南明离火

——移动应用检测平台——

ANDROID 静态分析报告

Cally v1.2.2

分析日期: 2025-07-04 22:00:13

应用概览

文件名称:	594cf06e4f3ff8b8516e6b7b6068e02ae355363b86ae32ad0a2e3d3bd3388755 v1.2.2.apk
文件大小:	7.29MB
应用名称:	Cally
软件包名:	com.bin.calllogs
主活动:	com.bin.calllogs.activty.SplashActivity
版本号:	1.2.2
最小SDK:	24
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	49/100(中风险)
跟踪器检测:	5/432
杀软检测:	2 个杀毒软件报毒
MD5:	890ddb586c6d30e2b01f2678d1ba123b
SHA1:	9f33e517713a0c993dc634e34b09e834eac6ed33
SHA256:	594cf06e4f3ff8b8516e6b7b6068e02ae355363b86ae32ad0a2e3d3bd3388755

分析结果严重性分布

高危	中危	信息	安全	关注
3	17	2	2	1

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：13个，其中export的有： 3个
Receiver组件：12个，其中export的有： 3个
Provider组件：5个，其中export的有： 0个

应用签名证书信息

未能读取代码签名证书或没有可用的证书。

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.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.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.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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.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.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.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.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.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.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.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.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.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.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.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。
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.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.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。
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.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.bm.calllogs.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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.bin.calllogs.activty.DashBoardActivity	Schemes: tel://,

网络通信安全风险分析

序号	范围	严重级别	描述

Manifest 配置安全分析

高危: **0** | 警告: **8** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	Activity (com.bin.calllogs.activty.DashBoardActivity) 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。
2	Activity (com.bin.calllogs.activty.SubscriptionActivity) 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。

3	Service (com.bin.calllogs.dialer.services.CallService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_INCALL_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。
4	Broadcast Receiver (com.bin.calllogs.dialer.receivers.ActionReceiver) 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	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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。

6	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。
7	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [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。
8	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [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。

本报告由南明离火移动安全分析平台生成

代码安全漏洞检测

高危: **2** | 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
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	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
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	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
9	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
10	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
11	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

12	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
13	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

应用行为分析

编号	行为	标签	文件
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
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

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
00003	将压缩后的位图数据放入JSON对象中	相机	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
00091	从广播中检索数据	信息收集	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
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
00025	监视要执行的一般操作	反射	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
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
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
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
00013	读取文件并将其放入流中	文件	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
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

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
00189	获取短信内容	短信	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
00188	获取短信地址	短信	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
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
00010	读取敏感数据（SMS、CALLLOG）并将其放入 JSON 对象中	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
00012	读取数据并放入缓冲流	文件	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
00204	获取默认铃声	信息收集	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
00029	动态初始化类对象	反射	升级会员：解锁高级权限

00147	获取当前位置的时间	信息收集 位置	升级会员：解锁高级权限
00075	获取设备的位置	信息收集 位置	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
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
00110	查询ICCID号码	信息收集 电话服务	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
00121	创建目录	文件 命令	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
00104	检查给定路径是否是目录	文件	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
00028	从assets目录中读取文件	文件	升级会员：解锁高级权限
00034	查询当前数据网络类型	信息收集 网络	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	11/30	android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.CALL_PHONE android.permission.RECORD_AUDIO android.permission.READ_CONTACTS android.permission.READ_CALL_LOG android.permission.WRITE_CALL_LOG android.permission.WRITE_CONTACTS android.permission.READ_PHONE_STATE android.permission.MODIFY_AUDIO_SETTINGS android.permission.SYSTEM_ALERT_WINDOW
其它常用权限	7/46	android.permission.FOREGROUND_SERVICE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE com.google.android.gms.permission.AD_ID 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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
www.googleadservices.col	安全	否	No Geolocation information available.
googleads.g.doubleclick.nes	安全	否	No Geolocation information available.
csi.gstatic.col	安全	否	No Geolocation information available.

