南明离火
移动应用检测平台

ANDROID 静态分析报告

AInfluencers • v31.1.4

分析日期: 2025-07-07 07:38:49

应用概览

文件名称:	AInfluencers v31.1.4.apk
文件大小:	16.85MB
应用名称:	AInfluencers
软件包名:	com.ainfluencers
主活动:	com.ainfluencers.MainActivity
版本号:	31.1.4
最小SDK:	21
目标SDK:	34
加固信息:	未加壳
开发框架:	React Native
应用程序安全分数:	51/100 (中风险)
跟踪器检测:	1/432
杀软检测:	经检测，该文件安全
MD5:	53f7526a931e9ad0cd96c4b34732e887
SHA1:	deabe56fa567cd[illegible]1805afa55866b8a[illegible]53
SHA256:	e96640812[illegible]088afb1987fde2d[illegible]4875ac003b178880089684bbec365

分析结果严重性分布

高危	中危	信息	安全	关注
2	21	3	2	0

四大组件导出状态统计

Activity组件：19个，其中export的有： 1个
Service组件：16个，其中export的有： 3个
Receiver组件：22个，其中export的有： 6个

Provider组件：11个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: True
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: 2024-07-30 07:08:07+00:00
有效期至: 2054-07-30 07:08:07+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xe02d3a0ec213c3788053cc63e507c5caabe84eaa
哈希算法: sha256
证书MD5: 14b691178339d4af8b14542af315c70b
证书SHA1: 2017b46b35f8d204bd88aa09eba8a42b97abcec3
证书SHA256: 867b6cabf152c737a3333a55e911d55e2136418030fe06c1b7756cea9403a153
证书SHA512:
2912d7265e421fdfb8fc2ec8c93fbcd50fc04c654a087a693f33ccd8aafa8ce386b0a7bfc876f0d1d1f8c5723b54624191e19b01ab92eed1ad065f805792ce5e

公钥算法: rsa
密钥长度: 4096
指纹: b25763a841e6937d12067b187c6b27d4e026d5607c3b4212d2deda50f90e32df
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.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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.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.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_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。

android.permission.READ_MEDIA_VISUAL_USER_SELECTED	危险	允许从外部存储读取用户选择的图像或视频文件	允许应用程序从用户通过权限提示照片选择器选择的外部存储中读取图像或视频文件。应用程序可以检查此权限以验证用户是否决定使用照片选择器，而不是授予对 READ_MEDIA_IMAGES 或 READ_MEDIA_VIDEO 的访问权限。它不会阻止应用程序手动访问标准照片选择器。应与 READ_MEDIA_IMAGES 和/或 READ_MEDIA_VIDEO 一起请求此权限，具体取决于所需的媒体类型。
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_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.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.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.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）
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.ainfluencers.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
com.sec.android.provider.badge.permission.READ	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.android.launcher.permission.UPDATE_COUNT	普通	在应用程序上显示通知计数	在apex的应用程序启动图标上显示通知计数或徽章。
com.majeur.launcher.permission.UPDATE_BADGE	普通	在应用程序上显示通知计数	在solid的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。

com.huawei.android.launcher.permission.WRITE_SETTINGS	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
android.permission.READ_APP_BADGE	普通	显示应用程序通知	允许应用程序显示应用程序图标徽章。
com.oppo.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	未知	未知权限	来自 android 引用的未知权限。
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	未知权限	来自 android 引用的未知权限。
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.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。
android.permission.BROADCAST_CLOSE_SYSTEM_DIALOGS	未知	未知权限	来自 android 引用的未知权限。
android.permission.ACCESS_NOTIFICATION_POLICY	普通	标记访问通知策略的权限	对希望访问通知政策的应用程序的标记许可。
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	由 Google 定义的权限	由 Google 定义的自定义权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.ainfluencers.MainActivity	Schemes: https://, ainfluencer://, Hosts: @string/host, @string/branch_io_link, Path Prefixes: /auto-verify,

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全合规分析

高危: 0 | 警告: 1 | 信息: 1

标题	严重程度	描述信息
已签名应用	信息	应用已使用代码签名证书进行签名。

Manifest 配置安全分析

高危: **0** | 警告: **10** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	Broadcast Receiver (com.dieam.reactnativepushnotification.modules.RNPushNotificationBootEventReceiver) 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。
2	Service (com.dieam.reactnativepushnotification.modules.RNPushNotificationListenerService) 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。
3	Broadcast Receiver (io.invertase.firebase.messaging.ReactNativeFirebaseMessagingReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.c2dm.permission.SEND [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。
4	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。
5	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。
6	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.c2dm.permission.SEND [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。

7	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。
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。
9	Activity (app.notifee.core.NotificationReceiverActivity) 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。
10	Broadcast Receiver (app.notifee.core.AlarmPermissionBroadcastReceiver) 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。

代码安全漏洞检测

高危: **2** | 警告: **9** | 信息: **3** | 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	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

本报告由南明离火移动安全分析平台生成

3	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
4	此应用侦听剪贴板更改。一些恶意软件也会监听剪贴板更改	信息	OWASP MASVS: MSTG-PLATFORM-4	升级会员：解锁高级权限
5	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
6	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
7	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
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	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
10	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
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

12	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
13	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
14	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
15	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

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
00012	读取数据并放入缓冲流	文件	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
00036	从 res/raw 目录获取资源文件	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
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
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00175	获取通知管理器并取消通知	通知	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
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
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00134	获取当前WiFi IP地址	WiFi 信息收集	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
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
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
00072	将 HTTP 输入流写入文件	命令 网络 文件	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
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
00191	获取短信收件箱中的消息	短信	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
00195	设置录制文件的输出路径	录制音视频 文件	升级会员：解锁高级权限
00064	监控来电状态	控制	升级会员：解锁高级权限
00199	停止录音并释放录音资源	录制音视频	升级会员：解锁高级权限
00198	初始化录音机并开始录音	录制音视频	升级会员：解锁高级权限
00194	设置音源（MIC）和录制文件格式	录制音视频	升级会员：解锁高级权限
00197	设置音频编码器并初始化录音机	录制音视频	升级会员：解锁高级权限
00007	Use absolute path or directory for the output media file path	文件	升级会员：解锁高级权限
00196	设置录制文件格式和输出路径	录制音视频 文件	升级会员：解锁高级权限
00041	将录制的音频/视频保存到文件	录制音视频	升级会员：解锁高级权限
00092	发送广播	命令	升级会员：解锁高级权限
00192	获取短信收件箱中的消息	短信	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
00023	从当前应用程序启动另一个应用程序	反射 控制	升级会员：解锁高级权限
00079	隐藏当前应用程序的图标	规避	升级会员：解锁高级权限
00159	使用辅助服务执行通过文本获取节点信息的操作	无障碍服务	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
00188	获取短信地址	短信	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
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
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
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
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
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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	5/30	android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.VIBRATE android.permission.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK

其它常用权限	10/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.FOREGROUND_SERVICE com.google.android.c2dm.permission.RECEIVE android.permission.ACCESS_NOTIFICATION_POLICY 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
notifee.app	安全	否	**IP地址:** 13.32.115.166 **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
docs.swmansion.com	安全	否	**IP地址:** 104.21.27.136 **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
app.ainfluencer.com	安全	否	**IP地址:** 104.21.48.1 **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
influencers.ainfluencer.com	安全	否	**IP地址:** 104.21.48.1 **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

