7633c6b929af33618
证书SHA256: 67fb04b31454639522fbc83db9968446b51138b0d880e45f6174344de09c1510
证书SHA512:
1c3299037fc85b0b96143ec2eae776b3dd704058c575a5c9b97ffa2959362d9fea50f193e59a3761d417003d96a0015ee2a48432c7db7657e46c4d03e1a46659

公钥算法: rsa
密钥长度: 2048
指纹: 11c1dbe36f1a5208ffd5d03eb3f6729d8f459fb20863559aa75ae7fc112b0ea3
共检测到 1 个唯一证书

## 权限声明与风险分级

| 权限名称 | 安全等级 | 权限内容 | 权限描述 |
| --- | --- | --- | --- |
| android.permission.CAMERA | 危险 | 拍照和录制视频 | 允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像 |
| android.permission.FOREGROUND_SERVICE | 普通 | 创建前台Service | Android 9.0以上允许常规应用程序使用 Service.startForeground，用于Podcast播放（推送悬浮播放，锁屏播放） |
| 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SD卡内容 | 允许应用程序从SD卡读取信息。 |
| android.permission.INTERNET | 危险 | 完全互联网访问 | 允许应用程序创建网络套接字。 |
| android.permission.ACCESS_NETWORK_STATE | 普通 | 获取网络状态 | 允许应用程序查看所有网络的状态。 |
| android.permission.ACCESS_WIFI_STATE | 普通 | 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.READ_SMS | 危险 | 读取短信 | 允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。 |
| android.permission.SEND_SMS | 危险 | 发送短信 | 允许应用程序发送短信。恶意应用程序可能会不经您的确认就发送信息，给您带来费用。 |
| android.permission.RECEIVE_SMS | 危险 | 接收短信 | 允许应用程序接收短信。 恶意程序会在用户未知的情况下监视或删除。 |
| android.permission.READ_PHONE_STATE | 危险 | 读取手机状态和标识 | 允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。 |
| android.permission.READ_PHONE_NUMBERS | 危险 | 允许读取设备的电话号码 | 允许读取设备的电话号码。这是READ PHONE STATE授予的功能的一个子集，但对即时应用程序公开。 |
| android.permission.READ_CALL_LOG | 危险 | 读取通话记录 | 允许应用程序读取用户的通话记录 |

| | | | |
|---|---|---|---|
| android.permission.CALL_PHONE | 危险 | 直接拨打电话 | 允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。 |
| android.permission.MODIFY_AUDIO_SETTINGS | 危险 | 允许应用修改全局音频设置 | 允许应用程序修改全局音频设置，如音量。多用于消息语音功能。 |
| android.permission.ACCESS_COARSE_LOCATION | 危险 | 获取粗略位置 | 通过WiFi或移动基站的方式获取用户粗略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。 |
| android.permission.READ_CONTACTS | 危险 | 读取联系人信息 | 允允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。 |
| android.permission.WRITE_CONTACTS | 危险 | 写入联系人信息 | 允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。 |
| android.permission.GET_ACCOUNTS | 普通 | 探索已知账号 | 允许应用程序访问帐户服务中的帐户列表。 |
| android.permission.WAKE_LOCK | 危险 | 防止手机休眠 | 允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。 |
| android.permission.RECEIVE_BOOT_COMPLETED | 普通 | 开机自启 | 允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。 |
| android.permission.ACTION_MANAGE_OVERLAY_PERMISSION | 未知 | 未知权限 | 来自 android 引用的未知权限。 |
| android.permission.SYSTEM_ALERT_WINDOW | 危险 | 弹窗 | 允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。 |
| android.permission.DISABLE_KEYGUARD | 危险 | 禁用键盘锁 | 允许应用程序停用键锁和任何关联的密码安全设置。例如，在手机上接听电话时停用键锁，在通话结束后重新启用键锁。 |
| android.permission.GET_TASKS | 危险 | 检索当前运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。 |
| android.permission.QUERY_ALL_PACKAGES | 普通 | 获取已安装应用程序列表 | Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。 |
| android.permission.GET_CLIPS | 未知 | 未知权限 | 来自 android 引用的未知权限。 |
| android.permission.READ_CLIPS | 普通 | 读取剪贴板 | 这种权限的作用是允许应用读取剪贴板的内容。 |
| android.permission.WRITE_CLIPS | 普通 | 写入剪贴板 | 这种权限的作用是允许应用将数据写入剪贴板。 |
| android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS | 普通 | 使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限 | 应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。 |
| android.permission.REQUEST_DELETE_PACKAGES | 普通 | 请求删除应用 | 允许应用程序请求删除包。 |
| android.permission.RECEIVE_LAUNCH_BROADCASTS | 未知 | 未知权限 | 来自 android 引用的未知权限。 |
| android.permission.QUICKBOOT_POWERON | 普通 | 接收设备重启或快速启动的广播的权限 | 一个用于接收设备重启或快速启动的广播的权限。它允许应用程序在设备重新启动后执行一些操作，例如启动一个服务，更新一些数据，或者显示一些通知。 |



