南明离火
移动应用检测平台

ANDROID 静态分析报告

Bitroo • v3.0.0

分析日期: 2025-07-05 23:15:02

应用概览

文件名称:	Bitroo v3.0.0.apk
文件大小:	26.78MB
应用名称:	Bitroo
软件包名:	com.bitroo.up
主活动:	com.bitroo.up.SplashActivity
版本号:	3.0.0
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:	48/100 (中风险)
跟踪器检测:	5/432
杀软检测:	经检测，该文件安全
MD5:	eec1dd406fce08c83ec15768d363562d
SHA1:	4806a232048a23e[illegible]ba8644dad62c79081e
SHA256:	99420ac49d8[illegible]b53929be2028161ac6[illegible]3029bf38aa9eec03b868d845ff23d9

分析结果严重性分布

高危	中危	信息	安全	关注
4	24	5	2	0

四大组件导出状态统计

Activity组件：13个，其中export的有： 3个
Service组件：25个，其中export的有： 7个
Receiver组件：11个，其中export的有： 3个
Provider组件：13个，其中export的有： 1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: 2023-07-05 11:29:37+00:00
有效期至: 2053-07-05 11:29:37+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xcb288707ea1727045be2f70beaf136b4bee717d0
哈希算法: sha256
证书MD5: 3dc93cde6daab433f7dc9a9d667dbaf6
证书SHA1: fe671b8448123abd5174d251f08f0fac8fe77b21
证书SHA256: d84a77af1dd47759ad435ba96233bfe12acae351a02574929df4814ef3d32ebd
证书SHA512:
7ba8ea4720eb957bf4232aab17549a5563ea657f55aa790d8bdab55cc5e97f1061336900d4369d35fecde17069dfaa324a60e86db2f9913c0545ae8cd65b3551

公钥算法: rsa
密钥长度: 4096
指纹: 2e22d794cc8f89591374d4be5a15756c57de8a1b8a47aaf057f44524f951c0ed
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.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.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.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.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_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.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_MEDIA_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。
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，在手机屏幕关闭后台进程仍然运行。

com.android.vending.CHECK_LICENSE	未知	未知权限	来自 android 引用的未知权限。
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。
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.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.bitroo.up.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
com.hihonor.android.launcher.permission.CHANGE_BADGE	未知	未知权限	来自 android 引用的未知权限。
com.hihonor.push.permission.READ_PUSH_NOTIFICATION_INFO	未知	未知权限	来自 android 引用的未知权限。
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.bitroo.up.permission.MIPUSH_RECEIVE	未知	未知权限	来自 android 引用的未知权限。
com.meizu.flyme.permission.PUSH	未知	未知权限	来自 android 引用的未知权限。
com.meizu.flyme.push.permission.RECEIVE	普通	魅族push服务权限	魅族push服务权限。
com.bitroo.up.push.permission.MESSAGE	未知	未知权限	来自 android 引用的未知权限。
com.meizu.c2dm.permission.RECEIVE	普通	魅族push服务权限	魅族push服务权限。
com.bitroo.up.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	普通	OPPO推送服务	OPPO推送服务正常工作所必需的，它允许应用接收来自OPPO推送系统的消息。
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	普通	OPPO推送服务	OPPO推送服务正常工作所必需的，它允许应用接收来自OPPO推送系统的消息。
com.push.permission.UPSTAGESERVICE	未知	未知权限	来自 android 引用的未知权限。
com.bitroo.up.permission.PROCESS_PUSH_MSG	未知	未知权限	来自 android 引用的未知权限。
com.bitroo.up.permission.PUSH_PROVIDER	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.bitroo.up.MainActivity	Schemes: bitroo://,

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: **15** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、Media Player 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	Activity (com.bitroo.up.MainActivity) 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	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。
4	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。

