南明离火
移动应用检测平台

ANDROID 静态分析报告

管控平台 • v5.2.3.0.

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

分析日期: 2025-08-27 12:17:23

应用概览

文件名称:	管控平台无加固.apk
文件大小:	11.68MB
应用名称:	管控平台
软件包名:	com.iflytek.mdmservice
主活动:	com.iflytek.mdmservice.ui.MainActivity
版本号:	5.2.3.0.
最小SDK:	23
目标SDK:	23
加固信息:	未加壳
开发框架:	Java/Kotlin
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:	7367e44bab21c5d3b1960ceb7555a28e
SHA1:	9f2cc56e95d8e38e85fda8040c9ccb57c154df6
SHA256:	b0b556809de1580e7d6a4890f8bc37995057406ce534733072d68cf9da75b2

分析结果严重性分布

高危	中危	信息	安全	关注
10	76	3	2	0

四大组件导出状态统计

Activity组件：14个，其中export的有： 2个
Service组件：54个，其中export的有： 6个
Receiver组件：53个，其中export的有： 39个
Provider组件：15个，其中export的有： 13个

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

应用签名证书信息

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: C=CN, ST=Hubei, L=Wuhan, O=iflytek, OU=iflytek, CN=iflytek
签名算法: rsassa_pkcs1v15
有效期自: 2018-05-10 01:16:37+00:00
有效期至: 2043-05-04 01:16:37+00:00
发行人: C=CN, ST=Hubei, L=Wuhan, O=iflytek, OU=iflytek, CN=iflytek
序列号: 0x6e450692
哈希算法: sha256
证书MD5: e849a7ead4939671f84e453de415b805
证书SHA1: 589ce1c284e4d46350f7ce1bccff494ac1639cb4
证书SHA256: a3b3d6c649fd8e2ebda9418bbc66ecd6f09ddbe9fcb695f65c030c4806a6fdf9
证书SHA512:
ce542f6b311e404196e8b67e7398337fab50b7c19a0e01f76d78e56a12e4a350e48241b8a445e8945b500fb28bb2b0b8d214e00b77a5f7[illegible]56ac92d8d5c00fc7

公钥算法: rsa
密钥长度: 2048
指纹: 1d6e43e3cca92e3767abc0aaa05ba459ed3983857e99c6b4d53d2b3eeb6096f2
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.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
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_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.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.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.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.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.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）

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.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.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.CONTROL_ALWAYS_ON_VPN	未知	未知权限	来自 android 引用的未知权限。
android.permission.READ_PRIVILEGED_PHONE_STATE	签名(系统)	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.PACKAGE_USAGE_STATS	签名	更新组件使用统计	允许修改组件使用情况统计
android.permission.SET_TIME	签名(系统)	设置时间	允许应用程序更改手机的时间。
android.permission.SET_TIME_ZONE	危险	设置时区	允许应用程序设置时区。
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.WRITE_SECURE_SETTINGS	签名(系统)	修改安全系统设置	允许应用程序修改系统的安全设置数据。普通应用程序不能使用此权限。
com.android.launcher.permission.READ_SETTINGS	危险	读取桌面快捷方式	这种权限的作用是允许应用读取桌面快捷方式的设置。
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.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.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。
com.iflytek.mdm.permission.download	未知	未知权限	来自 android 引用的未知权限。
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.BATTERY_STATS	普通	修改电池统计	允许对手机电池统计信息进行修改
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。
andorid.permission.CHANGE_CONFIGURATION	未知	未知权限	来自 android 引用的未知权限。
android.permission.BIND_ACCESSIBILITY_SERVICE	签名	AccessibilityServices 需要进行系统绑定	必须由 AccessibilityService要求，以确保只有系统可以绑定到它。
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。