## 可浏览 Activity 组件分析

| ACTIVITY | INTENT |
| --- | --- |
| com.fafozixafigexi.dotejeku.bolekumo.zepupi | Schemes: sms://, mms://, mmsto://, smsto://, |

## 网络通信安全风险分析

| 序号 | 范围 | 严重级别 | 描述 |
| --- | --- | --- | --- |

## 证书安全合规分析

高危: **0** | 警告: **0** | 信息: **1**

| 标题 | 严重程度 | 描述信息 |
| --- | --- | --- |
| 已签名应用 | 信息 | 应用已使用代码签名证书进行签名。 |

## Manifest 配置安全分析

高危: **18** | 警告: **35** | 信息: **0** | 屏蔽: **0**

| 序号 | 问题 | 严重程度 | 描述信息 |
| --- | --- | --- | --- |
| 1 | 应用已启用明文网络流量 [android:usesCleartextTraffic=true] | 警告 | 应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可能监听或篡改传输数据。建议关闭明文流量，仅使用加密协议。 |
| 2 | 应用数据允许备份 [android:allowBackup=true] | 警告 | 该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。 |
| 3 | Activity (com.lawivehelowu.vezino.muyaxoheyafe) 易受 StrandHogg 2.0 攻击 | 高危 | 检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。 |
| 4 | Activity (com.lawivehelowu.vezino.Facebook) 易受 StrandHogg 2.0 攻击 | 高危 | 检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。 |
| 5 | Activity-Alias (com.lawivehelowu.vezino.Facebook) 未受保护。 [android:exported=true] | 警告 | 检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。 |
| 6 | Activity (com.lawivehelowu.vezino.Play) 易受 StrandHogg 2.0 攻击 | 高危 | 检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。 |
| 7 | Activity-Alias (com.lawivehelowu.vezino.Play) 未受保护。 [android:exported=true] | 警告 | 检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。 |

| | | | |
|---|---|---|---|
| 8 | Activity (com.lawivehelowu.vezino.Gmail) 易受 StrandHogg 2.0 攻击 | 高危 | 检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。 |
| 9 | Activity-Alias (com.lawivehelowu.vezino.Gmail) 未受保护。 [android:exported=true] | 警告 | 检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。 |
| 10 | Activity (com.lawivehelowu.vezino.Contacts) 易受 StrandHogg 2.0 攻击 | 高危 | 检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。 |
| 11 | Activity-Alias (com.lawivehelowu.vezino.Contacts) 未受保护。 [android:exported=true] | 警告 | 检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。 |
| 12 | Activity (com.lawivehelowu.vezino.Whatsapp) 易受 StrandHogg 2.0 攻击 | 高危 | 检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。 |
| 13 | Activity-Alias (com.lawivehelowu.vezino.Whatsapp) 未受保护。 [android:exported=true] | 警告 | 检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。 |
| 14 | Activity (com.lawivehelowu.vezino.Youtube) 易受 StrandHogg 2.0 攻击 | 高危 | 检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。 |
| 15 | Activity-Alias (com.lawivehelowu.vezino.Youtube) 未受保护。 [android:exported=true] | 警告 | 检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。 |
| 16 | Activity (com.lawivehelowu.vezino.Chrome) 易受 StrandHogg 2.0 攻击 | 高危 | 检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。 |
| 17 | Activity-Alias (com.lawivehelowu.vezino.Chrome) 未受保护。 [android:exported=true] | 警告 | 检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。 |
| 18 | Activity (com.lawivehelowu.vezino.Instagram) 易受 StrandHogg 2.0 攻击 | 高危 | 检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。 |
| 19 | Activity-Alias (com.lawivehelowu.vezino.Instagram) 未受保护。 [android:exported=true] | 警告 | 检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。 |