gitlab.com	安全	否	**IP地址:** 172.65.251.78 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
goo.gl	安全	否	**IP地址:** 142.250.72.148 **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
admob-gmats.uc.r.appspot.com	安全	否	**IP地址:** 172.67.202.182 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
firebase-settings.crashlytics.com	安全	否	No Geolocation information available.
phonetrackersfree.com	安全	否	**IP地址:** 172.67.202.182 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
pagead2.googlesyndication.com	安全	否	No Geolocation information available.

app-measurement.com	安全	是	**IP地址:** 180.163.150.161 **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
googlemobileadssdk.page.link	安全	否	**IP地址:** 172.67.202.182 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://googlemobileadssdk.page.link/ad-manager-android-update-manifest • https://googlemobileadssdk.page.link/admob-android-update-manifest	d/d/b/b/a/e0/a/h3.java
• https://phonetrackersfree.com/privacy.html	d/b/a/f/b/q.java
• https://phonetrackersfree.com/privacy.html	com/bin/calllogs/activty/PermissionActivity.java
• https://play.google.com/store/apps/details?id= • https://gitlab.com/bineshkumar16/adr/-/raw/main/adr.json?inline=false	com/bin/calllogs/activty/DashBoardActivity.java

• https://www.google.com/dfo/debugsignals • https://www.google.com/dfo/senddebugdata • https://googleads.g.doubleclick.nes/mads/static/mad/sdk/native/production/mraid/v3/mraid_app_banner.js • https://admob-gmats.uc.r.appspot.com/ • https://www.google.com/dfo/inappppreview • https://googleads.g.doubleclick.nes/mads/static/mad/sdk/native/production/mraid/v3/mraid_app_expanded_banner.js • https://googleads.g.doubleclick.nes • https://googleads.g.doubleclick.nes/mads/static/mad/sdk/native/production/mraid/v3/mraid_app_interstitial.js • https://googleads.g.doubleclick.nes/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html • https://googleads.g.doubleclick.nes/mads/static/mad/sdk/native/native_ads.html • https://pagead2.googlesyndication.col/pagead/ping?e=2&i= • https://www.google.com/dfo/linkdevice	d/d/b/b/h/a/rq.java
• https://phonetrackersfree.com/privacy.html	com/bin/calllogs/activty/DailerPermissionActivity.java
• www.google.com	d/d/b/b/a/e0/v.java
• https://accounts.google.com/o/oauth2/revoke?token=	d/d/b/b/c/b/e/d/f.java
• https://csi.gstatic.col/csi	d/d/b/b/h/a/fs.java
• https://googleads.g.doubleclick.nes/mads/static/mad/sdk/native/production/sdk-core-v40-impl.js • https://googleads.g.doubleclick.nes/mads/static/mad/sdk/native/sdk-core-v40-loader.html • https://googleads.g.doubleclick.nes/mads/static/mad/sdk/native/production/native_ads.js	d/d/b/b/h/a/ws.java
• https://pagead2.googlesyndication.col/pagead/gen_204?id=gmob-apps	d/d/b/b/a/b0/b.java
• https://googlemobileadssdk.page.link/admob-interstitial-policies	d/d/b/b/h/a/ri1.java

• https://googlemobileadssdk.page.link/admob-interstitial-policies	d/d/b/b/h/a/du0.java
• https://googlemobileadssdk.page.link/admob-interstitial-policies	d/d/b/b/h/a/l91.java
• https://app-measurement.com/a	d/d/b/b/h/h/cc.java
• https://goo.gl/j1swqy	d/d/b/b/h/h/x2.java
• https://www.google.com • www.google.com	d/d/b/b/i/b/d7.java
• https://goo.gl/naoooi • https://www.googleadservices.col/pagead/conversion/app/deeplink?id_type=adid&sdk_version=%s&rdid=%s&bundleid=%s&retry=%s	d/d/b/b/i/b/la.java
• https://app-measurement.com/a	d/d/b/b/i/b/y2.java
• https://firebase-settings.crashlytics.col/spi/v2/platforms/android/gmp/%s/settings	d/d/e/l/h/p/f.java
• https://firebase.google.com/support/privacy/init-options	d/d/e/r/f.java
• https://%s/%s/%s	d/d/e/r/n/c.java
• https://play.google.com/store/apps/details?id=	自研引擎-S