本报告由南明离火移动安全分析平台生成

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.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.CHANGE_COMPONENT_ENABLED_STATE	签名(系统)	启用或禁用应用程序组件	允许应用程序更改是否启用其他应用程序的组件。恶意应用程序可借此停用重要的手机功能。使用此权限时务必谨慎，因为这可能导致应用程序组件进入不可用、不一致或不稳定的状态。
com.iflytek.mdmadmin.provider.read	未知	未知权限	来自 android 引用的未知权限。
com.iflytek.mdmadmin.provider.write	未知	未知权限	来自 android 引用的未知权限。
com.iflytek.mdmstore.provider.read	未知	未知权限	来自 android 引用的未知权限。
com.iflytek.mdmstore.provider.write	未知	未知权限	来自 android 引用的未知权限。
com.iflytek.mdm.permission.FIX_API	未知	未知权限	来自 android 引用的未知权限。
com.iflytek.mdmservice.provider.write	未知	未知权限	来自 android 引用的未知权限。
com.iflytek.mdmservice.provider.read	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.MDM	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.MDM_SDCARD	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.MDM_BLUETOOTH	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.SDK_LAUNCHER	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.MDM_CONNECTIVITY	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.MDM_WIFI	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.MDM_NETWORK_MANAGER	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.MDM_PHONE	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.MDM_CAMERA	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.MDM_LOCATION	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.MDM_TELEPHONY	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.MDM_MMS	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.MDM_UPDATESTATE_MANAGER	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.MDM_PHONE_MANAGER	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.MDM_NFC	未知	未知权限	来自 android 引用的未知权限。

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

com.huawei.permission.sec.MDM_USB	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.MDM_CAPTURE_SCREEN	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.MDM_APP_MANAGEMENT	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.MDM_SETTINGS_RESTRICTION	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.MDM_VPN	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.MDM_DEVICE_OWNER	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.MDM_DEVICE_MANAGER	未知	未知权限	来自 android 引用的未知权限。
com.huawei.permission.sec.MDM_KEYGUARD	未知	未知权限	来自 android 引用的未知权限。
com.huawei.systemmanager.permission.ACCESS_INTERFACE	未知	未知权限	来自 android 引用的未知权限。
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.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.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
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。
getui.permission.GetuiService.com.iflytek.mdmservice	未知	未知权限	来自 android 引用的未知权限。
android.permission.REAL_GET_TASKS	未知	未知权限	来自 android 引用的未知权限。
com.iflytek.mdmservice.provider.readonly	未知	未知权限	来自 android 引用的未知权限。
android.permission.SCHEDULE_EXACT_ALARM	普通	精确的闹钟权限	允许应用程序使用准确的警报 API。
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”。

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

本报告由南明离火移动安全分析平台生成

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	应用已使用代码签名证书进行签名。

Manifest 配置安全分析

高危: **7** | 警告: **65** | 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	Content Provider (com.iflytek.mdmservice.provider.FrozenAppProvider) 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。
3	Activity（com.iflytek.mdmservice.ui.ShowActivity）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（23）升级至 28 及以上以获得平台级防护。
4	Activity 设置了 TaskAffinity 属性 (com.iflytek.mdmservice.ui.LockActivity)	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）。
5	Activity（com.iflytek.mdmservice.ui.LockActivity）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（23）升级至 28 及以上以获得平台级防护。
6	Activity（com.iflytek.mdmservice.ui.BatteryActivity）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（23） 升级至 28 及以上以获得平台级防护。
7	Activity (com.iflytek.mdmservice.ui.BatteryActivity) 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（23）升级至 29 及以上，从平台层面修复该漏洞。
8	Activity (com.iflytek.mdmservice.ui.BatteryActivity) 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。
9	Service (com.iflytek.mdmservice.service.BackgroundService) 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。

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

10	Service (com.iflytek.mdmservice.service.MdmApiService) 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	Service (com.iflytek.mdmservice.service.MdmSdkService) 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。
12	Broadcast Receiver (com.iflytek.mdmservice.receiver.AdminReceiver) 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。
13	Broadcast Receiver (com.iflytek.mdmservice.receiver.EduClassReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
14	Broadcast Receiver (com.iflytek.mdmservice.receiver.MdmCameraReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.iflytek.mdm.permission.CALL_API protectionLevel: normal [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受权限保护，但该权限保护级别为 normal。恶意应用可申请此权限并与组件交互。建议将权限保护级别设为 signature，仅允许同证书签名应用访问。
15	Broadcast Receiver (com.iflytek.mdmservice.receiver.MdmUsbStateReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.iflytek.mdm.permission.CALL_API protectionLevel: normal [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受权限保护，但该权限保护级别为 normal。恶意应用可申请此权限并与组件交互。建议将权限保护级别设为 signature，仅允许同证书签名应用访问。
16	Broadcast Receiver (com.iflytek.mdmservice.receiver.MdmGpsControlReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.iflytek.mdm.permission.CALL_API protectionLevel: normal [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受权限保护，但该权限保护级别为 normal。恶意应用可申请此权限并与组件交互。建议将权限保护级别设为 signature，仅允许同证书签名应用访问。