本报告由南明离火移动安全分析平台生成

| | | | |
|---|---|---|---|
| 20 | Activity (com.lawivehelowu.vezino.TikTok) 易受 StrandHogg 2.0 攻击 | 高危 | 检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。 |
| 21 | Activity-Alias (com.lawivehelowu.vezino.TikTok) 未受保护。 [android:exported=true] | 警告 | 检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。 |
| 22 | Activity (com.lawivehelowu.vezino.Telegram) 易受 StrandHogg 2.0 攻击 | 高危 | 检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。 |
| 23 | Activity-Alias (com.lawivehelowu.vezino.Telegram) 未受保护。 [android:exported=true] | 警告 | 检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。 |
| 24 | Activity (com.fafozixafigexi.dotejeku.zacibahewujivive) 未受保护。 [android:exported=true] | 警告 | 检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。 |
| 25 | Activity (com.fafozixafigexi.dotejeku.xirolafowuyavu) 易受 StrandHogg 2.0 攻击 | 高危 | 检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。 |
| 26 | Activity (com.fafozixafigexi.dotejeku.xirolafowuyavu) 未受保护。 [android:exported=true] | 警告 | 检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。 |
| 27 | Activity (com.fafozixafigexi.dotejeku.lufosigatize.vafa) 易受 StrandHogg 2.0 攻击 | 高危 | 检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。 |
| 28 | Activity (com.fafozixafigexi.dotejeku.lufosigatize.vafa) 未受保护。 [android:exported=true] | 警告 | 检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。 |
| 29 | Activity (com.fafozixafigexi.dotejeku.nenujojiroroju.kehenu) 易受 StrandHogg 2.0 攻击 | 高危 | 检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。 |
| 30 | Activity (com.fafozixafigexi.dotejeku.nenujojiroroju.kehenu) 未受保护。 [android:exported=true] | 警告 | 检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。 |
| 31 | Activity (com.fafozixafigexi.dotejeku.bilekumo.yeyotubivaga) 易受 StrandHogg 2.0 攻击 | 高危 | 检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。 |


本报告由南明离火移动安全分析平台生成

| | | | |
|---|---|---|---|
| 32 | Activity (com.fafozixafigexi.dotejeku.bolekumo.yeyotubivaga) 未受保护。 [android:exported=true] | 警告 | 检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。 |
| 33 | Activity (com.fafozixafigexi.dotejeku.covurafemutocahi.fuka) 易受 StrandHogg 2.0 攻击 | 高危 | 检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。 |
| 34 | Activity (com.fafozixafigexi.dotejeku.covurafemutocahi.fuka) 未受保护。 [android:exported=true] | 警告 | 检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。 |
| 35 | Service (com.fafozixafigexi.dotejeku.kege.yozu) 未受保护。 [android:exported=true] | 警告 | 检测到 Service 已导出，未受任何权限保护，任意应用均可访问。 |
| 36 | Service (com.fafozixafigexi.dotejeku.lufosigatize.lumojoco) 未受保护。 [android:exported=true] | 警告 | 检测到 Service 已导出，未受任何权限保护，任意应用均可访问。 |
| 37 | Service (com.fafozixafigexi.dotejeku.lufosigatize.muvecedugagu) 未受保护。 [android:exported=true] | 警告 | 检测到 Service 已导出，未受任何权限保护，任意应用均可访问。 |
| 38 | Service (com.fafozixafigexi.dotejeku.lufosigatize.relahorufo) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_NOTIFICATION_LISTENER_SERVICE [android:exported=true] | 警告 | 检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。 |
| 39 | Service (com.fafozixafigexi.dotejeku.yayibuyutopura.xuvizajujilete) 未受保护。 [android:exported=true] | 警告 | 检测到 Service 已导出，未受任何权限保护，任意应用均可访问。 |
| 40 | Service (com.fafozixafigexi.dotejeku.nelihuvexecile.casuwa) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_ACCESSIBILITY_SERVICE [android:exported=true] | 警告 | 检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。 |
| 41 | Broadcast Receiver (com.fafozixafigexi.dotejeku.nenujojirorohu.juzigowoniluju) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_DEVICE_ADMIN [android:exported=true] | 警告 | 检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。 |

| | | | |
|---|---|---|---|
| 42 | Broadcast Receiver (com.fafozixafigexi.dotejeku.diyifuwi.zuyocetiwa) 受权限保护，但应检查权限保护级别。<br>Permission: android.permission.RECEIVE_BOOT_COMPLETED<br>[android:exported=true] | 警告 | 检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。 |
| 43 | Broadcast Receiver (com.fafozixafigexi.dotejeku.diyifuwi.dejurekenumo) 未受保护。<br>[android:exported=true] | 警告 | 检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。 |
| 44 | Broadcast Receiver (com.fafozixafigexi.dotejeku.bolekumo.takecubu) 受权限保护，但应检查权限保护级别。<br>Permission: android.permission.BROADCAST_SMS<br>[android:exported=true] | 警告 | 检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。 |
| 45 | Activity (com.fafozixafigexi.dotejeku.bolekumo.zepupi) 易受 StrandHogg 2.0 攻击 | 高危 | 检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。 |
| 46 | Activity (com.fafozixafigexi.dotejeku.bolekumo.zepupi) 未受保护。<br>[android:exported=true] | 警告 | 检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。 |
| 47 | Activity (com.fafozixafigexi.dotejeku.jacebecitiyuda) 易受 StrandHogg 2.0 攻击 | 高危 | 检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。 |
| 48 | Activity (com.fafozixafigexi.dotejeku.jacebecitiyuda) 未受保护。<br>[android:exported=true] | 警告 | 检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。 |
| 49 | Broadcast Receiver (com.fafozixafigexi.dotejeku.bolekumo.leyapabu) 受权限保护，但应检查权限保护级别。<br>Permission: android.permission.BROADCAST_WAP_PUSH<br>[android:exported=true] | 警告 | 检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。 |
| 50 | Broadcast Receiver (com.fafozixafigexi.dotejeku.bolekumo.yilajaju) 受权限保护，但应检查权限保护级别。<br>Permission: android.permission.BROADCAST_SMS<br>[android:exported=true] | 警告 | 检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。 |

| | | | |
|---|---|---|---|
| 51 | Service (com.fafozixafigexi.dotejeku.bolekumo.bududu) 受权限保护，但应检查权限保护级别。<br>Permission: android.permission.SEND_RESPOND_VIA_MESSAGE [android:exported=true] | 警告 | 检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。 |
| 52 | Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。<br>Permission: android.permission.BIND_JOB_SERVICE [android:exported=true] | 警告 | 检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。 |
| 53 | 高优先级 Intent（999） - {2} 个命中 [android:priority] | 警告 | 通过设置较高的 Intent 优先级，应用可覆盖其他请求，可能导致安全风险。 |

## 代码安全漏洞检测

高危: **1** | 警告: **5** | 信息: **2** | 安全: **1** | 屏蔽: **0**

| 序号 | 问题 | 等级 | 参考标准 | 文件位置 |
|---|---|---|---|---|
| 1 | 应用程序记录日志信息,不得记录敏感信息 | 信息 | CWE: CWE-532: 通过日志文件的信息暴露<br>OWASP MASVS: MSTG-STORAGE-3 | 升级会员：解锁高级权限 |
| 2 | 不安全的Web视图实现。可能存在WebView任意代码执行漏洞 | 警告 | CWE: CWE-749: 暴露危险方法或函数<br>OWASP Top 10: M1: Improper Platform Usage<br>OWASP MASVS: MSTG-PLATFORM-7 | 升级会员：解锁高级权限 |
| 3 | 如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击 | 高危 | CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'）<br>OWASP Top 10: M1: Improper Platform Usage<br>OWASP MASVS: MSTG-PLATFORM-6 | 升级会员：解锁高级权限 |
| 4 | 应用程序使用不安全的随机数生成器 | 警告 | CWE: CWE-330: 使用不充分的随机数<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-6 | 升级会员：解锁高级权限 |

