



ANDROID 静态分析报告



巨甄 • v4.1.7

分析日期: 2024-05-19 21:49:59

i应用概览

文件名称:	1716103335464148471.apk
文件大小:	69.16MB
应用名称:	佢甄
软件包名:	hkangc.hkangcliaoshiduiejiqun.hkangc
主活动:	com.wind.im.MainActivity
版本号:	4.1.7
加固信息:	未加壳
应用程序安全分数:	45/100 (中风险)
跟踪器检测:	3/432
杀软检测:	AI评估: 很危险, 请谨慎安装
MD5:	13af429c29589ae37a1e54573ef8da44
SHA1:	a8b1957c3885dcbb9723e4d2455df41898dfa373
SHA256:	b58f09b5cf353b7acc92c652777d707d9b778384b1ad45c1f54bd1925c719459

分析结果严重性分布

高危	中危	信息	安全	关注
5	34	2	1	0

四大组件导出状态统计

Activity组件: 106个, 其中export的有: 3个
Service组件: 10个, 其中export的有: 7个
Receiver组件: 11个, 其中export的有: 11个
Provider组件: 10个, 其中export的有: 0个

应用签名证书信息

二进制文件已签名

v1 签名: True

v2 签名: True

v3 签名: True

v4 签名: False

主题: C=CN, ST=InTJ, L=qg00, O=sfaN, OU=AltM, CN=BLZ3

签名算法: rsassa_pkcs1v15

有效期自: 2024-05-16 15:01:48+00:00
 有效期至: 2051-10-02 15:01:48+00:00
 发行人: C=CN, ST=InTJ, L=qg00, O=sfaN, OU=AltM, CN=BLZ3
 序列号: 0x2f555aad
 哈希算法: sha256
 证书MD5: 1bf51fbab70449fe1115c09eeb3ebc36
 证书SHA1: 4a8f753acddaa299bce8e5d4d494d2a5897c38a8
 证书SHA256: cd8298b5b82a0d76e8c247deedc602c323a41099aab997552e7fc9774eacc76c
 证书SHA512:
 6fcc780951b95592504f21edb7d353dd91013b9ae0a5f5bae6e9acd39935875701c5e53c5c07736869d5e49803d7b13c7d46658316db7c6b8da522448f47a618

公钥算法: rsa
 密钥长度: 2048
 指纹: 5031cb0e85a36bfaaaa74b4fe958fddaaf22e0e6ed15ad72668ef951883efd15
 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.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.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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.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_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.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.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.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.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.RESTART_PACKAGES	普通	重启进程	允许程序自己重启或重启其他程序
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.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.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.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 <code>Service.startForeground</code> ，用于podcast播放（推送悬浮播放、锁屏播放）
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
com.heytao.mcs.permission.RECIEVE_MCS_MESSAGE	未知	未知权限	来自 android 引用的未知权限
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。
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.SYSTEM_OVERLAY_WINDOW	未知	未知权限	来自 android 引用的未知权限
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 <code>Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS</code> 的权限	应用程序必须拥有权限才能使用 <code>Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS</code> 。
hkangc.hkangcliaoshiduiejiqu.hkangc.permission.MIPUSH_RECEIVE	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。
hkangc.hkangcliaoshiduiejiqu.hkangc.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。
hkangc.hkangcliaoshiduiejiqu.hkangc.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
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错略的经纬度信息，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.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_LOCATION_EXTRA_COMMANDS	普通	访问定位额外命令	访问额外位置提供程序命令，恶意应用程序可能会使用它来干扰GPS或其他位置源的操作。
android.permission.ACCESS_BACKGROUND_LOCATION	危险	获取后台定位权限	允许应用程序访问后台位置。如果您正在请求此权限，则还必须请求ACCESS_COARSE_LOCATION或ACCESS_FINE_LOCATION。单独请求此权限不会授予您位置访问权限。
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。

com.meizu.flyme.permission.PUSH	未知	未知权限	来自 android 引用的未知权限。
hkangc.hkangc!aoshiduiejiqun.hkangc.permission.PROCESS_PUSH_MSG	未知	未知权限	来自 android 引用的未知权限。
hkangc.hkangc!aoshiduiejiqun.hkangc.permission.PUSH_PROVIDER	未知	未知权限	来自 android 引用的未知权限。
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。
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	未知权限	来自 android 引用的未知权限。
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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯

可浏览 Activity 组件分析

ACTIVITY	INTENT
	Schemes: 0x7f1200e9://,

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: 1 | 信息: 1

标题	严重程度	描述信息
已签名应用	信息	应用程序已使用代理签名证书进行签名

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	应用程序具有网络安全配置 [android:networkSecurityConfig=0x7f150003]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
2	应用程序数据存在被泄露的风险 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。
3	Activity () 未被保护。 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。

4	Activity设置了TaskAffinity属性 ()	警告	如果设置了 taskAffinity, 其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息, 请始终使用默认设置, 将 affinity 保持为包名
5	Service () 未被保护。 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。
6	Service () 未被保护。 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。
7	Broadcast Receiver (com.wind.im.push.receiver.VivoPushMessageReceiverImpl) 未被保护。 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。
8	Broadcast Receiver (com.xiaomi.push.service.receivers.NetworkStatusReceiver) 未被保护。 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。
9	Broadcast Receiver (com.xiaomi.push.service.receivers.PingReceiver) 未被保护。 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。
10	Broadcast Receiver (com.wind.im.push.receiver.XiaomiPushMessageReceiver) 未被保护。 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。
11	Service () 未被保护。 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。
12	Broadcast Receiver (com.wind.im.push.receiver.MeizuPushServerMsgReceiver) 未被保护。 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。
13	Service () 未被保护。 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。
14	Service () 未被保护。 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。
15	Broadcast Receiver (com.taobao.accs.EventReceiver) 未被保护。 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。
16	Broadcast Receiver (com.taobao.accs.ServiceReceiver) 未被保护。 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。
17	Service () 未被保护。 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。

18	Broadcast Receiver (com.tao bao.agoo.AgooCommondReceiver) 未被保护。 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。
19	Activity () 未被保护。 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。
20	Activity () 未被保护。 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。
21	Activity设置了TaskAffinity属性 ()	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
22	Broadcast Receiver (com.me izu.cloud.pushsdk.MzPushSystemReceiver) 未被保护。 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。
23	Broadcast Receiver (com.huawei.hms.support.api.push.PushMsgReceiver) 未被保护。 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。
24	Broadcast Receiver (com.huawei.hms.support.api.push.PushReceiver) 未被保护。 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。
25	Service () 未被保护。 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: 5 | 警告: 8 | 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
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	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任应用输入可能会导致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

4	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
5	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
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 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限
7	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
8	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	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
10	不安全的WebView实现。WebView忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
11	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
12	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

13	此应用程序可能会请求root（超级用户）权限	警告	CWE: CWE-250: 以不必要的权限执行 OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
14	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
15	SSL的不安全实现。信任所有证书或接受自签名证书是一个关键的安全漏洞。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
16	WebView域控制不严格漏洞	高危	CWE: CWE-73: 外部控制文件名或路径	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 CANNARY(栈保护)	RELRO	PATH (指定SO搜索路径)	RUNPATH (指定SO搜索路径)	FORTIFY(常用函数加强检查)	SYMBOL STRIPPED (裁剪符号表)
----	-----	------------	-----	--------------------	-------	-----------------	--------------------	-------------------	-------------------------

1	arm64-v8a/libcf-msc.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。		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。	No ne info 二进制文件没有设置运行时搜索路径或RPATH	N o n e i n f o 二进制文件没有设置RUNPATH	True info 二进制文件有以下加固函数:['_strle_n_chk','__strcpy_chk','__memcpy_chk','__memset_chk','__vsprintf_chk','__strcat_chk','__strncat_chk','__FD_SET_chk','__FD_ISSET_chk','__vsnprintf_chk','__memmove_chk','__read_chk','__strchr_chk','__strcpy_chk','__FD_CLR_chk','__strchr_chk']	Fa ls e w ar ni ng 符号可用
2	arm64-v8a/librtmp-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。		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。	No ne info 二进制文件没有设置运行时搜索路径或RPATH	N o n e i n f o 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	Fa ls e w ar ni ng 符号可用

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。	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。	No ne info 二进制文件没有设置运行时搜索路径或 RPATH	N o n e 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', '__strlen_chk', '__sprintf_chk', '__strchr_chk', '__strcpy_chk']	Fa ls e w a r n i n g 符 号 可 用
---	-----------------------------	--	---	---	--	--	--	---

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.VIBRATE android.permission.RECORD_AUDIO android.permission.CAMERA android.permission.READ_PHONE_STATE android.permission.GET_TASKS android.permission.MANAGE_AUDIO_SETTINGS android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED android.permission.SYSTEM_ALERT_WINDOW android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.READ_CONTACTS android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	12/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.FOREGROUND_SERVICE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.ACCESS_BACKGROUND_LOCATION android.permission.FLASHLIGHT

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
material.io	安全	否	IP地址: 216.239.32.21 国家: 美利坚合众国 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://material.io/design/components/dialogs.html#actions	com/afodestad/materialdialogs/MaterialDialog.java
127.0.0.1 - http://%s:%d/%s	com/danikula/videocache/HttpProxyCacheServer.java
http://%s:%d/%s	com/danikula/videocache/Pinger.java
javascript:document.body.innerHTML=	com/imacapp/home/web/KitWebViewClient.java
- https://graph.qq.com/ - https://api.weixin.qq.com/	com/imacapp/wind/api/LoginService.java
- http://www.baidu.com:8925 - https://67.211.78.206:7788/ 223.75.236.241 221.228.32.13 182.43.124.6 127.0.0.1	com/wind/im/BuildConfig.java
http://www.baidu.com:8925	com/wind/im/WindApp.java
http://%s:%s/api/exclude/siteconfig/servers	com/wind/imlib/bean/ServerBucket.java
1.2.3.4 127.0.0.1 1.3.101.110 1.3.101.111 18.244.0.188 140.205.122.6 1.2.0.4 1.3.101.113 151.232.21.132 43.231.234.23 1.3.101.112	lib/arm64-v8a/libcf-msc.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。

C++ 共享库	Android	在 Android 应用中运行原生代码。
IJKPlayer	Bilibili	IJKPlayer 是一款基于 FFmpeg 的轻量级 Android/iOS 视频播放器，具有 API 易于集成、编译配置可裁剪、支持硬件加速解码、DanmakuFlameMaster 架构清晰、简单易用等优势。
MMKV	Tencent	MMKV 是基于 mmap 内存映射的 key-value 组件，底层序列化/反序列化使用 protobuf 实现，性能高，稳定性强。

🔍 第三方追踪器检测

名称	类别	网址
AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
Huawei Mobile Services (HMS) Core	Analytics, Advertisement, Location	https://reports.exodus-privacy.eu.org/trackers/333

🔑 敏感凭证泄露检测

可能的密钥
f3423b38048b29b9e7bfec5c73e51ca1
d54bd5ac75afabf91078e5295c9df199
55e92a2be29cc6f1ea4d146fb9e6045d

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工具，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