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

17	Broadcast Receiver (com.iflytek.mdmservice.receiver.MdmTimeSettingReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.iflytek.mdm.permission.CALL_API protectionLevel: normal [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受权限保护，但该权限保护级别为 normal。恶意应用可申请此权限并与组件交互。建议将权限保护级别设为 signature，仅允许同证书签名应用访问。
18	Broadcast Receiver (com.iflytek.mdmservice.receiver.MdmBluetoothReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.iflytek.mdm.permission.CALL_API protectionLevel: normal [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受权限保护，但该权限保护级别为 normal。恶意应用可申请此权限并与组件交互。建议将权限保护级别设为 signature，仅允许同证书签名应用访问。
19	Broadcast Receiver (com.iflytek.mdmservice.receiver.MdmStoreDownloadFlagReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.iflytek.mdm.permission.CALL_API protectionLevel: normal [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受权限保护，但该权限保护级别为 normal。恶意应用可申请此权限并与组件交互。建议将权限保护级别设为 signature，仅允许同证书签名应用访问。
20	Broadcast Receiver (com.iflytek.mdmservice.receiver.MdmWhiteUrlReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.iflytek.mdm.permission.CALL_API protectionLevel: normal [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受权限保护，但该权限保护级别为 normal。恶意应用可申请此权限并与组件交互。建议将权限保护级别设为 signature，仅允许同证书签名应用访问。
21	Broadcast Receiver (com.iflytek.mdmservice.receiver.MdmPowerOffReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.iflytek.mdm.permission.CALL_API protectionLevel: normal [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受权限保护，但该权限保护级别为 normal。恶意应用可申请此权限并与组件交互。建议将权限保护级别设为 signature，仅允许同证书签名应用访问。
22	Broadcast Receiver (com.iflytek.mdmservice.receiver.MdmWifiAdvanceReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.iflytek.mdm.permission.CALL_API protectionLevel: normal [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受权限保护，但该权限保护级别为 normal。恶意应用可申请此权限并与组件交互。建议将权限保护级别设为 signature，仅允许同证书签名应用访问。

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

23	Broadcast Receiver (com.iflytek.mdmservice.receiver.MdmNavigationReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.iflytek.mdm.permission.CALL_API protectionLevel: normal [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受权限保护，但该权限保护级别为 normal。恶意应用可申请此权限并与组件交互。建议将权限保护级别设为 signature，仅允许同证书签名应用访问。
24	Broadcast Receiver (com.iflytek.mdmservice.receiver.MdmKeypadReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.iflytek.mdm.permission.CALL_API protectionLevel: normal [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受权限保护，但该权限保护级别为 normal。恶意应用可申请此权限并与组件交互。建议将权限保护级别设为 signature，仅允许同证书签名应用访问。
25	Broadcast Receiver (com.iflytek.mdmservice.receiver.MdmClearPwdReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.iflytek.mdm.permission.CALL_API protectionLevel: normal [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受权限保护，但该权限保护级别为 normal。恶意应用可申请此权限并与组件交互。建议将权限保护级别设为 signature，仅允许同证书签名应用访问。
26	Broadcast Receiver (com.iflytek.mdmservice.receiver.MdmResetFactoryReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.iflytek.mdm.permission.CALL_API protectionLevel: normal [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受权限保护，但该权限保护级别为 normal。恶意应用可申请此权限并与组件交互。建议将权限保护级别设为 signature，仅允许同证书签名应用访问。
27	Broadcast Receiver (com.iflytek.mdmservice.receiver.MdmClearAppsReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.iflytek.mdm.permission.CALL_API protectionLevel: normal [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受权限保护，但该权限保护级别为 normal。恶意应用可申请此权限并与组件交互。建议将权限保护级别设为 signature，仅允许同证书签名应用访问。
28	Broadcast Receiver (com.iflytek.mdmservice.receiver.MdmSilentInstallReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.iflytek.mdm.permission.CALL_API protectionLevel: normal [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受权限保护，但该权限保护级别为 normal。恶意应用可申请此权限并与组件交互。建议将权限保护级别设为 signature，仅允许同证书签名应用访问。