| | | | | |
|---|---|---|---|---|
| 5 | SHA-1是已知存在哈希冲突的弱哈希 | 警告 | CWE: CWE-327: 使用了破损或被认为是不安全的加密算法<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | 升级会员：解锁高级权限 |
| 6 | 此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它 | 信息 | OWASP MASVS: MSTG-STORAGE-10 | 升级会员：解锁高级权限 |
| 7 | 应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库 | 警告 | CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'）<br>OWASP Top 10: M7: Client Code Quality | 升级会员：解锁高级权限 |
| 8 | 文件可能包含硬编码的敏感信息，如用户名、密码、密钥等 | 警告 | CWE: CWE-312: 明文存储敏感信息<br>OWASP Top 10: M9: Reverse Engineering<br>OWASP MASVS: MSTG-STORAGE-14 | 升级会员：解锁高级权限 |
| 9 | 此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击 | 安全 | OWASP MASVS: MSTG-NETWORK-4 | 升级会员：解锁高级权限 |

## 应用行为分析

| 编号 | 行为 | 标签 | 文件 |
|---|---|---|---|
| 00147 | 获取当前位置的时间 | 信息收集<br>位置 | 升级会员：解锁高级权限 |
| 00075 | 获取设备的位置 | 信息收集<br>位置 | 升级会员：解锁高级权限 |
| 00115 | 获取设备的最后已知位置 | 信息收集<br>位置 | 升级会员：解锁高级权限 |
| 00013 | 读取文件并将其放入流中 | 文件 | 升级会员：解锁高级权限 |
| 00003 | 将压缩后的位图数据放入JSON对象中 | 相机 | 升级会员：解锁高级权限 |
| 00014 | 将文件读入流并将其放入 JSON 对象中 | 文件 | 升级会员：解锁高级权限 |
| 00004 | 获取文件名并将其放入 JSON 对象 | 文件<br>信息收集 | 升级会员：解锁高级权限 |
| 00204 | 获取默认铃声 | 信息收集 | 升级会员：解锁高级权限 |
| 00016 | 获取设备的位置信息并将其放入 JSON 对象 | 位置<br>信息收集 | 升级会员：解锁高级权限 |
| 00130 | 获取当前WIFI信息 | WiFi<br>信息收集 | 升级会员：解锁高级权限 |


本报告由南明离火移动安全分析平台生成

| | | | |
|---|---|---|---|
| 00193 | 发送短信 | 短信 | 升级会员：解锁高级权限 |
| 00009 | 将游标中的数据放入JSON对象 | 文件 | 升级会员：解锁高级权限 |
| 00040 | 发送短信 | 短信 | 升级会员：解锁高级权限 |
| 00208 | 捕获设备屏幕的内容 | 信息收集<br>屏幕 | 升级会员：解锁高级权限 |
| 00209 | 从最新渲染图像中获取像素 | 信息收集 | 升级会员：解锁高级权限 |
| 00210 | 将最新渲染图像中的像素复制到位图中 | 信息收集 | 升级会员：解锁高级权限 |
| 00023 | 从当前应用程序启动另一个应用程序 | 反射<br>控制 | 升级会员：解锁高级权限 |
| 00078 | 获取网络运营商名称 | 信息收集<br>电话服务 | 升级会员：解锁高级权限 |
| 00038 | 查询电话号码 | 信息收集 | 升级会员：解锁高级权限 |
| 00079 | 隐藏当前应用程序的图标 | 规避 | 升级会员：解锁高级权限 |
| 00085 | 获取ISO国家代码并将其放入JSON中 | 信息收集<br>电话服务 | 升级会员：解锁高级权限 |
| 00132 | 查询ISO国家代码 | 电话服务<br>信息收集 | 升级会员：解锁高级权限 |
| 00022 | 从给定的文件绝对路径打开文件 | 文件 | 升级会员：解锁高级权限 |
| 00189 | 获取短信内容 | 短信 | 升级会员：解锁高级权限 |
| 00188 | 获取短信地址 | 短信 | 升级会员：解锁高级权限 |
| 00200 | 从联系人列表中查询数据 | 信息收集<br>联系人 | 升级会员：解锁高级权限 |
| 00187 | 查询 URI 并检查结果 | 信息收集<br>短信<br>通话记录<br>日历 | 升级会员：解锁高级权限 |
| 00201 | 从通话记录中查询数据 | 信息收集<br>通话记录 | 升级会员：解锁高级权限 |
| 00077 | 读取敏感数据（短信、通话记录等） | 信息收集<br>短信<br>通话记录<br>日历 | 升级会员：解锁高级权限 |
| 00176 | 向联系人列表中的联系人发送短信 | 短信 | 升级会员：解锁高级权限 |
| 00053 | 监视给定内容 URI 标识的数据更改（SMS、MMS 等） | 短信 | 升级会员：解锁高级权限 |
| 00011 | 从 URI 查询数据（SMS、CALLLOGS） | 短信<br>通话记录<br>信息收集 | 升级会员：解锁高级权限 |
| 00191 | 获取短信收件箱中的消息 | 短信 | 升级会员：解锁高级权限 |
| 00162 | 创建 InetSocketAddress 对象并连接到它 | socket | 升级会员：解锁高级权限 |

