南明离火
移动应用检测平台

ANDROID 静态分析报告

Phone • v5.2.2

本报告由南明离火移动安全分析平台生成

分析日期: 2025-04-04 11:47:55

应用概览

文件名称:	Phone v5.2.2.apk
文件大小:	7.67MB
应用名称:	Phone
软件包名:	com.grice.dialer
主活动:	com.oneui.mobile.presentation.MobileActivity
版本号:	5.2.2
最小SDK:	26
目标SDK:	35
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	51/100 (中风险)
跟踪器检测:	3/432
杀软检测:	经检测，该文件安全
MD5:	fb9c5227defe75f2e2db39acb0c1e4ba
SHA1:	6a4e4ad13b84b5cff660b3cb5f7c0b0731833dbb
SHA256:	fa9a58c8d09436b9f6033ca5e0ba7fff83a7ea79c3e52c72657ea5fbb6f73b1d

分析结果严重性

高危	中危	信息	安全	关注
1	15	2	1	1

四大组件信息

Activity组件：12个，其中export的有： 0个
Service组件：14个，其中export的有： 2个
Receiver组件：13个，其中export的有： 4个
Provider组件：4个，其中export的有： 0个

证书信息

二进制文件已签名
v1 签名: False
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2023-05-04 16:58:36+00:00
有效期至: 2053-05-04 16:58:36+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x68a05954960b47657ade1ed7845cfa39fd65c6ba
哈希算法: sha256
证书MD5: 726bf74066f10932e639dad08c95c17a
证书SHA1: bb420e50e5246586611b963052025525d25423b8
证书SHA256: bd151dc695634487358462b482e058c88364aa94da3d1afa2cdb446d5d89471f
证书SHA512:
2eb6134c9ca2ca27d26e02ab5bd32bbe87bcfb0d966da37e5994895225bc02ad950f4b525f2f84d8c0eb20605f3c4a0c63dccd0fa21766827403c0ff24fe1709

公钥算法: rsa
密钥长度: 4096
指纹: 178053eb0309fe044486ae45121f0fdbe9f1dd4da735f5d2bba7919cddbba5fa
找到 1 个唯一证书

应用权限

权限名称	安全等级	权限内容	权限描述
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。
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。
com.android.vending.BILLING	普通	应用程序具有应用内购买	允许应用程序从 Google Play 进行应用内购买。
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.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.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.WRITE_CONTACTS	危险	写入联系人信息	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。
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.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.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.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.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）
android.permission.MANAGE_OWN_CALLS	普通	使呼叫应用程序能够管理自己的呼叫	允许通过自我管理的ConnectionService API管理自己的调用的调用应用程序。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.telecom.action.CONFIGURE_PHONE_ACCOUNT	未知	未知权限	来自 android 引用的未知权限。
android.permission.READ_SYNC_SETTINGS	普通	读取同步设置	允许应用程序读取同步设置，例如是否为“联系人”启用同步。
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.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。
com.android.voicemail.permission.ADD_VOICEMAIL	未知	未知权限	来自 android 引用的未知权限。
android.permission.ADD_VOICEMAIL	危险	将语音邮件添加到系统	允许应用程序将语音邮件添加到系统中。
android.permission.FOREGROUND_SERVICE_PHONE_CALL	普通	在通话期间启用前台服务	允许常规应用程序使用类型为“phoneCall”的 Service.startForeground。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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.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_ADSERVICES_AD_ID	普通	允许应用访问设备的广告 ID。	此 ID 是 Google 广告服务提供的唯一、用户可重置的标识符，允许应用出于广告目的跟踪用户行为，同时维护用户隐私。
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	普通	允许应用程序访问广告服务归因	这使应用能够检索与广告归因相关的信息，这些信息可用于有针对性的广告目的。应用程序可以收集有关用户如何与广告互动的数据，例如点击或展示，以衡量广告活动的有效性。
android.permission.ACCESS_ADSERVICES_TOPICS	普通	允许应用程序访问广告服务主题	这使应用程序能够检索与广告主题或兴趣相关的信息，这些信息可用于有针对性的广告目的。
android.permission.USE_BIOMETRIC	普通	使用生物识别	允许应用使用设备支持的生物识别方式。
android.permission.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。应用程序应改为请求USE_BIOMETRIC
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。

com.grice.dialer.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

可浏览的Activity组件

ACTIVITY	INTENT
com.oneui.mobile.presentation.MobileActivity	Schemes: tel://,

网络通信安全

序号	范围	严重级别	描述

证书安全分析

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	应用程序使用代码签名证书进行签名

MANIFEST分析

高危: **1** | 警告: **7** | 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	Activity （com.oneui.mobile.presentation.MobileActivity）如果未对输入进行校验，此配置允许同一设备上没有任何权限的第三方应用程序调用它并发起电话呼叫，而无需用户交互。	高危	一个导出的Activity ，如果没有对接收Intent的输入验证，则可以调用拨号程序进行拨打电话而无需用户交互，这很可能是一个高危漏洞，请人工核验。参考：CVE-2024-37574
3	Service (com.oneui.mobile.presentation.feature.calling.CallService) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_INCALL_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	Broadcast Receiver (com.oneui.mobile.presentation.feature.calling.CallActionReceiver) 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。

5	Service (androidx.work.impl.background.systemjob.SystemJobService) 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。
6	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver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。
7	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	发现一个 Broadcast Receiver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。
8	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver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。

</> 安全漏洞检测

高危: **0** | 警告: **5** | 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	应用程序使用SQLite数据库执行原始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
3	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

4	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
5	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
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	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
8	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

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
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
00014	将文件读入流并将其放入 JSON 对象中	文件	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
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
00132	查询ISO国家代码	电话服务 信息收集	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
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
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
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00173	获取 AccessibilityNodeInfo 屏幕中的边界并执行操作	无障碍服务	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

敏感权限分析

类型	匹配	权限
恶意软件常用权限	11/30	android.permission.WAKE_LOCK android.permission.READ_CONTACTS android.permission.WRITE_CONTACTS android.permission.READ_PHONE_STATE android.permission.CALL_PHONE android.permission.READ_CALL_LOG android.permission.WRITE_CALL_LOG android.permission.MODIFY_AUDIO_SETTINGS android.permission.RECORD_AUDIO android.permission.SYSTEM_ALERT_WINDOW android.permission.VIBRATE
其它常用权限	7/46	com.google.android.gms.permission.AD_ID android.permission.INTERNET android.permission.FOREGROUND_SERVICE android.permission.FLASHLIGHT android.permission.ACCESS_NETWORK_STATE com.google.android.c2dm.permission.RECEIVE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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。

域名检测

域名	状态	中国境内	位置信息
firebase-settings.crashlytics.com	安全	是	**IP地址:** 180.163.150.34 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图

youtrack.jetbrains.com	安全	否	**IP地址:** 63.33.88.220 **国家:** 爱尔兰 **地区:** 都柏林 **城市:** 都柏林 **纬度:** 53.344151 **经度:** -6.267249 **查看:** Google 地图
www.gricemobile.com	安全	否	**IP地址:** 172.217.12.147 **国家:** 美国 **地区:** 纽约 **城市:** 纽约市 **纬度:** 40.713192 **经度:** -74.006065 **查看:** Google 地图

URL链接分析

URL信息	源码文件
• https://www.gricemobile.com/privacy-policy	D3/t.java
• https://firebase.google.com/docs/crashlytics/get-started?platform=android#add-plugin	a2/C0311w.java
• https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings	I2/q.java
• https://firebase.google.com/docs/crashlytics/get-started?platform=android#add-plugin	a2/C0171w.java
• https://%s/%s/%s	W2/c.java
• https://youtrack.jetbrains.com/issue/kt-55980	Z4/C.java

FIREBASE数据库分析

标题	严重程度	描述信息

Firebase远程配置已启用	警告	Firebase远程配置URL （https://firebaseremoteconfig.googleapis.com/v1/projects/1024929666603/namespaces/firebase:fetch?key=AIzaSyA_HAZ_myRPzG_gfBc0tPQRmAmOZxGCKEo） 已启用。请确保这些配置不包含敏感信息。响应内容如下所示:
		
		{
		"entries": {
		"bn_ad": "ca-app-pub-9724255327554994/5912402030",
		"bn_ad_collapsible_load_time": "11",
		"bn_ad_debug": "ca-app-pub-3940256099942544/9214589741",
		"in_ad": "ca-app-pub-9724255327554994/6927847683",
		"in_ad_count": "3",
		"in_ad_debug": "ca-app-pub-3940256099942544/1033173712",
		"in_ad_time": "13",
		"na_ad": "ca-app-pub-9724255327554994/6015401862",
		"na_ad_debug": "ca-app-pub-3940256099942544/2247696110",
		"na_me_ad": "ca-app-pub-9724255327554994/8999484394",
		"ns_bn_ad": "",
		"ns_bn_ad_collapsible": "",
		"phone_in": "ca-app-pub-9724255327554994/6927847683",
		"phone_in_debug": "ca-app-pub-3940256099942544/1033173712",
		"sha_1": "BB:42:0E:50:E5:24:65:86:61:1B:96:30:52:02:E5:25:D2:54:23:B8"
		},
		"state": "UPDATE",
		"templateVersion": "299"
		}

第三方SDK

SDK名称	开发者	描述信息
Google Play Billing	Google	Google Play 结算服务可让您在 Android 上销售数字内容。本文档介绍了 Google Play 结算服务解决方案的基本构建基块。要决定如何实现特定的 Google Play 结算服务解决方案，您必须了解这些构建基块。
Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。
Jetpack App Startup	Google	App Startup 库提供了一种直接，高效的方法来在应用程序启动时初始化组件。库开发人员和应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。
Jetpack 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。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。
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。

追踪器

名称	类别	网址
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

密钥凭证

可能的密钥
AdMob广告平台的=> "com.google.android.gms.ads.APPLICATION_ID" : "@string/app_pub_id"
"com.google.firebase.crashlytics.mapping_file_id" : "41bbdc88a2784c2c9581df5f034e49a4"
"google_api_key" : "AIzaSyA_HAZ_myRPzG_gfBc0tPQRmAmOZxGCKEo"
"google_app_id" : "1:1024929666603:android:191f4ed464e2cea6e83c6e"
"google_crash_reporting_api_key" : "AIzaSyA_HAZ_myRPzG_gfBc0tPQRmAmOZxGCKEo"
470fa2b4ae81cd56ecbcda9735803434cec591fa
610c7938-e2cf-424e-9887-10ca1ad1abe1

GooglePlay应用信息

标题: 电话 - 联系人和电话

评分: 4.315196 **安装:** 1,000,000+ **价格:** 0 **Android版本支持:** **分类:** 通讯 **Play Store URL:** com.grice.dialer

开发者信息: GriceMobile, 7004979521025124660, Vietnam, https://gricemobile.github.io, helper@gricemobile.com,

发布日期: 2023年5月23日 **隐私政策:** Privacy Link

关于此应用:

轻量级的手机应用程序，漂亮的用户界面和许多有用的功能。 基本功能： * 查看联系人列表，联系人详情 * 添加、修改、删除联系人 * 查看通话记录列表，通话记录详情 * 删除通话记录，查看通话记录详情。 * 从常用联系人或通话记录屏幕快速拨打电话。 来电： * 手机锁定时滑动接听，如果您想拒接来电，请点击"提醒"和"拒绝来电"。 * 手机解锁时快速接听。 * 设置为从横幅或全屏显示来电。 在通话屏幕中： *美丽的通话画面 *添加新呼叫、合并或交换呼叫。 *支持在通话过程中输入 DTMF 键 *管理电话会议、拆分或结束子通话。 多 SIM 卡： *选择 SIM 卡与支持 Multi-SIM 卡的手机拨打电话 *在最近屏幕中显示接听或拨打电话的 SIM 卡插槽。 通话背景： *将图片设置为通话背景。 联系人海报：为每个联系人设置通话背景。 闪光警报： *接到来电时控制闪光灯。 *您仅可以为静音模式启用此功能。 连接性： *支持耳机或蓝牙耳机 *通话期间更改音频路线。 更多设置： 通过消息拒绝、阻止号码、假电话、来电提醒、联系人显示选项.... 权限 * 计费、互联网 捐款以支持我们的开发团队。 * CALL_PRIVILEGED、CALL_PHONE、RECORD_AUDIO 拨打或接听电话。 * CONTACTS 显示、删除联系人。 * CALL_LOG 显示 删除通话记录。 反馈 * 如果您在使用本应用程序时遇到任何问题，请告知我们，我们将尽快检查并更新。 * 电子邮件： helper@gricemobile.com

免责声明及风险提示:

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。