南明离火
移动应用检测平台

ANDROID 静态分析报告

星界云手机 v1.7.6

分析日期: 2025-07-07 14:33:52

应用概览

文件名称:	XingJie-V1.7.6_chinac.apk
文件大小:	75.63MB
应用名称:	星界云手机
软件包名:	com.chinac.mobile
主活动:	com.huayun.cloud.MapActivity
版本号:	1.7.6
最小SDK:	24
目标SDK:	35
加固信息:	未加壳
开发框架:	Flutter
应用程序安全分数:	50/100 (中风险)
跟踪器检测:	4/432
杀软检测:	恶意软件
MD5:	6d256c291d68b600506120eb04fcbaed
SHA1:	91fd093d14f0457cec0421dd97f8ffd3a8ad2360
SHA256:	7fca0f416e38a735b6555c70b6a7956a9265dbbc3bf71fcf533f92ce72e30ca

恶意软件家族情报

恶意家族	开通会员，查看恶意软件家族归属
描述信息	升级会员：解锁高级权限
C2服务器	升级会员：解锁高级权限
凭证数据	升级会员：解锁高级权限
关联情报	升级会员：解锁高级权限

分析结果严重性分布

高危	中危	信息	安全	关注
1	34	2	1	0

四大组件导出状态统计

Activity组件：19个，其中export的有： 9个
Service组件：24个，其中export的有： 7个
Receiver组件：14个，其中export的有： 3个
Provider组件：8个，其中export的有： 1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=86, ST=fujian, L=xiamen, O=Huayun, OU=Huayun, CN=Huayun
签名算法: rsassa_pkcs1v15
有效期自: 2021-04-26 08:26:52+00:00
有效期至: 2046-04-20 08:26:52+00:00
发行人: C=86, ST=fujian, L=xiamen, O=Huayun, OU=Huayun, CN=Huayun
序列号: 0x2ea15d9d
哈希算法: sha256
证书MD5: 64dfea20697866befff13ed1d153e402
证书SHA1: aa9365076a8f74cd85139c7247dc13fc1dca6a8e
证书SHA256: 998651a4aeb3cbaf9c9047d3c59d7b5696dbd876f664d15ab74f0fa1edd562c0
证书SHA512:
a2eb852ee238d02251dc6888820bdf00e76cf5b34f1c20faa11e07187550afac0e2c9e50170afe1d679d30c5d46cc58ad2d3fae8179acddbb8e4ba9acad99302

公钥算法: rsa
密钥长度: 2048
指纹: 6327131740b9f6175c6bb4145dad76fa96f2a...a6209ade06af071bfe82980473
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.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后台进程仍然运行。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。

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.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.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。
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.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.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.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.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.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.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。
com.chinac.mobile.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
android.permission.BROADCAST_PACKAGE_ADDED	签名	接收新增APP的通知	它允许一个应用程序接收到其他应用程序添加新包（即新安装的可执行文件）的广播消息。
android.permission.BROADCAST_PACKAGE_CHANGED	签名	接收APP变化的通知	它允许一个应用程序接收到其他应用程序变化（安装、卸载、修改）的广播消息。
android.permission.BROADCAST_PACKAGE_INSTALL	签名	接收APP安装的通知	它允许一个应用程序接收到其他应用程序安装新包（即新安装的可执行文件）的广播消息。
android.permission.BROADCAST_PACKAGE_REPLACED	签名	接收APP替换的通知	它允许一个应用程序接收到其他应用程序被覆盖安装的广播消息。
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。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	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。
com.vivo.notification.permission.BADGE_ICON	普通	桌面图标角标	vivo平台桌面图标角标，接入vivo平台后需要用户手动开启，开启完成后收到新消息时，在已安装的应用桌面图标右上角显示“数字角标”。
android.permission.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。

本报告由南明离火移动安全分析平台生成

com.chinac.mobile.permission.PROCESS_PUSH_MSG	未知	未知权限	来自 android 引用的未知权限。
com.chinac.mobile.permission.PUSH_PROVIDER	未知	未知权限	来自 android 引用的未知权限。
com.meizu.flyme.push.permission.RECEIVE	普通	魅族push服务权限	魅族push服务权限。
com.chinac.mobile.push.permission.MESSAGE	未知	未知权限	来自 android 引用的未知权限。
com.meizu.c2dm.permission.RECEIVE	普通	魅族push服务权限	魅族push服务权限。
com.chinac.mobile.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	普通	OPPO推送服务	OPPO推送服务正常工作所必需的，它允许应用接收来自OPPO推送系统的消息。
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	普通	OPPO推送服务	OPPO推送服务正常工作所必需的，它允许应用接收来自OPPO推送系统的消息。
com.chinac.mobile.permission.MIPUSH_RECEIVE	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.huayun.cloud.MapActivity	Schemes: chinac://, Hosts: www.chinac.com, Path Prefixes: /
com.tencent.tauth.AuthActivity	Schemes: tencent1111820426://,

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: **0** | 警告: **24** | 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，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	应用已配置网络安全策略 [android:networkSecurityConfig=@7F0F0003]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。
3	Activity (com.tencent.tauth.AuthActivity) 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。
4	Broadcast Receiver (com.dexterous.flutterlocalnotifications.ScheduledNotificationReceiver) 未受保护。 [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。
5	Activity (com.journeyapps.barcodescanner.CaptureActivity) 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。
6	Activity (com.huawei.hms.hmsscankit.ScanKitActivity) 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。
7	Service (com.heytap.msp.push.service.CompatibleDataMessageCallbackService) 受权限保护，但应检查权限保护级别。 Permission: com.coloros.mcs.permission.SEND_MCS_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。
8	Service (com.heytap.msp.push.service.DataMessageCallbackService) 受权限保护，但应检查权限保护级别。 Permission: com.heytap.mcs.permission.SEND_PUSH_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。
9	Broadcast Receiver (org.android.agoo.vivo.PushMessageReceiverImpl) 未受保护。 [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。
10	Service (com.xiaomi.push.service.XMPushService) 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。

11	Broadcast Receiver (com.huawei.hms.support.api.push.PushMsgReceiver) 受权限保护。 Permission: com.chinac.mobile.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	检测到 Broadcast Receiver 已导出，但受权限保护。
12	Broadcast Receiver (com.huawei.hms.support.api.push.PushReceiver) 受权限保护。 Permission: com.chinac.mobile.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	检测到 Broadcast Receiver 已导出，但受权限保护。
13	Activity 设置了 TaskAffinity 属性 (com.jarvan.fluwx.wxapi.FluwxWXEntryActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
14	Activity 设置了 TaskAffinity 属性 (com.chinac.mobile.wxapi.WXEntryActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
15	Activity-Alias (com.chinac.mobile.wxapi.WXEntryActivity) 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-Alias (com.chinac.mobile.wxapi.WXPayEntryActivity) 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。
17	Activity (com.alipay.sdk.app.PayResultActivity) 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。
18	Activity (com.alipay.sdk.app.AlipayResultActivity) 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。
19	Activity 设置了 TaskAffinity 属性 (com.umeng.message.notify.UHuaMessageNotifyActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
20	Activity-Alias (com.umeng.message.UMessageNotifyActivity) 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。

21	Service (com.huawei.hms.support.api.push.service.HmsMsgService) 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。
22	Content Provider (com.huawei.hms.support.api.push.PushProvider) 未受保护。 [android:exported=true]	警告	检测到 Content Provider 已导出，未受任何权限保护，任意应用均可访问。
23	Service (com.meizu.cloud.pushsdk.NotificationService) 受权限保护，但应检查权限保护级别。 Permission: com.meizu.cloud.push.permission.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。
24	Service (com.vivo.push.sdk.service.CommandClientService) 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。
25	Broadcast Receiver (org.android.agoo.xiaomi.MiPushBroadcastReceiver) 未受保护。 [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。
26	Service (com.xiaomi.mipush.sdk.PushMessageHandler) 受权限保护，但应检查权限保护级别。 Permission: com.xiaomi.xmsf.permission.MIPUSH_RECEIVE [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。
27	Activity (com.xiaomi.mipush.sdk.NotificationClickedActivity) 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。

代码安全漏洞检测

高危: **1** | 警告: **8** | 信息: **2** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置

1	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 OWASP Top 10: M5: Insufficient Cryptography 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 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
3	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
4	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
5	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
6	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
7	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
8	此应用侦听剪贴板更改。一些恶意软件也会监听剪贴板更改	信息	OWASP MASVS: MSTG-PLATFORM-4	升级会员：解锁高级权限

9	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
10	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'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限
11	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)

1	arm64-v8a/libapp.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	Not Applicable info RELRO 检查不适用于 Flutter/Dart 二进制文件	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	False info 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 info 符号被剥离
2	arm64-v8a/libmsoptimize.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。	False high 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项 -fstack-protector-all 来启用栈哨兵。该对于 Dart/Flutter 库不适用，除非使用了 Dart FFI	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	False warning 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 info 符号被剥离

3	arm64-v8a/libtnet-3.1.14.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: ['__strrchr_chk', '__strlen_chk', '__sprintf_chk', '__strchr_chk', '__strcpy_chk']	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00056	修改语音音量	控制	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
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
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
00208	捕获设备屏幕的内容	信息收集 屏幕	升级会员：解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	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 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 命令	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
00065	获取SIM卡提供商的国家代码	信息收集	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
00036	从 res/raw 目录获取资源文件	反射	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 信息收集	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
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00083	查询IMEI号	信息收集 电话服务	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
00046	方法反射	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
00094	连接到 URL 并从中读取数据	命令 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 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
00102	将手机扬声器设置为打开	命令	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	8/30	android.permission.WAKE_LOCK android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.REQUEST_INSTALL_PACKAGES android.permission.MODIFY_AUDIO_SETTINGS android.permission.VIBRATE android.permission.READ_PHONE_STATE android.permission.GET_TASKS

其它常用权限	7/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_NETWORK_STATE android.permission.ACCESS_WIFI_STATE com.google.android.gms.permission.AD_ID

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
journeyapps.com	安全	否	**IP地址:** 216.137.39.6 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243304 **查看:** Google 地图
api-push.in.meizu.com	安全	否	**IP地址:** 206.161.233.191 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 赫恩登 **纬度:** 38.978210 **经度:** -77.386993 **查看:** Google 地图
api.flutter.dev	安全	否	**IP地址:** 199.36.158.100 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://api-push.in.meizu.com/garcia/api/client/	com/meizu/f0/a.java
• https://journeyapps.com/ • https://github.com/journeyapps/zxing-android-embedded	自研引擎-S
• https://api.flutter.dev/flutter/material/scaffold/of.html	lib/arm64-v8a/libapp.so

Firebase 配置安全检测

标题	严重程度	描述信息

Firebase远程配置已禁用	安全	Firebase远程配置URL（ https://firebaseremoteconfig.googleapis.com/v1/projects/849923563846/namespaces/firebase:fetch?key=AIzaSyCLUKRoymfxsASIeNOOMcE6PHYpKNnJfe0 ）已禁用。响应内容如下所示：
		{
		"state": "NO_TEMPLATE"
		}

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Flutter	Google	Flutter 是谷歌的移动 UI 框架，可以快速在 iOS 和 Android 上构建高质量的原生用户界面。
Bugly	Tencent	腾讯 Bugly，为移动开发者提供专业的异常上报和运营统计，帮助开发者快速发现并解决异常，同时掌握产品运营动态，及时跟进用户反馈。
岳鹰全景监控	Alibaba	岳鹰全景监控，是阿里 UC 官方出品的先进移动应用线上监控平台，为多家知名企业提供服务。
WebRTC	WebRTC	借助 WebRTC，您可以在基于开放标准的应用程序中添加实时通信功能。它支持在同级之间发送视频，语音和通用数据，从而使开发人员能够构建功能强大的语音和视频通信解决方案。该技术可在所有现代浏览器以及所有主要平台的本机客户端上使用。WebRTC 背后的技术被实现为一个开放的 Web 标准，并在所有主要浏览器中均以常规 JavaScript API 的形式提供。
HMS Scan Kit	Huawei	统一扫码服务（Scan Kit）提供便捷的条形码和二维码扫描、解析、生成能力，帮助您快速构建应用内的扫码功能。得益于华为在计算机视觉领域能力的积累，Scan Kit 可以实现远距离码或小型码的检测和自动放大，同时针对常见复杂扫码场景（如反光、暗光、污损、模糊、柱面）做了针对性识别优化，提升扫码成功率与用户体验。Scan Kit 支持 Android 和 iOS 系统集成。其中，Android 系统集成 Scan Kit 后支持横屏扫码能力。
移动统计分析	Umeng	U-App 作为一款专业、免费的移动统计分析产品。在日常业务中帮您解决多种数据相关问题，如数据采集与管理、业务监测、用户行为分析、App 稳定性监控及实现多种运营方案等。助力互联网企业充分挖掘用户行为数据价值，找到产品更新迭代方向，实现精细化运营，全面提升业务增长效能。
支付宝 SDK	Alipay	支付宝开放平台基于支付宝海量用户，将强大的支付、营销、数据能力，通过接口等形式开放给第三方合作伙伴，帮助第三方合作伙伴创建更具竞争力的应用。
HMS Core	Huawei	HMS Core 是华为终端云服务提供的端、云开放能力的合集，助您高效构建精品应用。
Huawei Push	Huawei	华为推送服务（HUAWEI Push Kit）是华为为开发者提供的消息推送平台，建立了从云端到终端的消息推送通道。开发者通过集成 HUAWEI Push Kit 可以实时推送消息到用户终端应用，构筑良好的用户关系，提升用户的感知度和活跃度。
ZXing Android Embedded	JourneyApps	Barcode scanning library for Android, using ZXing for decoding.
腾讯开放平台	Tencent	腾讯核心内部服务，二十年技术沉淀，助你成就更高梦想。
友盟推送	Umeng	基于友盟+全域数据建立精准的消息推送平台，为开发者提供更灵活、更智能、更有效的消息推送方案，有效提升用户粘性，提高 App 活跃度。

本报告由南明离火移动安全分析平台生成

vivo Push	vivo	vivo 推送是 Funtouch OS 上系统级消息推送平台，帮助开发者在 vivo 平台有效提升活跃和留存。通过和系统的深度结合，建立稳定可靠、安全可控、高性能的消息推送服务，帮助不同行业的开发者挖掘更多的运营价值。
MiPush	Xiaomi	小米消息推送服务在 MIUI 上为系统级通道，并且全平台通用，可以为开发者提供稳定、可靠、高效的推送服务。
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。
AppGallery Connect	Huawei	为开发者提供移动应用全生命周期服务，覆盖全终端全场景，降低开发成本，提升运营效率，助力商业成功。
HMS Core AAID	Huawei	华为推送服务开放能力合集提供的匿名设备标识(AAID) 实体类与令牌实体类包。异步方式获取的 AAID 与令牌通过此包中对应的类承载返回。
HMS ML Kit	Huawei	机器学习服务（ML Kit）提供机器学习套件，为开发者使用机器学习能力开发各类应用，提供优质体验。得益于华为长期技术积累，ML Kit 为开发者提供简单易用、服务多样、技术领先的机器学习能力，助力开发者更快更好地开发各类 AI 应用。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Meizu Push	Meizu	魅族推送服务是由魅族公司为开发者提供的消息推送服务，开发者可以向集成了魅族 push SDK 的客户端实时地推送通知或者消息，与用户保持互动，提高活跃率。
OPPO Push	OPPO	OPPO PUSH 是 ColorOS 上的系统级通道，为开发者提供稳定，高效的消息推送服务。

第三方追踪器检测

名称	类别	网址
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
Huawei Mobile Services (HMS) Core	Location, Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/333
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119
Yueying Crash SDK	Analytics, Crash reporting	https://reports.exodus-privacy.eu.org/trackers/448

敏感凭证泄露检测

可能的密钥
vivo推送的=> "com.vivo.push.api_key" : "91b1f10cbc76ef76ba7d229ba5483b61"
百度地图的=> "com.baidu.lbsapi.API_KEY" : "PbcrgNxt7iP5iZya2uy4B6wtolLtOegP"
vivo推送的=> "com.vivo.push.app_id" : "105479843"
华为HMS Core 应用ID的=> "com.huawei.hms.client.appid" : "appid=104195759"
凭证信息=> "BUGLY_APP_ID" : "cdcd900ce7"
凭证信息=> "UMENG_APP_ID" : "605b119674e00260862b74cd"

vivo推送的=> "local_iv" : "MzMsMzQsMzUsMzYsMzcsMzgsMzksNDAsNDEsMzIsMzgsMzcsMzYsMzUsMzQsMzMsI0AzNCwzMiwzMywzNywzMywzNCwzMiwzMywzMywzMywzNCw0MSwzNSwzNSwzMiwzMiwjQDMzLDM0LDM1LDM2LDM3LDM4LDM5LDQwLDQxLDMyLDM4LDM3LDMzLDM1LDM0LDMzLCNAMzQsMzIsMzMsMzMsMzcsMzMsMzQsMzQsMzIsMzMsMzMsMzMsMzMsMzQsNDEsMzUsMzIsMzIsMzI"
"security_public_key" : "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8hzUojzHX8jDL+97pqr7CaLiKSsZ0aOES7FUcX7vh9PoEDbCKNCTakRXdS5EiurPk3QpvsAGbfyIs7JWKm4py9KcIdJsZRh9onknVeAVlU++jnrGFGEYfQb8iKzClN059gYeeJBs9mwi7RGU9tj0KHUG659v5sMBxv7zNse3fJQIDAQAB"
"google_app_id" : "1:849923563846:android:8b8c13e3252caac0d64547"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"library_zxingandroidembedded_author" : "JourneyApps"
"google_crash_reporting_api_key" : "AIzaSyCLUKRoymfxsASIeNOOMcE6PHYpKNnJfe0"
"google_api_key" : "AIzaSyCLUKRoymfxsASIeNOOMcE6PHYpKNnJfe0"
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
0781a33309574092a44e6888b070d188
dab05edbc68a9d7c0ab47be476de0d5e
4a2ca769d79f4856bb3bd982d30de790
426ac0b9ede24a4c85a56d024cd3f2b7
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
605b119674e00260862b74cd
a54da332f3f44f0980e104d87edde0ec

免责声明及风险提示