| | | | |
|---|---|---|---|
| 00163 | 创建新的 Socket 并连接到它 | socket | 升级会员：解锁高级权限 |
| 00063 | 隐式意图（查看网页、拨打电话等） | 控制 | 升级会员：解锁高级权限 |
| 00051 | 通过setData隐式意图（查看网页、拨打电话等） | 控制 | 升级会员：解锁高级权限 |
| 00036 | 从 res/raw 目录获取资源文件 | 反射 | 升级会员：解锁高级权限 |
| 00192 | 获取短信收件箱中的消息 | 短信 | 升级会员：解锁高级权限 |
| 00091 | 从广播中检索数据 | 信息收集 | 升级会员：解锁高级权限 |
| 00160 | 使用辅助服务执行通过视图 ID 获取节点信息的操作 | 无障碍服务 | 升级会员：解锁高级权限 |
| 00161 | 对可访问性节点信息执行可访问性服务操作 | 无障碍服务 | 升级会员：解锁高级权限 |
| 00159 | 使用辅助服务执行通过文本获取节点信息的操作 | 无障碍服务 | 升级会员：解锁高级权限 |
| 00168 | 使用辅助服务执行全局操作，通过文本获取节点信息 | 无障碍服务 | 升级会员：解锁高级权限 |
| 00169 | 使用辅助服务执行全局操作，通过视图 ID 获取节点信息 | 无障碍服务 | 升级会员：解锁高级权限 |
| 00173 | 获取 AccessibilityNodeInfo 屏幕中的边界并执行操作 | 无障碍服务 | 升级会员：解锁高级权限 |
| 00096 | 连接到 URL 并设置请求方法 | 命令<br>网络 | 升级会员：解锁高级权限 |
| 00123 | 连接到远程服务器后将响应保存为 JSON | 网络<br>命令 | 升级会员：解锁高级权限 |
| 00089 | 连接到 URL 并接收来自服务器的输入流 | 命令<br>网络 | 升级会员：解锁高级权限 |
| 00030 | 通过给定的 URL 连接到远程服务器 | 网络 | 升级会员：解锁高级权限 |
| 00109 | 连接到 URL 并获取响应代码 | 网络<br>命令 | 升级会员：解锁高级权限 |
| 00094 | 连接到 URL 并从中读取数据 | 命令<br>网络 | 升级会员：解锁高级权限 |
| 00108 | 从给定的 URL 读取输入流 | 网络<br>命令 | 升级会员：解锁高级权限 |
| 00148 | 创建到给定主机地址的套接字连接 | 网络<br>命令 | 升级会员：解锁高级权限 |
| 00018 | 准备好 JSON 对象并填充位置信息 | 位置<br>信息收集 | 升级会员：解锁高级权限 |
| 00137 | 获取设备的最后已知位置 | 位置<br>信息收集 | 升级会员：解锁高级权限 |
| 00113 | 获取位置并将其放入 JSON | 信息收集<br>位置 | 升级会员：解锁高级权限 |
| 00172 | 检查管理员权限以（可能）获取它们 | admin | 升级会员：解锁高级权限 |
| 00202 | 打电话 | 控制 | 升级会员：解锁高级权限 |
| 00203 | 将电话号码放入意图中 | 控制 | 升级会员：解锁高级权限 |