youtu.be	安全	否	**IP地址:** 104.21.27.136 **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
shopify.github.io	安全	否	**IP地址:** 185.199.110.153 **国家:** 美国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065647 **经度:** -79.891724 **查看:** Google 地图
codepush.appcenter.ms	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• http://www.ummulqura.org.sa/index.aspx • https://redux-toolkit.js.org/Errors?code • https://blog.ainfluencer.com/reasons-you-were-rejected-as-an-influencer • https://tools.ieft.org/html/bcp47 • http://fb.me/use-check-prop-typesaveWebGLVarrayIndexOfferLatecancelledocument-text-outline1F9D3-1F3FD1F9D3-1F3FE03E2431F9D3-1F3FFollower • https://docs.swmansion.com/react-native-reanimated/docs/fundamentals/glossary • https://bit.ly/3cXEKWfetchPageToken • https://docs.sentry.io/platforms/react-native/troubleshooting • https://react.dev/link/refs-must-have-owner • https://docs.swmansion.com/react-native-reanimated/docs/guides/troubleshooting • https://react.dev/link/strict-mode-string-ref • http://www.staff.science.uu.nl • https://redux.js.org/Errors?code • https://react.dev/link/invalid-hook-call • https://spotlightjs.com • http://momentjs.com/guides • https://spotlightjs.com/sidecar/npx/assets/src/assets/images/post_url_isActionCreatorblike	自研引擎-A
• https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenFragment.java
• https://docs.swmansion.com/react-native-reanimated/docs/guides/troubleshooting#mismatch-between-java-code-version-and-c-code-version • https://docs.swmansion.com/react-native-reanimated/docs/guides/troubleshooting#java-side-failed-to-resolve-c-code-version	com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java
• file:///freshchat_assets/freshchat_hacks.js' • file:///android_res/raw/normalize.css	com/freshchat/consumer/sdk/l/s.java
• https://youtu.be/i_8gqv06yvg • https://influencers.ainfluencer.com/api/en	com/ainfluencers/BuildConfig.java

本报告由南明离火移动安全分析平台生成

• https://docs.swmansion.com/react-native-gesture-handler/docs/guides/migrating-off-rnghenabledroot	com/swmansion/gesturehandler/react/RNGestureHandlerEnabledRootView.java
• https://shopify.github.io/flash-list/docs/usage#cellrenderercomponent	com/shopify/reactnative/flash_list/AutoLayoutView.java
• https://notifee.app/react-native/docs/triggers#android-12-limitations	app/notifee/core/b.java
• http://10.0.2.2:8969/stream	io/sentry/SpotlightIntegration.java
• file:///freshchat_assets/freshchat_hacks.js' • file:///android_res/raw/freshchat_article_link_icon.png • file:///android_res/raw/normalize.css	com/freshchat/consumer/sdk/l/d.java
• https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenStackFragment.java
• file:///freshchat_assets/freshchat_hacks.js' • file:///android_res/raw/normalize.css	com/freshchat/consumer/sdk/activity/ArticleDetailActivity.java
• https://codepush.appcenter.ms/	com/microsoft/codepush/react/CodePush.java
• https://youtu.be/i_8gqv06yvg • https://app.ainfluencer.com/.well-known/assetlinks.json • https://influencers.ainfluencer.com/api/en • http://161.97.147.229:3000/	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/449823831339/namespaces/firebase:fetch?key=AIzaSyDgy4QeaCKBHLHBZz4jASGvX_h3VUPf59Q ） 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 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。
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。
Picasso	Square	一个强大的 Android 图片下载缓存库。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).
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。

第三方追踪器检测

名称	类别	网址
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

敏感凭证泄露检测

可能的密钥
凭证信息=> "io.branch.sdk.BranchKey" : "key_live_neIYWHneMtnDm0U4gHzcdpcCzp9njdL"
"ANDROID_CODE_PUSH_KEY" : "L4rxI2IGjPMfD9sUXDSvpkCpa6pk4ksvOXqog"
"CodePushDeploymentKey" : "L4rxI2IGjPMfD9sUXDSvpkCpa6pk4ksvOXqog"
"FRESH_CHAT_APP_ID" : "f6d94ed4-b45d-4372-9fa6-1c36d7de558"
"FRESH_CHAT_APP_KEY" : "1aa3b43f-3671-4231-8427-ff8db37aeb98"
"IOS_CODE_PUSH_KEY" : "OYIUUc7E6bxIVWvbz35XpajUBmEB4ksvOXqog"
"freshchat_file_provider_authority" : "com.ainfluencers"
"google_api_key" : "AIzaSyDgy4QeaCKBHLHBZz4jASGvX_h3VUPf59Q"
"google_app_id" : "1:449823831339:android:98e65aff713200dd72416e"
"google_crash_reporting_api_key" : "AIzaSyDgy4QeaCKBHLHBZz4jASGvX_h3VUPf59Q"
3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784

55066263022277343669578718895168534326250603453777594175500187360389116729240
115792089210356248762697446949407573529996955224135760342422259061068512044369
115792089210356248762697446949407573530086143415290314195533631308867097853951
109384903807373427451111239076680556993620759895168374899458639449595311615073501601370873757375962324859213229670631330943845253159101291214232748847898598 4
686479766013060971498190079908139321726943530014330540939446345918554318339765605212255964066145455497729631139148085803712198799971664381257402829111505714 8
115792089210356248762697446949407573530086143415290314195533631308867097853948
1ddaa4b892e61b0f7010597ddc582ed3
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
115792089237316195423570985008687907853269984665640564039457584007908834671663
36134250956749795798585127919587881956611106672985015071877198253568414405109
24b2477514809255df232947ce7928c4
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316
LtrxI2IGjPMfD9sUXDSvpkCpa6pk4ksvOXqog
41058363725152142129326129780047268409114441015993725554835256314039467401291
115792089237316195423570985008687907852837564279074904382605163141518161494337
48439561293906451759052585252797914202762949526041747995844080717082404635286
fbd94ed4-b45d-4372-9fa6-51c36d7de558
2758019355995970587784901184038904809305690585636156852142870730198868924130986086513626076488374510776543976 1230575
32670510020758816978083085130507043184471273380659243275938904335757337482424
OYIUUo7E6BuIVWvbz[illegible]XpajUBmEB4ksvOXqog
8325710961489029985546751289520108179287853048861315594709205902480503199884419224438643760392947333078086511627871
1aa3b43[illegible]677-4834-8427-ff8db37ae[illegible]98
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
73463f9d-70de-41f8-857[illegible]-58590bdd5903
266174080205021706322876871672336096072985916875697314770667136841880294499642780849154508062777190235209424122506555866215711354557091681416163731589599984 6
90bd96d1[illegible]0[illegible]3dbe341cc5a33f373183a
686479766013060971498190079908139321726943530014330540939446345918554318339765539424505774633321719753296399637136332111386476861244038034037280889270700544 9

6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087

Google Play 应用市场信息

标题: 影响力人士的 Ainfluencers

评分: 3.7627118 **安装:** 10,000+ **价格:** 0 **Android版本支持:** **分类:** 办公 **Play Store URL:** com.ainfluencers

开发者信息: Ainfluencers, Ainfluencers, None, https://ainfluencer.com/, support@ainfluencer.com,

发布日期: 2024年10月1日 **隐私政策:** Privacy link

关于此应用:

您是一位有影响力的人或内容创作者，希望通过您的才华、Instagram、TikTok 和 Youtube 上的社交关注度来开发展您的品牌吗？无论您是微型、宏观还是巨型影响者，您都来到了对的地方。 Ainfluencer 是您与您所在类别或领域的顶级企业和品牌建立每日付费合作伙伴关系和合作的首选免费市场。与 100,000 多个符合您的风格和受众的品牌建立联系，并因您的创造力而获得报酬！ 特点： - 每日付费机会：每天与领先品牌以及新兴企业发现新的付费合作机会。 - 轻松协作：与符合您的市场的品牌无缝连接和协作。 - 安全支付：快速安全地获得您合作的付款。我们将为您处理所有付款。 - 个人资料管理：展示您的作品集、评级、评论，并通过专业的影响者个人资料发展您的个人品牌。每次合作都会帮助您在未来的合作中建立信任。 分析：通过深入分析跟踪您的表现和参与度，以提升您的影响力。 为什么选择 Ainfluencer？ 将您的内容货币化：与欣赏您创造力的品牌合作，将您的热情转化为利润。 扩展您的网络：与寻找 Instagram 和 TikTok 影响者以及 Youtuber 的顶级品牌建立持久的关系。 - 值得信赖的平台：加入信任 Ainfluencer 的有影响力的社区，建立安全可靠的合作伙伴关系。 -立即下载 Ainfluencer 并开始将您的影响力转化为收入！

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。