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/752458926861/namespaces/firebase:fetch?key=AIzaSyB__8V9Ul-rfZJEqHZuI3J2C3r-EBJOrrM ） 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
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。
Audience Network SDK	Facebook	The Audience Network allows you to monetize your Android apps with Facebook ads. An interstitial ad is a full screen ad that you can show in your app. Typically interstitial ads are shown when there is a transition in your app. For example -- after finishing a level in a game or after loading a story in a news app.
Google Sign-In	Google	提供使用 Google 登录的 API。
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。
Audience Network	Facebook	通过 Facebook 广告使您通过移动媒体资源获利
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。

邮箱地址敏感信息提取

EMAIL	源码文件
sportsapart@gmail.com	com/bin/calllogs/activty/DashBoardActivity.java

第三方追踪器检测

名称	类别	网址

本报告由南明离火移动安全分析平台生成

Facebook Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/65
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
OpenTelemetry (OpenCensus, OpenTracing)	Analytics	https://reports.exodus-privacy.eu.org/trackers/412

敏感凭证泄露检测

可能的密钥
AdMob广告平台的=> "com.google.android.gms.ads.APPLICATION_ID" : "ca-app-pub-8224195300641531~4995301729"
"client_server_key" : "752458926861-ga882k07mqjacrfuab6rk2kr14piev27.apps.googleusercontent.com"
"com.google.firebase.crashlytics.mapping_file_id" : "5f6a6f7ab5af45abae918c7bdb0b804b"
"google_api_key" : "AIzaSyB__8V9Ul-rfZJEqHZuI3J2C3r-EBJOrrM"
"google_app_id" : "1:752458926861:android:be061590c3dec1d8c9fe44"
"google_crash_reporting_api_key" : "AIzaSyB__8V9Ul-rfZJEqHZuI3J2C3r-EBJOrrM"
par+dwhNQqYERCSr3oGtYtDVSGtZjjivKpppvR62Z9a5oLpkQQBW7bLTBnuHswur
4CrOvkE592Vc7D7JV+aPXCWH2JLB6HWAiQnf8iH090=
7UZ/EsEPgF4ZRZ1chhiVPxgR+NfE5rqmZss2fiG1QT0=

本报告由南明离火移动安全分析平台生成

CJ1WRc1PE+xR6/6qo7i2DCIPFySihC2gOkB+O3ToQfek8u0n5+HTKTUaxwoTaOup
tqyxGM79wOlAPNBhvtAr5QJDQ+dGmpZ4a1UkwVDI/lw=
nvmQ1oBnYa1ILuQMJvjx1Mgo4XB5M+iT4lATd49U3XYe7vyBu0LOBGvU5w3i5cNm
wZRBY7DIvhHC8r92vSELjU6e4pNwFbBY03stSUuM3+c=
mNltpdI3VDBY3uA+ghPe9p5qLzSeUQcB+n6ngmGQjAWxdqQOivCHaODCjPIyIowZ
qp6rBGTCbwl3Du6FT/SAKGuw1FuFEkW7uLvnpWgAVmj4gvXya3866ptnORhDDu8c
BoHpLQ4RSQbqcE+eMuZEof5jiC86JqfpyVXCcg3LjBM=
HZVgL6ylhUUkiV7kuTw4wEOapRhn6IpTUlLxZYnAszU=
Sax58YmBV76Rsz+gTyIxls7MHtcGZGY5FRuTBSGuOW4=
lmWiEsyvybM0j+41L12yTdEmhqJ1mxl8TMt/J058O+jb1bYarXjRgBdNW2ZFy83f
wkdkWHeqh0k+zNwmTrd5/YaupE9zOer3F4z77d5lKl4=
pAhkgz3GzpF3+CqXZzwu1qvOvu4xxNqL26Gmlx8dugI=
YfHvCp/fIECQ9h2Dc66KvN7XWoaMnV2BSJeyfKAdgmQ=
jg02i/nmjOtojnLha7JcDbUxDuBiOjLYE3Mte35yoaAgj1btcenznNGCOsuwWch
41X4XnTjMYwUHeiH3ObXd8ksoY4Uh2/EIVKHpHML+QDKOhWxgVYOi4zhfQqT5GR2
Uhh1veu39niuxW7XP7M2VcepuNqwMJAE2TJQ6F736qMVhS4VpHkM9ihzOV4bRsyj
9B7JBIdZiMTsL9pGng5cYqUaYpTzUoAB9RvGyrnjQF7CiisbO4+nhiSdhoC6VSqn
saBI+3h2Lt3SmMRiIzkSzE+qZwwlCo+f51BVnuQZD0hVVNns8vrAQWZ7UlWn/0b0
eQRTNlDk13qQgUviNcuPPX0vJqvEjzyxzBtk+QMugeI=
B3EEABB8EE11C2BE770B684D95219ECB

本报告由南明离火移动安全分析平台生成

wmJ4yDzysGY/F4MtACYt1Wuo4utI1izySyPuZQUSJhk=
e8c4x8hx2nAUk6VVuY651BKZ4rbinGDtu4h/2o24aJo=
dE9eOZLY1eX3llTY4h0xyyrKD5UgCxwXxmUW3B3njYU=
ZkhLHPiP7Uf4DooNt/1kizZNADm1b+h8tAhXSPwcPrPbN3t+Jx06DZwzXlYEhSXE
6CULVgyWOH82iLGcKn5rh8N75AqCrKeqiHuFUWI8W3RSLolOGMDqAOnKtNTX1AFe
8FdD2h+EoXCjg5eQhtMlQE5LkOSf3AVqgJYbaqrJZgg=
Y4VPax9NN/dKmqF+s9P1EMA+IqhcGIPpcbgTKYuHNMmPmp8MhTxur5CR0eiVwBHP
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n

308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b300906035504061302555331133011060355040813 0a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d303830383231323331333345a170d333630313037323331333345a3074310b30090603550406130255533113301106035504081 30a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010 06dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf1dd44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb1f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7ef464c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
PfXuYpXR8QASWK08ChzZefD8h4IQvIx6Xugf6U+BJbFGNBOs3F9abkomDjkEKIY/
T+InekJlJ8RmIDkSOxSdVK3n60x123LKQKibAj90olVt6NWqXHdtrKrCRV+MIFdG
Bdd/SXecSQOrNYWNMJakrwr0suwau+ZSaygsyNqj5IcjiKGPVCNYxfh9jESu1wRd
atxCXkrFC9Qo4zr+qQKStinlw+xq4VCpNksBYKhnncQoFPxOQrQVA0Q5Y3uEyrMy9
WORPtHCVuMEv3v1W8NHqrRk35a2wyunOkGiiZJxdjaY=
pOQv/ncT1LaNtzYOMl87UsR5TvsuG5ecw6dyIcJCym+lewlOBw6IZhtgwF1qNMNH
Cb3a/0oybs716dPr7UCf4ZWTrxhPatWThTypQohUWkM=

1MAz8AsFFFR6PX7Q/aoiTCXDxA7Y87QD+tiULVUCjXhSqmeyoEv99dhFUigp84ha
et7+F9y0bmWPaNewdNSgaLaOgYWThlyODluK68jSELk=
MdKUmuf6DBtYuVjgv6h8BEjHuBvX5PE/R2XdoeGNJT0=
cxQLOgxIjd5GqHFd887UzcTVGYJaF4w3kSTCXM9zwKU=
8+Gsu284Xz8VlJdhu6cTHCdcvCVVHyOiPBH/5JkF0bc=
6f32224f52472dca661b0406b6d073cf
iJMtal0QkdCCvDIFbIXn2Msn+SEpgaeW0QkQ5fhgj50r8RtLZhDVC6lwnLAWkcW0
K1BE5iDLpIxaZZJp7C4O3DsdHGbDPO0C9L+hxNcDxpM=
BoYdDgxF0J4Z6qBFEz0Y0ptcEBy4vkae+v/aE6rWTPA=
u0deiS9oYmD364nfSsTKCoaogh75qkGLLRLBySCBkzjAL+3CKcuH0JuCgAzQyxJ
b418c6babba4f8390c3679e68e27b148
mgC3WGYZcRZZUEO15izZ6XddH7Xv5j+uDXn1fcHyPpA=
Egu28ffoQSw9KOwYfG/AJmF7fqmf54ISsd5MNAcPHGo=
rrjLlsla978gQsd21zlsNlBIZxX695vD5/bR0YoaFWUKt9pBHEKqU2V70kXmeqs
470fa2b4ae81cd56ecbcda9735803434cec591fa
SIWeD0mZWtt+r44TzGlKsRDDYnRFr4kkvUC1v+CRvf1A=
50C4883907597803F9BF3C085C768ED6
2FC8CB612ECB05649F7A43C1D166A919
R2RBJfxfdXZyH4kWmH3CYK5g20DhfXioszVJ9FTqzrY=
85FE603910593C6039EB04F05A005FA9

本报告由南明离火移动安全分析平台生成

308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d010104050030819431 0b3009060355040613025553311330110603550408130a43616c69666f726e6961131630140603550407130 d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b130741 6e64726f69643110300e06035504031307416e64726f6964312230200609 2a864886f70d0109011613616e6 4726f696440616e64726f69642e636f6d301e170d303830343135323333635365a170d3335303930313233 333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311 630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f6964311030 0e060355040b1307416e64726f69643110300e06035504031307416e64726f6964312230200609 2a864886f 70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105 000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c7e1bdb6d1db8 913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b9278948f0b22001994a929 15e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d0 51196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a35222ad06b8cc185eb15579e ef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c18 8ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf 066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d060355 d0e041604148d1cc5be954c433c6186 3a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c67863a15b04cbc03f24 fe0b2a1819aa48197308194310b3009060355040613025553113301106035504081 30a43616c69666f726e 6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f696 43110300e060355040b1307416e64726f6964311030006035504031307416e64726f6964312230200609 2a 864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c060 3551d13040530030101ff300d06092a864886f70d0101040500038201010019d30cf105fb78923f4c0d7dd22 3233d40967acfce00081d5bd7c6e9d6ed206b0e1209506416ca244939913d26b4aa0e0f524cad2bb5c6e 4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e678186673a3be56daf0b77b1c229e3c255 e3e84c905d2387efba09cbf13b202b4e5a22c93263484a28d2fc29fa9f1939759733afd8aa160f4296c2d01 63e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e5 1e5dd7b66787bef12fe97fba484c423fb4ff8cc494c0270f5051612ff6529393e8e46eac5bb21f277c151aa5f 2aa627d1e89da70ab6033d9de3b9897bfff7ea9b3e1243f60b
AIzaSyDRKQ9d6kfsoZ12lUnZcZnBYyH69HExNPE
All9dLPTMei/eCIBoDimh2kewv7aPoVe9eZ80kN1esN4=
sZcaWvHk5YMGi5Y+UpjcpSXXN/uJAE5+o93AJh0tgcKgvaqPrd4dFC6HKBJZfNCh
pQ8JnVS7yUZANCXtBym35/Ifx7Qa6SIA2WAFLNMh0sw=
0G0hVgzXcUXHuzEKOxAON/a0c4+sHPmbkckIOa2TK0w=

Google Play 应用市场信息

标题: Call Analysis - Call Backup

评分: 4.5694447 安装: 100,000+ 价格: 0 **Android**版本支持: 分类: 工具 **Play Store URL:** com.bin.calllogs

开发者信息: CallG, CallG, None, https://v9fd71e52.app-ads-txt.com/app-ads.txt, sportsappart@gmail.com,

发布日期: 2022年6月11日 隐私政策: Privacy link

关于此应用:

Cally 是通话管理器和通话数据分析的最佳应用程序，有助于拨打电话并跟踪您的通话数据。该应用程序包括许多功能，如呼叫拨号器、呼叫分析、呼叫日志使用统计、呼叫备份和恢复。 Cally - 呼叫备份和恢复见解 # 默认电话应用程序拨号器： Cally 提供了一个带有通话界面的简单电话拨号器，供用户管理通话。通话过程中，您可以静音/取消静音、切换免提、保持通话。 # 通话记录分析和过滤： Cally 帮助您保留无限的通话记录（大多数手机会保留最近 15 天的通话并删除较旧的通话），以便您可以保留更长时间的通话记录 你想要的。您还可以按持续时间、频率和新近度分析呼叫。呼叫分析器还支持高级过滤器，例如日期范围和呼叫类型：来电、去电 未接来电、已屏蔽 呼叫，不接听呼叫，并且从不接听呼叫。最适合呼叫分析和呼叫历史记录管理器。 # 联系人搜索和每个联系人的详细报告： Cally 帮助您按姓名、号码搜索联系人，并对每个联系人进行通话分析，例如通话统计、通话时长图、通话记录历史记录，只需单击联系人，您就可以访问全面的通话记录。 联系人报告，例如来电总数、去电总数、未接来电、拒绝来电、阻止来电和从未接听来电。 # Google Drive 上的通话记录备份： Cally 允许您从 Google 云端硬盘进行备份和恢复。您可以链接多个谷歌驱动器帐户和 开始按日、周、月备份通话数据。备份永远不会丢失您的通话数据。 Cally 提供了一种简单的方法来进行通话记录备份和恢复。 # 导出通话记录数据： 您可以将通话记录数据导出为 Microsoft Excel (XLS) 或 CSV 格式和 PDF 格式。这对于离线分析通话记录非常有帮助。 # 在您的设备上备份和恢复通话记录 Cally 允许您随时备份通话记录数据并在手机上恢复备份。您可以与其他人共享这些通话备份文件 设备来恢复它。它最适合通话记录备份和恢复。 # 标记通话备注： Cally 允许您在每次通话中添加备注，它将帮助您使用此通话备注进行搜索和过滤。您还可以过滤呼叫、查看 通过通话记录进行分析和通话摘要。 # 通话记录管理器： 这个应用程序存储无限数量的通话记录和许多更高级的功能，一般Android手机保持有限的来电数量通话记录。 Cally 第一次存储这些所有呼叫，但是该应用程序每天都会积累更多的呼叫日志数据，为您提供对更大的通话数据进行分析。它将帮助您进行每日通话分析。 # 单个联系人的通话记录图 Cally 允许您详细分析单个号码的通话记录，例如每日来电和持续时间、拨出电话和持续时间、未接来电 呼叫、拒绝呼叫、阻止呼叫和从未接听的呼叫。 # 附加功能： 查看日志中的主要呼叫者和最长呼叫持续时间 前 10 名来电/去电 查看每天的平均通话次数和持续时间 易于理解的统计屏幕 代表呼叫类别图和持续时间图 以 pdf 格式和 excel 格式保存通话报告 每日、每周、每月和每年的见解 遇到未知来电时，无需保存号码，可直接在 WhatsApp 上发送消息 各种呼叫类别，如来电、去电、未接、拒绝、阻止、未知来电、未接听去电、从未接听来电、从不 出席 外出 注意：我们不会在云服务器上保存您的任何数据，例如通话记录或联系人列表或设备信息。该应用程序仅利用您设备上存储的通话记录和联系人列表。 Cally 应用程序是为 Android™ 精心打造的，受到数百万用户的喜爱（□□）。请使用一次这个应用程序并分享您的想法和建议。我们喜欢您的反馈！或建议。

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。