南明离火
移动应用检测平台

# ANDROID 静态分析报告

永不言弃!! • v3.3

分析日期: 2025-04-08 10:14:31

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

# 应用概览

| | |
|---|---|
| 文件名称: | 永不言弃!! v3.3.apk |
| 文件大小: | 35.16MB |
| 应用名称: | 永不言弃!! |
| 软件包名: | com.invictus.impossiball |
| 主活动: | .MainActivity |
| 版本号: | 3.3 |
| 最小SDK: | 10 |
| 目标SDK: | 21 |
| 加固信息: | 未加壳 |
| 开发框架: | Java/Kotlin |
| 应用程序安全分数: | 49/100 (中风险) |
| 跟踪器检测: | 4/432 |
| 杀软检测: | 17 个杀毒软件报毒 |
| MD5: | c066e1f2684c1f861cb2b880e809d5dc |
| SHA1: | b4b625513eb5272228846e5e564b68ec38aa3cad |
| SHA256: | 77870068c1358a1[illegible]df9823b0dfdc486c2c[illegible]d1f1bbd33b6b863299eb6f0 |

# 分析结果严重性分布

| 高危 | 中危 | 信息 | 安全 | 关注 |
|---|---|---|---|---|
| 3 | 16 | 1 | 2 | 0 |

# 四大组件导出状态统计

| |
|---|
| Activity组件：10个，其中export的有： 1个 |
| Service组件：6个，其中export的有： 1个 |
| Receiver组件：1个，其中export的有： 1个 |
| Provider组件：0个，其中export的有： 0个 |

# 应用签名证书信息

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

二进制文件已签名
v1 签名: True
v2 签名: False
v3 签名: False
v4 签名: False
主题: C=hello, ST=朝阳区, L=北京, O=东品西尚, OU=东品西尚, CN=姜振
签名算法: rsassa_pkcs1v15
有效期自: 2012-07-17 01:08:59+00:00
有效期至: 2067-04-20 01:08:59+00:00
发行人: C=hello, ST=朝阳区, L=北京, O=东品西尚, OU=东品西尚, CN=姜振
序列号: 0x13ab6e32
哈希算法: sha256
证书MD5: fb155e14be697bb4bd735f30676cf5db
证书SHA1: 2cf827a5d003bc0bf2f8ec25cb8b7404af1b57eb
证书SHA256: 2e7b77d54ffdb0effba85728abac470d76701e3751f9d4fcd49e4950c2681703
证书SHA512:
d6d4237cebe4dbf6097a07ca18781d6257cb705d1ce79407b70ce731677bb0b62dce3b409cfdacfe7a9ee65b246384eb4730116[illegible]f2c781629f2df8c225b77f0

找到 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.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.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.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.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.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.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.RECORD_AUDIO | 危险 | 获取录音权限 | 允许应用程序获取录音权限。 |
| android.permission.SYSTEM_OVERLAY_WINDOW | 未知 | 未知权限 | 来自 android 引用的未知权限。 |
| 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.MOUNT_UNMOUNT_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序装载和卸载可移动存储器的文件系统。 |
| android.permission.VIBRATE | 普通 | 控制振动器 | 允许应用程序控制振动器，用于消息通知振动功能。 |
| android.permission.CHANGE_NETWORK_STATE | 危险 | 改变网络连通性 | 允许应用程序改变网络连通性。 |
| 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.CHANGE_WIFI_STATE | 危险 | 改变Wi-Fi状态 | 允许应用程序改变Wi-Fi状态。 |
| 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。 |

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

| | | | |
|---|---|---|---|
| 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.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.READ_LOGS | 危险 | 读取系统日志文件 | 允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。 |
| android.permission.ACCESS_FINE_LOCATION | 危险 | 获取精确位置 | 通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。 |
| 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.WRITE_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。 |
| android.permission.ACCESS_DOWNLOAD_MANAGER | 签名(系统) | 访问下载管理器 | 这个权限是允许应用访问下载管理器，以便管理大型下载操作。 |
| android.permission.DOWNLOAD_WITHOUT_NOTIFICATION | 普通 | 后台下载文件 | 这个权限是允许应用通过下载管理器下载文件，且不对用户进行任何提示。 |
| 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.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。 |
| com.android.launcher.permission.INSTALL_SHORTCUT | 签名 | 创建快捷方式 | 这个权限是允许应用程序创建桌面快捷方式。 |
| com.xiaomi.sdk.permission.PAYMENT | 未知 | 未知权限 | 来自 android 引用的未知权限。 |
| com.android.vending.BILLING | 普通 | 应用程序具有应用内购买 | 允许应用程序从 Google Play 进行应用内购买。 |
| android.permission.CHANGE_WIFI_MULTICAST_STATE | 危险 | 允许接收WLAN多播 | 允许应用程序接收并非直接向您的设备发送的数据包。这样在查找附近提供的服务时很有用。这种操作所耗电量大于非多播模式。 |
| android.permission.GET_PACKAGE_SIZE | 普通 | 测量应用程序空间大小 | 允许一个程序获取任何package占用空间容量。 |
| 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。 |

## 可浏览 Activity 组件分析

| ACTIVITY | INTENT |
|---|---|
| com.wandoujia.standalone_sdk.StandAloneSdkActivity | Schemes: wdj://,<br>Hosts: \ 100042086, |

## 网络通信安全风险分析

本报告由南明离火移动安全分析平台生成

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

## 证书安全合规分析

高危: **1** | 警告: **0** | 信息: **1**

| 标题 | 严重程度 | 描述信息 |
|---|---|---|
| 已签名应用 | 信息 | 应用程序使用代码签名证书进行签名 |
| 应用程序容易受到 Janus 漏洞的影响 | 高危 | 应用程序使用 v1 签名方案进行签名，如果仅使用 v1 签名方案进行签名，则在 Android 5.0-8.0 上容易受到 Janus 漏洞的影响。在使用 v1 和 v2/v3 方案签名的 Android 5.0-7.0 上运行的应用程序也容易受到攻击。 |

## Manifest 配置安全分析

高危: **0** | 警告: **4** | 信息: **0** | 屏蔽: **0**

| 序号 | 问题 | 严重程度 | 描述信息 |
|---|---|---|---|
| 1 | 应用程序数据存在被泄露的风险<br>未设置[android:allowBackup]标志 | 警告 | 这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。 |
| 2 | Activity (com.wandoujia.standalone_sdk.StandAloneSdkActivity) 未被保护。<br>存在一个intent-filter。 | 警告 | 发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。 |
| 3 | Broadcast Receiver (com.wandoujia.standalone_sdk.BootReceiverWrapper) 未被保护。<br>存在一个intent-filter。 | 警告 | 发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。 |
| 4 | Service (com.ehoo.post.EhooPostService) 未被保护。<br>存在一个intent-filter。 | 警告 | 发现 Service与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Service是显式导出的。 |

## 代码安全漏洞检测

高危: **2** | 警告: **10** | 信息: **1** | 安全: **2** | 屏蔽: **0**

| 序号 | 问题 | 等级 | 参考标准 | 文件位置 |
|---|---|---|---|---|
| 1 | MD5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 |
| 2 | 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 |

本报告由南明离火移动安全分析平台生成

| | | | | |
|---|---|---|---|---|
| 3 | 应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据 | 警告 | CWE: CWE-276: 默认权限不正确<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | 升级会员：解锁高级权限 |
| 4 | 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 |
| 5 | 此应用程序可能具有Root检测功能 | 安全 | OWASP MASVS: MSTG-RESILIENCE-1 | 升级会员：解锁高级权限 |
| 6 | 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 |
| 7 | 启用了调试配置。生产版本不能是可调试的 | 高危 | CWE: CWE-919: 移动应用程序中的弱点<br>OWASP Top 10: M1: Improper Platform Usage<br>OWASP MASVS: MSTG-RESILIENCE-2 | 升级会员：解锁高级权限 |
| 8 | 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 |
| 9 | 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 |
| 10 | 应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。 | 高危 | CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-3 | 升级会员：解锁高级权限 |
| 11 | 可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息 | 警告 | CWE: CWE-200: 信息泄露<br>OWASP Top 10: M1: Improper Platform Usage<br>OWASP MASVS: MSTG-PLATFORM-7 | 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
本报告由南明离火移动安全分析平台生成

| | | | | |
|---|---|---|---|---|
| 12 | 应用程序创建临时文件。敏感信息永远不应该被写进临时文件 | 警告 | CWE: CWE-276: 默认权限不正确<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | 升级会员：解锁高级权限 |
| 13 | 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 |
| 14 | IP地址泄露 | 警告 | CWE: CWE-200: 信息泄露<br>OWASP MASVS: MSTG-CODE-2 | 升级会员：解锁高级权限 |
| 15 | 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 |

## Native 库安全加固检测

| 序号 | 动态库 | NX(堆栈禁止执行) | PIE | STACK CANARY(栈保护) | RELRO | RPATH（指定SO搜索路径） | RUNPATH（指定SO搜索路径） | FORTIFY(常用函数加强检查) | SYMBOLS STRIPPED(裁剪符号表) |
|---|---|---|---|---|---|---|---|---|---|

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | arm64-v8a/libwdj_adnetwork.so | True<br>info<br>二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。 | 动态共享对象 (DSO)<br>info<br>共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。 | True<br>info<br>这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出 | Full RELRO<br>info<br>此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。 | None<br>info<br>二进制文件没有设置运行时搜索路径或 RPATH | None<br>info<br>二进制文件没有设置 RUNPATH | False<br>warning<br>二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用。 | True<br>info<br>符号被剥离 |

## 应用行为分析

| 编号 | 行为 | 标签 | 文件 |
|---|---|---|---|
| 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 |
| 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 |
| 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 |
| 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 |
| 00010 | 读取敏感数据（SMS、CALLLOG）并将其放入 JSON 对象中 | 短信<br>通话记录<br>信息收集 | 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 |
| 00013 | 读取文件并将其放入流中 | 文件 | 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 |

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

| | | | |
|---|---|---|---|
| 00062 | 查询WiFi信息和WiFi Mac地址 | WiFi<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 |
| 00033 | 查询IMEI号 | 信息收集 | 升级会员：解锁高级权限 |
| 00082 | 获取当前WiFi MAC地址 | 信息收集<br>WiFi | 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 |
| 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 |
| 00031 | 检查当前正在运行的应用程序列表 | 反射<br>信息收集 | 升级会员：解锁高级权限 |
| 00134 | 获取当前WiFi IP地址 | WiFi<br>信息收集 | 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 |
| 00121 | 创建目录 | 文件<br>命令 | 升级会员：解锁高级权限 |
| 00175 | 获取通知管理器并取消通知 | 通知 | 升级会员：解锁高级权限 |
| 00125 | 检查给定的文件路径是否存在 | 文件 | 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 |
| 00012 | 读取数据并放入缓冲流 | 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 |
| 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 |
| 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 |
| 00038 | 查询电话号码 | 信息收集 | 升级会员：解锁高级权限 |
| 00067 | 查询IMSI号码 | 信息收集 | 升级会员：解锁高级权限 |
| 00083 | 查询IMEI号 | 信息收集<br>电话服务 | 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 |
| 00035 | 查询已安装的包列表 | 反射 | 升级会员：解锁高级权限 |
| 00054 | 从文件安装其他APK | 反射 | 升级会员：解锁高级权限 |
| 00076 | 获取当前WiFi信息并放入JSON中 | 信息收集<br>WiFi | 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
本报告由南明离火移动安全分析平台生成

| | | | |
|---|---|---|---|
| 00072 | 将 HTTP 输入流写入文件 | 命令<br>网络<br>文件 | 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 | 13/30 | android.permission.READ_PHONE_STATE<br>android.permission.SYSTEM_ALERT_WINDOW<br>android.permission.RECORD_AUDIO<br>android.permission.VIBRATE<br>android.permission.READ_CONTACTS<br>android.permission.WAKE_LOCK<br>android.permission.SEND_SMS<br>android.permission.ACCESS_FINE_LOCATION<br>android.permission.RECEIVE_BOOT_COMPLETED<br>android.permission.WRITE_SETTINGS<br>android.permission.GET_TASKS<br>android.permission.ACCESS_COARSE_LOCATION<br>android.permission.CALL_PHONE |
| 其它常用权限 | 8/46 | android.permission.ACCESS_NETWORK_STATE<br>android.permission.INTERNET<br>android.permission.ACCESS_WIFI_STATE<br>android.permission.WRITE_EXTERNAL_STORAGE<br>android.permission.READ_EXTERNAL_STORAGE<br>android.permission.CHANGE_NETWORK_STATE<br>android.permission.CHANGE_WIFI_STATE<br>com.android.launcher.permission.INSTALL_SHORTCUT |

常用: 已知恶意软件广泛滥用的权限。

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 |
|---|---|---|---|
| l.supfast.net | 安全 | 否 | No Geolocation information available. |
| upgrade.wandoujia.com | 安全 | 否 | No Geolocation information available. |
| ssp.tadseeker.com | 安全 | 否 | No Geolocation information available. |
| ads.supfast.net | 安全 | 否 | No Geolocation information available. |

## URL 链接安全分析

| URL信息 | 源码文件 |
|---|---|
| • http://yunpan.cn/cVMcyzjutr5RN<br>• http://yunpan.cn/cVMLQJWZbcqFW<br>• http://www.ascendercorp.com/<br>• http://scripts.sil.org/OFL<br>• http://www.ascendercorp.com/typedesigners.html | 自研引擎-A |

本报告由南明离火移动安全分析平台生成

| | |
|---|---|
| • https://upgrade.wandoujia.com/event<br>• https://upgrade.wandoujia.com/upgrade<br>• 1.0.0.1 | com/wandoujia/standalone_api/upgrade/SilentUpdate.java |
| • http://ads.supfast.net/network/v2/init | com/wandoujia/ads/sdk/requests/f.java |
| • http://l.supfast.net/muce/data/sink?profile=%1$s&vc=%2$s&vn=%3$s&gzip=true&encrypt=true&key_version=2 | com/wandoujia/ads/sdk/legacy/log/h.java |
| • http://ads.supfast.net/network/v3/app/list | com/wandoujia/ads/sdk/requests/a.java |
| • http://ssp.tadseeker.com/jssdk/ssp/video/getad.do<br>• http://ssp.tadseeker.com/jssdk/ssp/video/validateishavevideo.do | utils/Constant.java |

## 第三方 SDK 组件分析

| SDK名称 | 开发者 | 描述信息 |
|---|---|---|
| File Provider | Android | FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file://Uri 以促进安全分享与应用程序关联的文件。 |

## 第三方追踪器检测

| 名称 | 类别 | 网址 |
|---|---|---|
| Google AdMob | Advertisement | https://reports.exodus-privacy.eu.org/trackers/312 |
| IAB Open Measurement | Advertisement, Identification | https://reports.exodus-privacy.eu.org/trackers/328 |
| Tencent Stats | Analytics | https://reports.exodus-privacy.eu.org/trackers/116 |
| Umeng Analytics | | https://reports.exodus-privacy.eu.org/trackers/119 |

## 敏感凭证泄露检测

| 可能的密钥 |
|---|
| "chartboost_unity_app_id" : "4f7b433509b6025804000002" |
| 0627f71ad446f8ec327be42ab1a92c73 |
| 6X8Y4XdM2Vhvn0KfzcEatGnWaNU= |
| 961453575460764ca5bc4a3ebc089e44 |
| 1e05e0e27b804482b24a6132d81f27a2 |
| b543e392e2f8470d3a9342ec08dc02a5 |
| fe9285eacf37c951e1f8d54666721835 |
| qSX538Vb4hDkQ2sFtrbANWQTkCjzckKa |
| 07a25f16f6e4437aba3c705a61b84534 |

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

本报告仅用于学习与研究目的，禁止用于任何商业或非法用途。 

| |
|---|
| 3C1A0B7D67EAAACB9BCEAC7309F6A739 |
| 071e0c8e08802e19c807b1d579804c86 |

## 免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐隐患。

© 2025 南明离火 - 移动安全分析平台自动生成

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成