南明离火
移动应用检测平台

ANDROID 静态分析报告

myRAS • v4.4.0

分析日期: 2025-04-15 16:46:18

应用概览

文件名称:	myRAS v4.4.0.apk
文件大小:	37.97MB
应用名称:	myRAS
软件包名:	com.ras.mobile
主活动:	com.ras.mobile.MainActivity
版本号:	4.4.0
最小SDK:	23
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:	54/100 (中风险)
跟踪器检测:	2/432
杀软检测:	经检测，该文件安全
MD5:	a733b872252274b226041ec61372d49a
SHA1:	60038b999724ac32ff79af653f34bf33e78313ca
SHA256:	351adaa737c8da2c30e7d313fc5974c2128af3269afb3a962dd9f61a964851d2

分析结果严重性分布

高危	中危	信息	安全	关注
1	18	2	2	0

四大组件导出状态统计

Activity组件：7个，其中export的有： 2个
Service组件：22个，其中export的有： 2个
Receiver组件：11个，其中export的有： 5个
Provider组件：12个，其中export的有： 0个

应用签名证书信息

二进制文件已签名
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: 2019-10-16 21:29:50+00:00
有效期至: 2049-10-16 21:29:50+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xb78fb33116b78a8458c39ea2118a3356af4bf2b9
哈希算法: sha256
证书MD5: 88149a5f00b114694bf268bed8894c95
证书SHA1: d45b5fb38f1b966a579244125b3e816bce391d32
证书SHA256: 87521622c2a77a408b0f6a150c1d913c3b1945605e11f076e5e08617d90b24b1
证书SHA512:
9b0ead74cb211be022137ac0249b9b1f869f2611d2ef4a81795c113cd7dcb18092dff33eb62d9b850dc6779bd5833ada68f7cde69b9668d1609a557745bbec3

公钥算法: rsa
密钥长度: 4096
指纹: fdd4a1149e7b3940930de44a118759844e4eb77ee644499a5553d353291a52cb
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_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_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_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.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.BLUETOOTH_ADVERTISE	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够向附近的蓝牙设备进行广告。
android.permission.BLUETOOTH_CONNECT	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够连接到配对的蓝牙设备。
android.permission.BLUETOOTH_SCAN	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够发现和配对附近的蓝牙设备。
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.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.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.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.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
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_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.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_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.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.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
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。
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.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_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。
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.ras.mobile.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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。
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.providers.gsf.permission.READ_GSERVICES	未知	未知权限	来自 android 引用的未知权限。
com.google.android.gms.permission.ACTIVITY_RECOGNITION	危险	允许应用程序识别身体活动	允许应用程序识别身体活动。

可疑常 Activity 组件分析

ACTIVITY	INTENT

com.ras.mobile.MainActivity	Schemes: myras://, com.ras.mobile://, exp+myras://,

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	应用程序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	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	Broadcast Receiver (io.invertase.firebase.messaging.ReactNativeFirebaseMessagingReceiver) 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。
3	Activity (com.canhub.cropper.CropImageActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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。
4	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。
5	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。

6	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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。
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。
9	Activity (app.notifee.core.NotificationReceiverActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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 (app.notifee.core.AlarmPermissionBroadcastReceiver) 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。

代码安全漏洞检测

高危: **1** | 警告: **6** | 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	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

3	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
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	启用了调试配置。生产版本不能是可调试的	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
7	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
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	警告	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限
10	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

应用行为分析

编号	行为	标签	文件
00091	从广播中检索数据	信息收集	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

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
00121	创建目录	文件 命令	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
00125	检查给定的文件路径是否存在	文件	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
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00001	初始化位图对象并将数据（例如JPEG）压缩为位图对象	相机	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
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
00012	读取数据并放入缓冲流	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
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
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

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
00038	查询电话号码	信息收集	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
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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	8/30	android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.SYSTEM_ALERT_WINDOW android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	12/46	android.permission.ACCESS_NETWORK_STATE android.permission.BLUETOOTH android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE android.permission.FOREGROUND_SERVICE com.google.android.c2dm.permission.RECEIVE com.google.android.gms.permission.AD_ID com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE android.permission.ACCESS_NOTIFICATION_POLICY com.google.android.gms.permission.ACTIVITY_RECOGNITION

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

expo.dev	安全	否	**IP地址:** 104.18.4.104 **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
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
notifee.app	安全	否	**IP地址:** 172.64.206.80 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件

• https://developer.huawei.com/repo/ • http://www.ummulqura.org.sa/index.aspx • http://dogs.are.greater • https://spotlightjs.com/sidecar/npx/common-documents/listCacheClearia-expanded • https://www.jitpack.io • https://docs.sentry.io/platforms/react-native/troubleshooting/ • https://reqres.in/api/ReactNativeBlobUtil-blobs/ • https://api-v2.mydaily.ras-groupe.com/api-360 • https://espace-personnel.ppr.myras.frCA • http://invertase.link/android • https://docs.swmansion.com/react-native-reanimated/docs/guides/troubleshooting • https://dumper-cgi.stsweb.fr • https://espace-personnel.myras.fr • https://myras.fr/conditions-generales/family-situations/liste_des_offresolveDefaultPropspanToTransactionTraceContextinnerHeighttps • https://sentry.io/ • https://github.com/date-fns/date-fns/blob/master/docs/unicodeTokens.mdashapesERR_SE_CON_0048_UNEXPECTED_ERROReactNativeBlobUtil • https://github.com/henninghall/react-native-date-picker/issues/404 • http://www.staff.science.uu.nl/ • https://docs.sentry.io/platforms/javascript/best-practices/browser-extensions/common/time-off-reason/listCacheDelete • https://sentry.io/welcome/job-types/worker/add-document-signed-fullScreenSwipeEnabled_getHistoryBreadcrumbHandlereanimatedDummyras • https://dev.to/li/how-to-requestpermission-for-devicemotion-and-deviceorientation-events-in-ios-13-46g2. • https://play.google.com/store/apps/details?id=com.ras.mobile&hl=frCH.3e • https://espace-personnel.mydaily.pro • https://docs.swmansion.com/react-native-reanimated/docs/fundamentals/glossary/ • https://myras.fr/utilisation-de-librairies-tiers/job-types/editor__crop-containerDimensionlarrhkPrimediumseagreenableStallTrackingetTopickAllargeTitleFontWeighttps • https://spotlightjs.com • https://browser.sentry-cdn.com.android.voicemail.permission.READ • http://fb.me/use-check-prop-types_de_contratsCan • https://github.com/date-fns/date-fns/blob/master/docs/upgradeGuide.md	自研引擎-A
• https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenStackFragment.java
• https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenFragment.java
• https://github.com/expo/expo/tree/main/packages/expo-splash-screen#-configure-android	expo/modules/splashscreen/singletons/SplashScreen.java
• https://github.com/expo/expo	expo/modules/securestore/encryptors/HybridAESEncryptor.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
• https://github.com/software-mansion/react-native-screens/issues	com/swmansion/rnscreens/utils/ScreenDummyLayoutHelper.java
• https://expo.dev	expo/modules/webbrowser/CustomTabsActivitiesHelperKt.java
• https://docs.swmansion.com/react-native-gesture-handler/docs/guides/migrating-off-rnghenabledroot	com/swmansion/gesturehandler/react/RNGestureHandlerEnabledRootView.java
• http://10.0.2.2:8969/stream	io/sentry/SpotlightIntegration.java

• https://notifee.app/react-native/docs/triggers#android-12-limitations	app/notifee/core/b.java

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/15016367498/namespaces/firebase:fetch?key=AIzaSyADsGTVADzcfGNdFqHjhCvQW3hnsR7Cc-o）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。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Jetpack ProfileInstaller	Google	此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 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
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

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

敏感凭证泄露检测

可能的密钥
"blob_provider_authority" : "com.ras.mobile.blobs"
"google_api_key" : "AIzaSyADsGTVADzcfGNdFqHjhCvQW3hnsR7Cc-o"
"google_app_id" : "1:15016367498:android:d0ba728010b49426012473"
"google_crash_reporting_api_key" : "AIzaSyADsGTVADzcfGNdFqHjhCvQW3hnsR7Cc-o"
24b2477514809255df232947ce7928c4
1ddaa4b892e61b0f7010597ddc582ed3

Google Play 应用市场信息

标题: my RAS – Emploi et Intérim

评分: 4.6354465 **安装:** 100,000+ **价格:** 0 **Android版本支持:** **分类:** 办公 **Play Store URL:** com.ras.mobile

开发者信息: RAS Intérim, RAS+Int%C3%A9rim, None, http://www.myras.fr/, poledigital@ras-interim.fr,

发布日期: None **隐私政策:** Privacy link

关于此应用:

有了我的 RAS，做临时工更容易了！ 使用我们的 my R.A.S 应用程序简化您的生活：所有管理信息都触手可及。您可以专注于您的工作，剩下的交给我们。 只需单击几下即可将您的申请发送给我们，以注册并接收根据您的个人资料量身定制的工作机会，同时受益于我们招聘专家的个性化支持。 此外，该应用程序是完全免费的！ 超过60,000名临时工信任我们，为什么不呢？ 我们是运输（重型货车司机、卡车司机）和物流（叉车操作员）方面的专家，在许多其他活动领域也有招聘广告。我们提供大众配送、零售、移动、绿地、服务、建筑、物流、健康、工业、旅游、酒店/餐厅、活动、运输和物流、体育和福利以及奢侈品方面的任务。 您是学生、自由职业者还是临时工？对于临时工作、CDD、CDI或季节性工作？我们为您提供与您个人资料的工作。 轻松创建您的个人资料！ 填写您的简历并发送注册所需的所有行政文件。您有一个完全安全的空间来传输您的个人信息。 发送您的简历并接收我们的工作机会！ 选择您感兴趣的职业和职位类型、执行任务所需的地点以及所需的工作时间。 管理您的行政文件！ 每个月下载并接收您的工资单，并直接在应用程序上签署您的派遣合同。 我们竭诚为您服务，帮助您找到临时任务以及定期或永久合同，以满足您所有的临时或永久工作搜索。 简而言之，随时随地工作！凭借我们由 170 多家机构组成的网络，您附近一定有一项任务！ 在我们的临时 m/f 报价中，您会发现： - 邮递员 - 仓库管理员 - 机器司机 - 卡车司机 - 公共工程 - 做饭 - 路 - 梅森 - 供暖工程师 - 学生工作 - 景观设计师 - 画家 - 道路养护剂 - 电工 - 收银员 - 救生员 - 分选剂 每天都会为您提供新任务！ 我们的顾问每天都会提供新的临时工作机会！请记住定期检查您的个人资料。 此外，实时修改和更新您的可用性！ 我们的专家每天 24 小时为您提供持续服务；每周 7 天！事实上，R.A.S Interim 为您带来了求职过程中的所有专业知识。 我们是许多活动领域的专家，可为您提供个性化支持，帮助您搜索并找到适合您个人资料的工作。我们是您需要的临时工作申请，共同打造您的专业项目！ 也找到我们 在我们的网站上： 如果您是候选人，您可以查阅我们的报价并在我们的网站上提交您的简历：https://www.ras-interim.fr/ https://www.fms-interim.fr/ 有用的链接： 隐私政策：https://myras.fr/politique-de-confidentialite/ 一般条件：https://myras.fr/conditions-generales/ 在社交网络上找到我们： 脸书：https://www.facebook.com/RasInterim/ 推特：https://twitter.com/ras_interim 优酷：https://www.youtube.com/channel/UCi45_g6i0UVDuVL5WH0VmqA 领英：https://www.linkedin.com/company/ras-interim-france Instagram：https://www.instagram.com/rasinterimfrance/ 电子邮件支持：poledigital@ras-interim.fr

免责声明及风险提示: