南明离火
移动应用检测平台

ANDROID 静态分析报告

WS

registration accounts v10.1.3

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: 2025-04-01 22:26:47

应用概览

文件名称:	registration account v10.1.3.apk
文件大小:	20.5MB
应用名称:	registration account
软件包名:	wkokhxm.bybifa
主活动:	.WwbipqmxorMkzv04
版本号:	10.1.3
最小SDK:	14
目标SDK:	22
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	50/100 (中风险)
杀软检测:	17 个杀毒软件报毒
MD5:	233978c3ec1e4686c85b89d5097349d3
SHA1:	96d9f3e5358989fee0517b64[illegible]b0fdc2c56
SHA256:	0321c05f4c9e31bee56c437ddb881652078e7058b[illegible]912fbe7f1926f3c3e1c

分析结果严重性分布

高危	中危	信息	安全	关注
1	18	0	1	0

四大组件导出状态统计

Activity组件：6个，其中export的有：0个
Service组件：5个，其中export的有：4个
Receiver组件：15个，其中export的有：11个
Provider组件：1个，其中export的有：0个

应用签名证书信息

二进制文件已签名

本报告由南明离火移动安全分析平台生成

v1 签名: True
v2 签名: False
v3 签名: False
v4 签名: False
主题: C=RU, O=Android, OU=Mobile Development, CN=Application
签名算法: rsassa_pkcs1v15
有效期自: 2023-11-28 06:01:01+00:00
有效期至: 2051-04-15 06:01:01+00:00
发行人: C=RU, O=Android, OU=Mobile Development, CN=Application
序列号: 0x5bd1dcfd
哈希算法: sha256
证书MD5: 1f593875b45da2725778aafbbe710c1a
证书SHA1: 95f59b843f7ab9ba49f0185910390288308a81da
证书SHA256: eefc7342877bd2a3d1f2c28eb3790a243cadd8deb1e2f161fa2ee57335fea289
证书SHA512:
b381d5f3057270933bd92b71a9efd9f307e644046ba140c9faf6dc2a10141a3d948da49150e74affe2e190aa997a95927838d5cf23965cad830de2efea97af5

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_SUPERUSER	危险	获取超级用户权限	有root的设备声明超级用户权限
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.QUICKBOOT_POWERON	普通	接收设备重启或快速启动的广播的权限	一个用于接收设备重启或快速启动的广播的权限。它允许应用程序在设备重新启动后执行一些操作，例如启动一个服务、更新一些数据，或者显示一些通知。
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收短信。 恶意程序会在用户未知的情况下监视或删除。
android.permission.RECEIVE_MMS	危险	接收彩信	允许应用程序接收和处理彩信。恶意应用程序可借此监视您的信息，或者将信息删除而不向您显示。
android.permission.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
android.permission.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入手机或 SIM 卡中存储的短信。恶意应用程序可借此删除您的信息。
android.permission.BROADCAST_SMS	签名	发送已收到短信的广播	允许应用程序广播已收到短信的通知。恶意应用程序可借此伪造收到的短信。
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。
android.permission.PROCESS_INCOMING_CALLS	未知	未知权限	来自 android 引用的未知权限。
android.permission.CALL_PRIVILEGED	签名(系统)	直接拨打任何电话号码	允许应用程序在您不介入的情况下拨打任何电话（包括紧急呼救）。恶意应用程序可借此向应急服务机构拨打骚扰电话甚至非法电话。
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.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录
android.permission.WRITE_CALL_LOG	危险	写入通话记录	允许应用程序写入（但不读取）用户的通话记录数据。
android.permission.ANSWER_PHONE_CALLS	危险	允许应用程序接听来电	一个用于以编程方式应答来电的运行时权限。
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.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
com.android.alarm.permission.SET_ALARM	未知	未知权限	来自 android 引用的未知权限。
android.permission.USE_EXACT_ALARM	普通	允许在未经用户许可的情况下使用精确的警报	允许应用使用精确的警报。
android.permission.CAPTURE_AUDIO_HOTWORD	未知	未知权限	来自 android 引用的未知权限。
android.permission.GET_INTENT_SENDER_INTENT	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.UPDATE_LOCK	未知	未知权限	来自 android 引用的未知权限。
android.permission.DISAE_KEYGUARD	未知	未知权限	来自 android 引用的未知权限。
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.MODIFY_PHONE_STATE	签名(系统)	修改手机状态	允许应用程序控制设备的电话功能。拥有此权限的应用程序可自行切换网络、打开和关闭无线通信等，而不会通知您。
android.permission.READ_PHONE_NUMBERS	危险	允许读取设备的电话号码	允许读取设备的电话号码。这是READ PHONE STATE授予的功能的一个子集，但对即时应用程序公开。
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.NEARBY_WIFI_DEVICES	危险	需要通过 Wi-Fi 进行广告和连接到附近的设备	需要能够通过 Wi-Fi 进行广告宣传和连接到附近的设备。
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.ACCESS_MOCK_LOCATION	危险	获取模拟定位信息	获取模拟定位信息，一般用于帮助开发者调试应用。恶意程序可以用它来覆盖真实位置信息源。
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。

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.INSTALL_LOCATION_PROVIDER	签名(系统)	安装位置提供商	创建用于测试的模拟位置信息源。恶意程序可以用它来覆盖由真实位置信息源，如GPS或网络提供商返回的位置或状态，或者监视和报告您的位置到外部源
android.permission.CONTROL_LOCATION_UPDATES	签名(系统)	控制定位更新	允许获得移动网络定位信息改变。普通应用程序不能使用此权限。
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.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.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.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.PROCESS_OUTGOING_CALLS	危险	拦截外拨电话	允许应用程序处理外拨电话或更改要拨打的号码。恶意应用程序可能会借此监视、另行转接甚至阻止外拨电话。
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.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.UPDATE_DEVICE_STATS	签名(系统)	更新设备状态	允许应用程序更新设备状态。
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.CAPTURE_VIDEO_OUTPUT	普通	允许捕获视频输出	允许应用程序捕获视频输出。
android.permission.CAPTURE_AUDIO_OUTPUT	签名(系统)	允许捕获音频输出	允许应用程序捕获音频输出。
android.permission.CAPTURE_SECURE_VIDEO_OUTPUT	普通	允许捕获安全视频输出	允许应用程序捕获安全视频输出。
android.permission.RECORD_VIDEO	未知	未知权限	来自 android 引用的未知权限。
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_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.WRITE_MEDIA_STORAGE	签名(系统)	获取外置SD卡的写权限	允许应用程序在外置SD卡中进行写入操作。
android.permission.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。
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.USE_FULL_SCREEN_INTENT	普通	全屏通知	Android 10以后的全屏 Intent 的通知。
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。

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.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_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。
android.permission.SET_PROCESS_LIMIT	危险	限制运行的进程个数	允许应用程序控制将运行的进程数上限。普通应用程序从不需要使用此权限。
android.permission.INSTALL_PACKAGES	签名(系统)	请求安装APP	允许应用程序安装全新的或更新的 Android 包。恶意应用程序可能会借此添加其具有任意权限的新应用程序。
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.DELETE_PACKAGES	签名(系统)	删除应用程序	允许应用程序删除 Android 包。恶意应用程序可借此删除重要的应用程序。
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.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.START_ACTIVITIES_FROM_BACKGROUND	未知	未知权限	来自 android 引用的未知权限。
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。
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.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.ACCESS_SURFACE_FLINGER	签名	访问SurfaceFlinger	允许应用程序使用SurfaceFlinger低级别功能。
android.permission.READ_FRAME_BUFFER	签名	读取帧缓冲区	允许应用程序读取帧缓冲区中的内容,比如抓屏程序。
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.MANAGE_DEVICE_ADMINS	未知	未知权限	来自 android 引用的未知权限。
android.permission.INTERACT_ACROSS_USERS	未知	未知权限	来自 android 引用的未知权限。
android.permission.INTERACT_ACROSS_USERS_FULL	签名	允许应用程序在所有用户之间进行交互	允许应用程序在所有用户之间进行交互。这包括在其他用户的应用程序中创建活动、发送广播和执行其他操作。
oppo.permission.OPPO_COMPONENT_SAFE	签名	特定于 OPPO 设备的权限	它用于授予应用访问某些系统级功能或组件的能力，否则这些功能或组件会因安全原因而受到限制。此权限可确保只有受信任的应用程序才能与 OPPO 系统的敏感部分进行交互。
com.huawei.permission.external_app_settings.USE_COMPONENT	签名	特定于华为设备的权限	它用于授予应用访问某些系统级功能或组件的能力，否则这些功能或组件会因安全原因而受到限制。该权限确保只有受信任的应用才能与华为系统的敏感部分进行交互。

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.monitor.permission.ANDROID_MONITOR_CHECKER	未知	未知权限	来自 android 引用的未知权限。

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: **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: **17** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过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	Service (.iablsWl7t1H) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
3	Service (.YmuoghrgUnbbgh30) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_NOTIFICATION_LISTENER_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
4	Service (.fQ761l10) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_ACCESSIBILITY_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
5	Service (.GJPtOmMU2j) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

本报告由南明离火移动安全分析平台生成

6	Broadcast Receiver (.NlmiqviFkabri) 未被保护。[android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
7	Broadcast Receiver (.ZOu7tX0x6WK) 未被保护。[android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
8	Broadcast Receiver (.ny5e399) 未被保护。[android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
9	Broadcast Receiver (.PsmgttnrenIprynn) 未被保护。[android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
10	Broadcast Receiver (.wEwSD2U98U) 未被保护。[android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
11	Broadcast Receiver (.extYQTj) 受权限保护, 但是应该检查权限的保护级别。Permission: android.permission.BIND_DEVICE_ADMIN [android:exported=true]	警告	发现一个 Broadcast Receiver 共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
12	Broadcast Receiver (.jifep6H5MP) 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	Broadcast Receiver (.Meccpfhllsrb) 未被保护。[android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
14	Broadcast Receiver (.LdcmhiyrPjfsw) 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。
15	Broadcast Receiver (.AxlnanlgwGkboyd) 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 (.BuezsptjcZdbnya28) 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	高优先级的Intent （2147483647） - {3} 个命中 [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。

代码安全漏洞检测

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

序号	问题	等级	参考标准	文件位置

本报告由南明离火移动安全分析平台生成

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

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/libamsqlite.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

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	arm64-v8a/libamutils.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	arm64-v8a/libmyrec.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
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

敏感权限滥用分析

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

类型	匹配	权限
恶意软件常用权限	24/30	android.permission.RECEIVE_BOOT_COMPLETED android.permission.RECEIVE_SMS android.permission.RECEIVE_MMS android.permission.READ_SMS android.permission.WRITE_SMS android.permission.CALL_PHONE android.permission.READ_CALL_LOG android.permission.WRITE_CALL_LOG android.permission.GET_ACCOUNTS android.permission.WAKE_LOCK android.permission.READ_PHONE_STATE android.permission.READ_CONTACTS android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.PROCESS_OUTGOING_CALLS android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.SYSTEM_ALERT_WINDOW android.permission.MODIFY_AUDIO_SETTINGS android.permission.VIBRATE android.permission.WRITE_SETTINGS android.permission.REQUEST_INSTALL_PACKAGES android.permission.GET_TASKS android.permission.PACKAGE_USAGE_STATS
其它常用权限	17/46	android.permission.ACCESS_SUPERUSER android.permission.BROADCAST_SMS android.permission.FOREGROUND_SERVICE android.permission.ACCESS_MOCK_LOCATION android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.ACCESS_BACKGROUND_LOCATION android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.BATTERY_STATS android.permission.BLUETOOTH android.permission.INTERNET android.permission.CHANGE_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_SURFACE_FLINGER android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS

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
anmon.name	安全	否	**IP地址:** 168.119.91.88 **国家:** 德国 **地区:** 萨克森 **城市:** 法尔肯施泰因 **纬度:** 50.477852 **经度:** 12.371563 **查看:** Google 地图

本报告由南明离火移动安全分析平台生成

URL 链接安全分析

URL信息	源码文件
• https://plus.google.com/ • https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	自研引擎-A
• https://anmon.name/mch.html	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。
LAME	The LAME Project	LAME is a high quality MPEG Audio Layer III (MP3) encoder licensed under the LGPL.
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。

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