| | | | |
|---|---|---|---|
| 00055 | 查询短信内容及电话号码来源 | 短信<br>信息收集 | 升级会员：解锁高级权限 |
| 00048 | 查询短信内容 | 短信<br>信息收集 | 升级会员：解锁高级权限 |
| 00049 | 查询短信发送者的电话号码 | 短信<br>信息收集 | 升级会员：解锁高级权限 |
| 00015 | 将缓冲流（数据）放入 JSON 对象 | 文件 | 升级会员：解锁高级权限 |
| 00005 | 获取文件的绝对路径并将其放入 JSON 对象 | 文件 | 升级会员：解锁高级权限 |
| 00012 | 读取数据并放入缓冲流 | 文件 | 升级会员：解锁高级权限 |
| 00128 | 查询用户账户信息 | 信息收集<br>账号 | 升级会员：解锁高级权限 |
| 00002 | 打开相机并拍照 | 相机 | 升级会员：解锁高级权限 |
| 00183 | 获取当前相机参数并更改设置 | 相机 | 升级会员：解锁高级权限 |
| 00001 | 初始化位图对象并将数据（例如JPEG）压缩为位图对象 | 相机 | 升级会员：解锁高级权限 |

## 敏感权限滥用分析

| 类型 | 匹配 | 权限 |
|---|---|---|
| 恶意软件常用权限 | 16/30 | android.permission.CAMERA<br>android.permission.READ_SMS<br>android.permission.SEND_SMS<br>android.permission.RECEIVE_SMS<br>android.permission.READ_PHONE_STATE<br>android.permission.READ_CALL_LOG<br>android.permission.CALL_PHONE<br>android.permission.MODIFY_AUDIO_SETTINGS<br>android.permission.ACCESS_COARSE_LOCATION<br>android.permission.READ_CONTACTS<br>android.permission.WRITE_CONTACTS<br>android.permission.GET_ACCOUNTS<br>android.permission.WAKE_LOCK<br>android.permission.RECEIVE_BOOT_COMPLETED<br>android.permission.SYSTEM_ALERT_WINDOW<br>android.permission.GET_TASKS |
| 其它常用权限 | 7/46 | android.permission.FOREGROUND_SERVICE<br>android.permission.WRITE_EXTERNAL_STORAGE<br>android.permission.READ_EXTERNAL_STORAGE<br>android.permission.INTERNET<br>android.permission.ACCESS_NETWORK_STATE<br>android.permission.ACCESS_WIFI_STATE<br>android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS |

常用: 已知恶意软件经常滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

## 恶意域名威胁检测

| 域名 | 状态 | 中国境内 | 位置信息 |
| --- | --- | --- | --- |
| api.whatsapp.com | 安全 | 否 | **IP地址:** 31.13.70.49<br>**国家:** 美国<br>**地区:** 加利福尼亚<br>**城市:** 洛杉矶<br>**纬度:** 34.052570<br>**经度:** -118.243904<br>**查看:** Google 地图 |

## URL 链接安全分析

| URL信息 | 源码文件 |
| --- | --- |
| • https://api.whatsapp.com/send?phone= | x2/c.java |
| • https://passwords.google.com<br>• https://myaccount.google.com<br>• https://pay.google.com<br>• https://accounts.google.com/_/lookup/accountlookup<br>• https://mail.google.com<br>• https://accounts.google.com/_/signin/challenge<br>• https://ads.google.com<br>• https://accounts.google.com/signin/v2/identifier | com/fafozixafigexi/dotejeku/gijucenotosa/vubo/lavozisuvovono.java |
| • http://176.65.144.237:3434 | f17/g.java |

## 第三方 SDK 组件分析

| SDK名称 | 开发者 | 描述信息 |
| --- | --- | --- |
| Jetpack WorkManager | Google | 使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。 |
| Jetpack Room | Google | Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。 |

## 邮箱地址敏感信息提取

| EMAIL | 源码文件 |
| --- | --- |
| this@jage.apply | com/fafozixafigexi/dotejeku/jage.java |

## 敏感凭证泄露检测

| 可能的密钥 |
| --- |
| bc1ql34xd8yntv3m4kwaf8jqeth0p4fxkxg673vlf |
| qwertyuiopasdfghjklzxcvbnm1234567890 |
| 3Cf7d4A8D30035Af83058371f0C6D4369B5024Ca |
| 8aff2efc47fafe870c738f727dfcfc6e |

| |
|---|
| 258EAFA5-E914-47DA-95CA-C5AB0DC85B11 |
| cf029002fffdcadf079e8d0a1c9a70ac |

## 免责声明及风险提示: