南明离火
移动应用检测平台

ANDROID 静态分析报告

医路轻松 • v1.1.3

分析日期: 2025-10-10 14:30:49

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:	base.apk
文件大小:	53.16MB
应用名称:	医路轻松
软件包名:	com.qshealth.ylqs
主活动:	com.qshealth.qsdoctor.MainActivity
版本号:	1.1.3
最小SDK:	24
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	41/100 (中风险)
跟踪器检测:	1/432
杀软检测:	AI评估：安全
MD5:	f5b3e5d21fc958e535d5dea4e6f5a30c
SHA1:	15ccd7d4d96ad53dfbefe0c74024cb8795b5e940
SHA256:	b28f3a205af2643[illegible]7caa889b3a6462f8ea5c59ce016645e92d20d16d7fb

分析结果严重性分布

高危	中危	信息	安全	关注
4	11	2	1	0

四大组件导出状态统计

Activity组件：3个，其中export的有： 0个
Service组件：1个，其中export的有： 0个
Receiver组件：1个，其中export的有： 1个
Provider组件：3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

APK已签名
v1 签名: False
v2 签名: True
v3 签名: False
v4 签名: False
主题: CN=qs, OU=qs, O=qs, L=bj, ST=bj, C=86
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-15 07:55:59+00:00
有效期至: 2050-04-09 07:55:59+00:00
发行人: CN=qs, OU=qs, O=qs, L=bj, ST=bj, C=86
序列号: 0x1
哈希算法: sha256
证书MD5: 3fdee54f4cf7507281631378df85d355
证书SHA1: d59f342b20806e6c66b3fa17ff261142e553dd03
证书SHA256: 3f86265a5f00e0d65158ce97ff2ea8638224415f344c81d8b127956a720a184f
证书SHA512:
923ddd80511155b7353989f470d41cfc7d5c80261cac372070ffb8d9fd8b334081012ecd7517815337dd12b2595f0ee147a6f7db94e30f3a5e78f0aa34b3901c

公钥算法: rsa
密钥长度: 2048
指纹: f42a38cbf04fef6bab2a57ceb935d29088c0c9f91c232367f02618a5e0c6649d
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看到的图像。
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.READ_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
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.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.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.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。
com.qshealthylqs.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
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_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。

可浏览 Activity 组件分析

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

ACTIVITY	INTENT
com.qshealth.qsdoctor.MainActivity	Schemes: qsdoctor://, https://, Hosts: qshealth.com, qsdoctor.qshealth.com, Path Prefixes: /app/distributeDoctor,

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: **1** | 警告: **2** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	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。
2	App 链接 assetlinks.json 文件未找到 [android:name=com.qshealth.qsdoctor.MainActivity] [android:host=https://qsdoctor.qshealth.com]	高危	App Link 资产验证 URL（https://qsdoctor.qshealth.com/.well-known/assetlinks.json）未找到或配置不正确。（状态码：404）。应用程序链接允许用户通过 Web URL 或电子邮件直接跳转到移动应用。如果 assetlinks.json 文件缺失或主机/域配置错误，恶意应用可劫持此类 URL，导致网络钓鱼攻击，泄露 URI 中的敏感信息（如 PII、OAuth 令牌、魔术链接/重置令牌等）。请务必通过托管 assetlinks.json 文件并在 Activity 的 intent-filter 中设置 [android:autoVerify="true"] 来完成 App Link 域名验证。
3	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限的保护级别。 Permission: android.permission.DUMP [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。

代码安全漏洞检测

高危: **3** | 警告: **7** | 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 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	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

2	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 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
3	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 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限
4	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 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
5	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
6	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 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
7	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 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
8	已启用远程WebView调试	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
9	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 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	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 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-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
本报告由南明离火移动安全分析平台生成

11	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'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
12	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
13	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 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	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/libmediapipe_tasks_vision_jni.so	True info 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) info 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 info 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 info 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 info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	True info 二进制文件有以下加固函数: ['__strchr_chk', '__vsnprintf_chk', '__strlen_chk', '__memcpy_chk', '__strncat_chk', '__read_chk']	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
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
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
00013	读取文件并将其放入流中	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
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
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
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00028	从assets目录中读取文件	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	5/30	android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.READ_PHONE_STATE

本报告由南明离火移动安全分析平台生成

其它常用权限	5/46	android.permission.READ_MEDIA_IMAGES android.permission.READ_EXTERNAL_STORAGE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE

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
stackoverflow.com	安全	否	**IP地址:** 141.250.176.14 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
api-ai-face.qingsongchou.com	安全	是	**IP地址:** 103.107.36.27 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.274085 **经度:** 120.15507 **查看:** 高德地图
journeyapps.com	安全	否	**IP地址:** 216.137.39.95 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
api-med.duoerehospital.com	安全	是	**IP地址:** 47.96.196.217 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.274085 **经度:** 120.15507 **查看:** 高德地图
files-center.qschou.com	安全	是	**IP地址:** 61.147.216.44 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图

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

www.tensorflow.org	安全	否	**IP地址:** 142.250.176.14 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.386051 **经度:** -122.083847 **查看:** Google 地图
test-api-med.qschou.com	安全	是	**IP地址:** 47.99.106.214 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.274085 **经度:** 120.15507 **查看:** 高德地图
test-api-ai-face.qingsongchou.com	安全	是	**IP地址:** 47.99.106.214 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.274085 **经度:** 120.15507 **查看:** 高德地图
qsdoctor.qshealth.com	安全	是	**IP地址:** 47.110.12.15 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.274085 **经度:** 120.15507 **查看:** 高德地图
beian.miit.gov.cn	安全	是	**IP地址:** 27.155.113.108 **国家:** 中国 **地区:** 福建 **城市:** 福州市 **纬度:** 26.099774 **经度:** 119.302249 **查看:** 高德地图
developer.android.google.cn	安全	否	**IP地址:** 142.250.189.3 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
api-med.qschou.com	安全	是	**IP地址:** 203.107.36.27 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.274085 **经度:** 120.15507 **查看:** 高德地图
health.qschou.com	安全	是	**IP地址:** 47.96.195.219 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.274085 **经度:** 120.15507 **查看:** 高德地图

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

test-api-health.duoerehospital.com	安全	是	**IP地址:** 36.103.228.17 **国家:** 中国 **地区:** 宁夏 **城市:** 银川 **纬度:** 38.487194 **经度:** 106.230909 **查看:** 高德地图
sensors-data.qingsongchou.com	安全	是	**IP地址:** 116.62.65.169 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.274085 **经度:** 120.15507 **查看:** 高德地图
centerapi.qschou.com	安全	是	**IP地址:** 47.96.196.217 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.274085 **经度:** 120.15507 **查看:** 高德地图
m.qshealth.com	安全	是	**IP地址:** 47.110.12.15 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.274085 **经度:** 120.15507 **查看:** 高德地图
api-health.duoerehospital.com	安全	是	**IP地址:** 47.96.196.217 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.274085 **经度:** 120.15507 **查看:** 高德地图
test-api-med.duoerehospital.com	安全	是	**IP地址:** 47.99.106.214 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.274085 **经度:** 120.15507 **查看:** 高德地图

URL链接安全分析

URL信息	源码文件
• https://qsdoctor.qshealth.com/newAgreement?code=a5b3996628944e2a9354868d1ee517a1Q&amp • https://qsdoctor.qshealth.com/newAgreement?code=b43df6e249a64b5cb490fddf59d93f62Q&amp • https://www.baidu.com • https://p0.meituan.net/merchantpic/3da8c4c4032075aba58c600a5907c3392260342.jpg%40watermark%3D0	自研引擎-A

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

• https://groups.google.com/d/msg/guava-announce/zhztfg7yf3o/rqnnwdheewaj • https://stackoverflow.com/q/5189914/28465	autovalue/shaded/com/google$/common/base/C$Platform.java
• http://health.qschou.com	com/qshealth/qsdoctor/repo/remote/params/TokenPlusParams.java
• https://m.qshealth.com/doctor-app/journal/list • https://m.qshealth.com/doctor-app/medical-tools/science-articles?content_type=1 • https://m.qshealth.com/doctor-app/medical-tools/science-articles?content_type=2	com/qshealth/qsdoctor/widgets/DialogsKt.java
• https://m.qshealth.com/doctor-app/agent-qs/medical-research • https://m.qshealth.com/doctor-app/agent-qs/doc-interpret-assistant	com/qshealth/qsdoctor/feature/home/HomePageKt.java
• https://sensors-data.qingsongchou.com/sa?project=production	com/qshealth/qsdoctor/App.java
• https://files-center.qschou.com/yljk_jkmall/20241218/df994f28e14047b0a7adae29579cb338 • https://files-center.qschou.com/yljk_jkmall/20241218/d59727aa6b14a13f2d79344e47ee813f • https://qsdoctor.qshealth.com/static/img-empty.40b101af.png • https://qsdoctor.qshealth.com/media/interview?id= • https://files-center.qschou.com/yljk_jkmall/20241218/bf7a7f1ea957b83e05a3d83a0db8f28a • https://files-center.qschou.com/yljk_jkmall/20241218/0063bb260854334f2dd4fda71fa97b41 • https://qsdoctor.qshealth.com/media/video?id=	com/qshealth/qsdoctor/feature/workbench/WorkPageKt.java
• https://beian.miit.gov.cn/#/integrated/index • https://qsdoctor.qshealth.com/my/agreementlist • https://qsdoctor.qshealth.com/newagreement?code= • https://qsdoctor.qshealth.com/newagreement?code=da82e6e3b6964a7eb2434e96ba7aa9b&title= 第三方共享清单 • https://qsdoctor.qshealth.com/account	com/qshealth/qsdoctor/feature/me/SettingPageKt.java
• https://centerapi.qschou.com	com/qshealth/qsdoctor/repo/remote/ApiCenter.java
• https://m.qshealth.com/doctor-app/journal/list • https://m.qshealth.com/doctor-app/medical-tools/science-articles?content_type=1 • https://m.qshealth.com/doctor-app/agent-qs/medical-research • https://m.qshealth.com/doctor-app/agent-qs/doc-interpret-assistant • https://m.qshealth.com/doctor-app/science-article/list • https://m.qshealth.com/doctor-app/medical-tools/science-articles?content_type=2	com/qshealth/qsdoctor/repo/remote/model/ToolBoxRespKt.java
• https://m.qshealth.com/doctor-app/agent-qs/medical-research • https://m.qshealth.com/doctor-app/medical-tools/science-articles?content_type=1 • https://m.qshealth.com/doctor-app/agent-qs/doc-interpret-assistant	com/qshealth/qsdoctor/feature/index/IndexVm.java
• https://developer.android.google.cn/static/develop/ui/compose/images/graphics-roundedcorners.png?hl=zh-cn	com/qshealth/qsdoctor/feature/videotask/task/widgets/ViewSecionsKt.java
• https://www.baidu.com/img/pctm_d9c8750bed0b3c7d089fa7d55720d6cf.png	com/duoerehospital/devideotool/widgets/PhotoViewKt.java
• https://groups.google.com/d/msg/guava-announce/zhztfg7yf3o/rqnnwdheewaj • https://stackoverflow.com/q/5189914/28465	autovalue/shaded/com/google$/common/collect/C$Platform.java
• https://api-med.qschou.com • https://test-api-med.qschou.com	com/qshealth/qsdoctor/repo/remote/ApiMedQs.java
• https://api-med.duoerehospital.com • https://test-api-med.duoerehospital.com	com/qshealth/qsdoctor/repo/remote/ApiMed.java

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

• https://api-health.duoerehospital.com • https://qsdoctor.qshealth.com/media/article?id= • https://test-api-health.duoerehospital.com	com/qshealth/qsdoctor/repo/remote/ApiHealth.java
• https://api-ai-face.qingsongchou.com/ • https://test-api-ai-face.qingsongchou.com/	com/qshealth/qsdoctor/repo/remote/ApiFace.java
• https://qsdoctor.qshealth.com/newagreement?code=a5b3996628944e2a9354868d1ee517a1&title=%e5%8c%bb%e7%94%9f%e6%b3%a8%e5%86%8c%e5%8d%8f%e8%ae%ae-%e5%8c%bb%e7%96%97 • https://qsdoctor.qshealth.com/newagreement?code=b43df6e249a64b5cb490fddf59d93f62&title=%e8%bd%bb%e6%9d%be%e5%8c%bb%e6%82%a3%e6%95%b0%e5%ad%97%e5%8c%96%e6%9c%8d%e5%8a%a1%e5%b9%b3%e5%8f%b0%e9%9a%90%e7%a7%81%e6%94%bf%e7%ad%96-%e5%8c%bb%e7%96%97	com/qshealth/qsdoctor/repo/remote/ApiKt.java
• https://github.com/journeyapps/zxing-android-embedded • https://journeyapps.com/	自研引擎-S
• data::bounding_box • data::relative_bounding_box • https://www.tensorflow.org/lite/guide/ops_custom • file:line • https://www.tensorflow.org/lite/guide/ops_select	lib/arm64-v8a/libmediapipe_tasks_vision_jni.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Jetpack Camera	Google	CameraX 是 Jetpack 的新增库。利用该库，可以更轻松地向应用添加相机功能。该库提供了很多兼容性修复程序和备选方法，有助于在众多设备上打造一致的开发者体验。
ZXing Android Embedded	JourneyApps	Barcode scanning library for Android, using ZXing for decoding.
神策分析 SDK	神策	神策分析，是针对企业级客户推出的深度用户行为分析产品，支持私有化部署，客户端、服务器、业务数据、第三方数据的全端采集和建模，驱动营销渠道效果评估、用户精细化运营改进、产品功能及用户体验优化、老板看板辅助管理决策、产品个性化推荐改造、用户标签体系构建等应用场景。作为 PaaS 平台支持二次开发，可通过 BI、大数据平台、CRM、ERP 等内部 IT 系统，构建用户数据体系，让用户行为数据发挥深远价值。
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。
Jetpack App Startup	Google	App Startup 库提供了一种直接，高效的方法来在应用程序启动时初始化组件。库开发人员和应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).

第三方追踪器检测

名称	类别	网址
Sensors Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/248

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

敏感凭证泄露检测

可能的密钥
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"library_zxingandroidembedded_author" : "JourneyApps"
0063bb260854334f2dd4fda71fa97b41
da82e6e3b6964a7eb2434ee96ba7aa9b
7e95a0b5e6a848189586d6cca9d66482
145780b0fef2ae266c665fa4b10cc0df8e41d293
e02a9beb3ddc477db22f9888a6c87150
b43df6e249a64b5cb490fddf59d93f62
bf7a7f1ea957b83e05a3d83a0db8f28a
d59727aa6b14a13f2d79344e47ee813f
a5b3996628944e2a9354868d1ee517a1
d9c8750bed0b3c7d089fa7d55720d6cf
df994f28e14047b0a7adae29579cb338

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