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

29	Broadcast Receiver (com.iflytek.mdmservice.receiver.MdmEyeComfortReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.iflytek.mdm.permission.CALL_API protectionLevel: normal [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受权限保护，但该权限保护级别为 normal。恶意应用可申请此权限并与组件交互。建议将权限保护级别设为 signature，仅允许同证书签名应用访问。
30	Broadcast Receiver (com.iflytek.mdmservice.receiver.MdmColorBlindnessReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.iflytek.mdm.permission.CALL_API protectionLevel: normal [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受权限保护，但该权限保护级别为 normal。恶意应用可申请此权限并与组件交互。建议将权限保护级别设为 signature，仅允许同证书签名应用访问。
31	Broadcast Receiver (com.iflytek.mdmservice.receiver.MdmEyeProtectReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.iflytek.mdm.permission.CALL_API protectionLevel: normal [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受权限保护，但该权限保护级别为 normal。恶意应用可申请此权限并与组件交互。建议将权限保护级别设为 signature，仅允许同证书签名应用访问。
32	Broadcast Receiver (com.iflytek.mdmservice.receiver.MdmResetNetworkReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.iflytek.mdm.permission.CALL_API protectionLevel: normal [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受权限保护，但该权限保护级别为 normal。恶意应用可申请此权限并与组件交互。建议将权限保护级别设为 signature，仅允许同证书签名应用访问。
33	Broadcast Receiver (com.iflytek.mdmservice.receiver.ToastReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
34	Broadcast Receiver (com.iflytek.mdmservice.receiver.TimeChangeReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
35	Broadcast Receiver (com.iflytek.mdmservice.receiver.InstallSourceControlReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.iflytek.mdm.permission.CALL_API protectionLevel: normal [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受权限保护，但该权限保护级别为 normal。恶意应用可申请此权限并与组件交互。建议将权限保护级别设为 signature，仅允许同证书签名应用访问。

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

36	Broadcast Receiver (com.iflytek.mdmservice.receiver.WakeWorkerReceiver) 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。
37	Broadcast Receiver (com.iflytek.mdmservice.receiver.OpenAdminReceiver) 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。
38	Broadcast Receiver (com.iflytek.mdmservice.receiver.EyeProtectListenerReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
39	Broadcast Receiver (com.iflytek.mdmservice.receiver.SyncTimeReceiver) 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。
40	Content Provider (com.iflytek.mdmservice.provider.PolicyProvider) 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。
41	Content Provider (com.iflytek.mdmservice.provider.PolicyTempProvider) 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。
42	Content Provider (com.iflytek.mdmservice.provider.PolicyHelperProvider) 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。
43	Content Provider (com.iflytek.mdmservice.provider.WoBListProvider) 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。
44	Content Provider (com.iflytek.mdmservice.provider.MdmProvider) 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。
45	Content Provider (com.iflytek.mdmservice.provider.AppInfoProvider) 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。

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

46	Content Provider (com.iflytek.mdmservice.provider.AlarmProvider) 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。
47	Content Provider (com.iflytek.mdmservice.provider.AppInfoOpenProvider) 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。
48	Content Provider (com.iflytek.mdmservice.provider.DeviceInfoProvider) 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。
49	Content Provider (com.iflytek.mdmservice.provider.UserInfoProvider) 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。
50	Content Provider (com.iflytek.mdmservice.provider.SystemConfigProvider) 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。
51	Broadcast Receiver (com.iflytek.mdmservice.receiver.MdmRefeshServiceData) 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。
52	Broadcast Receiver (com.iflytek.mdmservice.receiver.LaunchReceiver) 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。
53	Broadcast Receiver (com.iflytek.mdmservice.receiver.LogoutReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
54	Broadcast Receiver (com.iflytek.mdmservice.receiver.StipulationReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
55	Broadcast Receiver (com.iflytek.mdmservice.receiver.ScreenWakeLockReceiver) 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。

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

56	Activity 设置了 TaskAffinity 属性 (com.igexin.sdk.PushActivity)	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）。
57	Activity 设置了 TaskAffinity 属性 (com.igexin.sdk.GActivity)	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）。
58	Activity (com.igexin.sdk.GActivity) 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（23）升级至 29 及以上，从平台层面修复该漏洞。
59	Activity (com.igexin.sdk.GActivity) 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。
60	Broadcast Receiver (com.iflytek.mdmservice.receiver.EnvironmentSwitcherReceiver) 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。
61	Broadcast Receiver (com.iflytek.mdmservice.receiver.TrustAppReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.iflytek.mdm.permission.CALL_API protectionLevel: normal [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受权限保护，但该权限保护级别为 normal。恶意应用可申请此权限并与组件交互。建议将权限保护级别设为 signature，仅允许同证书签名应用访问。
62	Broadcast Receiver (com.iflytek.mdmservice.receiver.ShutdownReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
63	Activity（com.iflytek.mdmservice.policy.ui.WarnActivity）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（23） 升级至 28 及以上以获得平台级防护。
64	Broadcast Receiver (com.iflytek.mdmservice.receiver.AlarmReceiver) 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。
65	Broadcast Receiver (com.iflytek.mdmservice.receiver.ObserverReceiver) 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。

本报告由南明离火移动安全分析平台生成

66	Service (com.iflytek.mdmservice.service.ExportSilentInstallService) 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。
67	Activity（com.iflytek.oauth.activity.behaviorlogin.EDUBehaviorRiskWebActivity）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（23） 升级至 28 及以上以获得平台级防护。
68	Content Provider (com.iflytek.edu.log.bizbase.process.EDULogDataProvider) 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。
69	Broadcast Receiver (com.iflytek.edu.apm.base.timer.ExactTimer$TimeTaskReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式使用，存在安全风险。
70	Service (com.igexin.sdk.GService) 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。
71	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。 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。
72	高优先级 Intent（1000） - {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: **3** | 警告: **9** | 信息: **3** | 安全: **2** | 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 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
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

本报告由南明离火移动安全分析平台生成

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
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	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
7	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
8	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
9	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
10	此应用程序使用SQL Cipher。SQL Cipher为sqlite数据库文件提供256位AES加密	信息	OWASP MASVS: MSTG-CRYPTO-1	升级会员：解锁高级权限
11	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

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	此应用程序使用SQL Cipher，确保密钥没有硬编码在代码中	信息	OWASP MASVS: MSTG-CRYPTO-1	升级会员：解锁高级权限
13	使用弱加密算法	高危	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
14	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
15	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
16	不安全的Web视图实现。Web视图忽略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
17	该文件是World Writable。任何应用程序都可以写入文件	高危	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

Native 库安全加固检测

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

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	armeabi/libcsunflower.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	False warning 二进制文件没有加固函数。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

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

2	armeabi/libcwatchdog.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	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	armeabi/libzxprotect.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	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

应用行为分析

编号	行为	标签	文件
00078	获取网络运营商名称	信息收集 电话服务	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

00189	获取短信内容	短信	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
00188	获取短信地址	短信	升级会员：解锁高级权限
00011	从 URI 查询数据（SMS、CALLLOGS）	短信 通话记录 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
00200	从联系人列表中查询数据	信息收集 联系人	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 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 短信 通话记录 日历	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
00013	读取文件并将其放入流中	文件	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
00062	查询WiFi信息和WiFi Mac地址	WiFi 信息收集	升级会员：解锁高级权限
00042	查询WiFi BSSID及扫描结果	信息收集 WiFi	升级会员：解锁高级权限
00130	获取当前WIFI信息	WiFi 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
00116	获取当前WiFi MAC地址并放入JSON中	WiFi 信息收集	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 WiFi	升级会员：解锁高级权限
00082	获取当前WiFi MAC地址	信息收集 WiFi	升级会员：解锁高级权限
00112	获取日历事件的日期	信息收集 日历	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
00067	查询IMSI号码	信息收集	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

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

00079	隐藏当前应用程序的图标	规避	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
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
00052	删除内容 URI 指定的媒体（SMS、CALL_LOG、文件等）	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
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	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
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
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
00016	获取设备的位置信息并将其放入 JSON 对象	位置 信息收集	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 位置	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 命令	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 命令	升级会员：解锁高级权限
00126	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	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
00024	Base64 解码后写入文件	反射 文件	升级会员：解锁高级权限
00058	连接到特定的WIFI网络	WiFi 控制	升级会员：解锁高级权限
00139	获取当前WiFi id	信息收集 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

00025	监视要执行的一般操作	反射	升级会员：解锁高级权限
00066	查询ICCID号码	信息收集	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	12/30	android.permission.RECEIVE_BOOT_COMPLETED android.permission.READ_PHONE_STATE android.permission.SYSTEM_ALERT_WINDOW android.permission.CAMERA android.permission.PACKAGE_USAGE_STATS android.permission.WRITE_SETTINGS android.permission.VIBRATE android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.WAKE_LOCK android.permission.GET_TASKS android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	12/46	android.permission.BLUETOOTH android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.FOREGROUND_SERVICE android.permission.ACCESS_BACKGROUND_LOCATION android.permission.CHANGE_NETWORK_STATE android.permission.BATTERY_STATS android.permission.CHANGE_WIFI_STATE android.permission.BLUETOOTH_ADMIN

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
greenrobot.org	安全	否	**IP**地址: 85.13.163.69 国家: 德国 地区: 图林根 城市: 弗里德斯多夫 纬度: 50.604919 经度: 11.035770 查看: Google 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

csmp.ceshiservice.cn	安全	是	**IP地址:** 123.249.47.229 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
mpas-sentry.xfpaas.com	安全	是	**IP地址:** 59.110.175.141 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
nisportal.10010.com	安全	是	**IP地址:** 124.64.196.20 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
iws.openspeech.cn	安全	是	**IP地址:** 36.7.109.160 国家: 中国 地区: 中国安徽 城市: 合肥 纬度: 31.820592 经度: 117.227219 查看: 高德地图
csmp.changyan.cn	安全	是	**IP地址:** 203.107.33.101 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
aidp.changyan.com	安全	是	**IP地址:** 203.107.32.209 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
scs.openspeech.cn	安全	是	**IP地址:** 117.48.148.47 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

zxid-m.mobileservice.cn	安全	是	**IP地址:** 115.231.163.68 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
data.openspeech.cn	安全	是	**IP地址:** 117.48.148.47 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
pre-aidp.changyan.com	安全	是	**IP地址:** 117.48.149.55 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
acs.amazonaws.com	安全	否	No Geolocation information available.
aid.mobileservice.cn	安全	是	**IP地址:** 115.231.163.68 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
xpush.voicecloud.cn	安全	是	**IP地址:** 42.62.116.74 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
docs.sentry.io	安全	否	**IP地址:** 203.107.33.101 国家: 美国 地区: 加利福尼亚 城市: 核桃 纬度: 34.020519 经度: -117.865532 查看: Google 地图
www.yixuexiao.cn	安全	是	**IP地址:** 203.107.33.101 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

www.zetetic.net	安全	否	**IP地址:** 13.227.74.122 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
jkintranet.changyan.com	安全	是	**IP地址:** 203.107.33.101 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.dcp.ceshiservice.cn	安全	是	**IP地址:** 117.48.149.55 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
dcp.changyan.com	安全	是	**IP地址:** 203.107.33.101 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
hdns.openspeech.cn	安全	是	**IP地址:** 101.200.180.128 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

URL 链接安全分析

URL信息	源码文件
• http://itcxpush.openspeech.cn/login.do • http://test-apiplat.changyan.com/m2/ice • http://xpush.voicecloud.cn/pushnode.do • http://itcxpush.openspeech.cn/app.do • http://itcxpush.openspeech.cn/v1/tags/sdk/tags.do • http://xpush.voicecloud.cn/v1/tags/sdk/tags.do • http://itcxpush.openspeech.cn/pushnode.do • http://xpush.voicecloud.cn/app.do • http://xpush.voicecloud.cn/login.do	自研引擎-A
• http://acs.amazonaws.com/groups/global/authenticatedusers • http://acs.amazonaws.com/groups/global/allusers • http://acs.amazonaws.com/groups/s3/logdelivery	com/obs/services/model/GroupGranteeEnum.java

本报告由南明离火移动安全分析平台生成

• 2.1.1.2	com/iflytek/edu/statistics/BuildConfig.java
• https://zxid-m.mobileservice.cn/sdk/uaid/get	com/zx/a/I8b7/c1.java
• https://zxid-m.mobileservice.cn/sdk/module/getcoremodule	com/zx/a/I8b7/x.java
• https://docs.sentry.io/clients/java/config/	io/sentry/event/a.java
• https://docs.sentry.io/clients/java/modules/android/	io/sentry/android/AndroidSentryClientFactory.java
• https://docs.sentry.io/clients/java/	io/sentry/dsn/a.java
• https://docs.sentry.io/clients/java/config/#in-application-stack-frames	b/a/a.java
• 2.1.1.2	com/iflytek/edu/statistics/plugin/EDULogStsPluginEntry.java
• www.baidu.com	com/iflytek/mdmcommon/NetUtils.java
• 223.5.5.5 • www.baidu.com	com/iflytek/mdmcommon/NetworkUtils.java
• www.baidu.com	com/iflytek/edu/apm/base/http/utils/EDULogNetUtils.java
• http://scs.openspeech.cn/scs • http://iws.openspeech.cn/online_param/config_update.php	com/iflytek/sunflower/config/a.java
• http://dcp.changyan.com/ • http://csmp.changyan.cn/	com/iflytek/edu/statistics/log/config/component/EDUComponentConstant.java
• www.yixuexiao.cn	com/iflytek/mdmbase/a/a.java
• http://hdns.openspeech.cn/sip/resolve?&srand=	com/iflytek/pushclient/d/g/a/c.java
• https://zxid-m.mobileservice.cn/sdk/config/init	com/zx/a/I8b7/g.java
• https://aid.mobileservice.cn/	com/zx/a/I8b7/g2.java
• https://aidp.changyan.com/open-svc/file/listststokenv2 • https://pre-aidp.changyan.com/open-svc/file/listststokenv2	a/b/a/d/c/f/b.java
• 59.61.88.200 • 59.61.88.219	com/iflytek/mdmlibrary/impl/p.java
• https://hisportal.10010.com:9001	com/zx/a/I8b7/g1.java
• https://pre-aidp.changyan.com/open-svc/file/recognition • https://aidp.changyan.com/open-svc/file/recognition	a/b/a/d/c/f/c.java
• http://jkintranet.changyan.com:8015	com/iflytek/mdmservice/k/z.java
• http://272add4c4b6c4f6cb12978fff439d7fe@mpas-sentry.xfpaas.com/55	com/iflytek/mdmservice/MDMApp.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

• 255.255.255.255 • 126.255.255.254 • 128.0.0.1 • 191.255.255.254 • 192.168.255.255 • 1.0.0.1	com/iflytek/mdmlibrary/a/a.java
• https://greenrobot.org/greendao/documentation/database-encryption/	org/greenrobot/greendao/g/b.java
• http://xpush.voicecloud.cn/v1/tags/sdk/tags.do • http://xpush.voicecloud.cn/pushnode.do • http://xpush.voicecloud.cn/app.do • http://xpush.voicecloud.cn/login.do	com/iflytek/pushclient/d/l/a.java
• https://csmp.changyan.cn/ • http://csmp.ceshiservice.cn/ • http://test.dcp.ceshiservice.cn/	com/iflytek/edu/log/bizbase/config/EDUDefStrategyHelper.java
• http://acs.amazonaws.com/groups/global/authenticatedusers • http://acs.amazonaws.com/groups/global/allusers • http://acs.amazonaws.com/groups/s3/logdelivery	com/obs/services/internal/o.java
• http://data.openspeech.cn/index.php/clientrequest/clientcollect/iscollect	com/iflytek/sunflower/task/b.java
• https://zxid-m.mobileservice.cn/sdk/channel/report	com/zx/a/I8b7/o2.java
• https://www.zetetic.net/sqlcipher/ • https://www.zetetic.net/sqlcipher/license/ • https://github.com/sqlcipher/android-database-sqlcipher	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
个推	个推	SDK 快速集成，免费试用使用。智能推送+场景推送，有效提升用户活跃度与粘性。
百度 LBS	Baidu	百度地图 Android SDK 是一套基于 Android 4.0 及以上版本设备的应用程序接口。 您可以使用该套 SDK 开发适用于 Android 系统移动设备的地图应用，通过调用地图 SDK 接口，您可以轻松访问百度地图服务和数据，构建功能丰富、交互性强的地图类应用程序。
SQLCipher	Zetetic	SQLCipher 是一个 SQLite 扩展，它提供数据库文件的 256 位 AES 加密能力。
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 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

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

2f2add4c4b6c4f6cb12978fff439d7fe@mpas-sentry.xfpaas.com	com/iflytek/mdmservice/MDMApp.java

第三方追踪器检测

名称	类别	网址
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97
Baidu Map		https://reports.exodus-privacy.eu.org/trackers/99
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

敏感凭证泄露检测

可能的密钥
百度地图的=> "com.baidu.lbsapi.API_KEY" : "jVqa6oemMUjPpkCwmztw84fIpgGiC16K"
个推-推送服务的=> "PUSH_APPID" : "4LUW1dpBbX5vmpzlsZeSg"
个推-推送服务的=> "GETUI_APPID" : "4LUW1dpBbX5vmpzlsZeSg"
凭证信息=> "IFLYTEK_APPKEY" : "5af009e7"
"library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/"
080c0addaf094b429971806c285e9d38
nKQTHaBxNTrjDrrnLHYoUogIFP9P+LS5Ua9i0onrn[illegible]yMp+n/yf+ejdU0A[illegible]
nb2QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC0Y+[illegible]qaLKaDLijxK
n3FgpZL+464f93Zu0re6doKzk6EY[illegible]bPaHTpvZ1BF185G[illegible]O63UnrfHli1JU
e5622ac949234d5c8475572a0[illegible]
nea0eWqeKM0I2RFb[illegible]dftkp4g6i2OA9e9R[illegible]ED81sGbVKaq3NQ=jqliO
00ccd806a03c[illegible]f884f5902102d95f6[illegible]c42219dd8a79b1465e186c0162a6771b55e7be7422c4af494ba0112ede4eb00fc751723f2c235ca419876e7103[illegible]22b72d754f66ff[illegible]f17c6cd2c9446e8c2bb5f4000a9c1c6577236a57e270bef07e7fe7bbec1f0e8993734c8bd4750e01feb21b6dc9
-361d28321796043df2db3dd1[illegible]2f4b4690cfa9f3d9e79397f4cb044ae9
MIICyDCCAbACCQC[illegible]Z6uTANBgkqhkiG9w0BAQsFADAlMQswCQYDVQQGEwJDUixlK
6defb35b059[illegible]6c9b091cf0d326
nusTjjSF[illegible]Dl6qOBXfdOQ2bKfreTynIzGUXk2UxB9P9LYFq124Pk93bwjuysSS31sifqYX
nMDgyOTA4MDg1OFowJTELMAkGA1UEBhMCQ04xFjAUBgNVBAoMDVVESUQgU0RLIFByij13K
wTuef3NyOxdN3r5MWadmXjHse9hzR9EkauispmVxeomdTB2npj29OhNrsUhaHuNhvnorLkhtO4nkfIQpgtwcy0q6m5

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

258EAFA5-E914-47DA-95CA-C5AB0DC85B11
ndkO2OrPD2LLosGvskAzXKNW2FfihAenUvQboKxgN6Ce638Iypg3QuopWJSsbWoV3LIx41
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
nfXK9AgMBAAEwDQYJKoZIhvcNAQELBQADggEBADauzLvXVQIyF2No4qaDcnod1SaaIxqKy
982a4f1ccf334affaeef1c7d0872a2a8
74b8d5ee25574b7cb5a1ebb718f18d83
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCaRPikR4WTAckHfIm80LCCoSGlCTogpFuC367bI4tYhryQnQgXIzNs8jS2wSHTeucmyjiWLpgFU4CnjfezI23V2AM0XOGeTICFmW86DkDe5PutddX/+bCAox19B8IMaUMBmWFM1qQZY837ppKKbrfTPALaog5xX9IlsjqYw9kICQIDAQAB
4465e786c1634dfcacc2f755b9007ecb
887d26e6de9e48b9a88fce1c61905305
wg4qVke8giFYcZozzgpf0KZVf0AKxicM6c8Q7E55ifATkulb4
82b79ad8551873a592e36abad22eeef5
c82febeb9a8f44fe9d3126a4a0192e81
nTjEWMBQGA1UECgwNVURJRCBTREsgUHJvZDAgFw0yMTA5MjIwODA4NThaGA8yMTIxKliqX
ed91c87d391f419fa6705a77a5331734
bCkPFoPcwU5jbPEmdawO3U0UHhNwlITxGeVUKrlbHS4aIo0Sla2xDTE3eFxoOxDTMBjUakDeyFIJQnUaT0eqhEInDGOrJm7s
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAJsqfq0gjyIi0OJ6DZfM1fwMfHefsorBtBHQoe2kMY5wpKedkKT8YIELHmFGkMB+jyUSAtoNTgQjE1Fe12icP8sCAwEAAQ==
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCjNXq+j1BRuv4PCOS+mp6fTTqqCfXYd50KUV7cTV4qRpUQOcq9nkiwroDVSpXehLSx2L3HICC9NRMH8p8cIOsOXk0V5XSeRbUJtUeGrWGA4ozR4Lmx1VcLgDorbi8komzOhflJ3ikz9924O20kg5qxQYl4Qs+XjootjyjqTqfPfwIDAQAB
9f23723f6a9b47cfa71e4243f70d1174
22b86ab5791149969bb4cf339c494a02
2f2add4c4b6c4f6cb12978fff439d7fe

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