5	Activity (com.engagelab.privates.common.component.MTCommonActivity) 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。
6	Activity (com.xiaomi.mipush.sdk.NotificationClickedActivity) 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。
7	Service (com.xiaomi.mipush.sdk.PushMessageHandler) 受权限保护，但应检查权限保护级别。 Permission: com.xiaomi.xmsf.permission.MIPUSH_RECEIVE [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 (com.engagelab.privates.push.platform.mi.callback.MTMiCallback) 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。
9	Service (com.meizu.cloud.pushsdk.NotificationService) 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。
10	Broadcast Receiver (com.engagelab.privates.push.platform.meizu.callback.MTMeizuCallback) 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。
11	Service (com.heytap.msp.push.service.CompatibleDataMessageCallbackService) 受权限保护，但应检查权限保护级别。 Permission: com.coloros.mcs.permission.SEND_MCS_MESSAGE [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。
12	Service (com.heytap.msp.push.service.DataMessageCallbackService) 受权限保护，但应检查权限保护级别。 Permission: com.heytap.mcs.permission.SEND_PUSH_MESSAGE [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。

13	Service (com.vivo.push.sdk.service.CommandClientService) 受权限保护，但应检查权限保护级别。 Permission: com.push.permission.UPSTAGESERVICE [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。
14	Broadcast Receiver (com.huawei.hms.support.api.push.PushMsgReceiver) 受权限保护。 Permission: com.bitroo.up.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	检测到 Broadcast Receiver 已导出，但受权限保护。
15	Broadcast Receiver (com.huawei.hms.support.api.push.PushReceiver) 受权限保护。 Permission: com.bitroo.up.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	检测到 Broadcast Receiver 已导出，但受权限保护。
16	Service (com.huawei.hms.support.api.push.service.HmsMsgService) 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。
17	Content Provider (com.huawei.hms.support.api.push.PushProvider) 未受保护。 [android:exported=true]	警告	检测到 Content Provider 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: **3** | 警告: **8** | 信息: **6** | 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	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
4	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
5	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	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	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	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
9	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
10	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
11	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

12	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
13	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
14	此应用程序使用SQL Cipher，确保密钥没有硬编码在代码中	信息	OWASP MASVS: MSTG-CRYPTO-1	升级会员：解锁高级权限
15	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
16	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
17	应用程序可以写入应用程序目录。敏感信息应加密	信息	CWE: CWE-276: 默认权限不正确 OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限

应用行为分析

编号	行为	标签	文件
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
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
00091	从广播中检索数据	信息收集	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

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
00028	从assets目录中读取文件	文件	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
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
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
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
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
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
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
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
00012	读取数据并放入缓冲流	文件	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
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
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
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
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
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
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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	2/30	android.permission.VIBRATE android.permission.WAKE_LOCK
其它常用权限	11/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_AUDIO android.permission.ACCESS_WIFI_STATE com.google.android.c2dm.permission.RECEIVE 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
codepush.appcenter.ms	安全	否	No Geolocation information available.
twitter.com	安全	否	**IP地址:** 151.101.192.84 **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
mobile.events.data.microsoft.com	安全	否	**IP地址:** 52.182.143.208 **国家:** 美国 **地区:** 爱荷华州 **城市:** 得梅因 **纬度:** 41.600449 **经度:** -93.609116 **查看:** Google 地图
in.appcenter.ms	安全	否	**IP地址:** 151.101.192.84 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 博伊顿 **纬度:** 36.667641 **经度:** -78.387497 **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
pinterest.com	安全	否	**IP地址:** 151.101.192.84 **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

URL 链接安全分析

URL信息	源码文件

• https://docs.swmansion.com/react-native-reanimated/docs/fundamentals/glossary • http://help.dottoro.com/lcbixvwm.phparseIsoWeekdayHeaderRemaining • https://bugzilla.mozilla.org/show_bug.cgi?id=947588__reactInternalMemoizedUnmaskedChildContextRefirestoreDeletedValuesInNestedArrayuseNavigationContainerRefirstRoutevopfirstWeekOffset • https://microsoft.github.io/code-pushContextProvidereadStreaminmax • http://momentjs.com/guides • https://redux.js.org/Errors?code=_CSS • http://phrogz.net/tmp/canvas_image_zoom.htmldrdharlbrkeyboardkeyPointsqufishttps • https://github.com/csstree/stylelint-validator/issues/29 • http://fb.me/use-check-prop-typesEnumOctavesuppressHighlightingetCouponStoreListatusBarStylebad-string-tokenqueueNativeCalling • https://github.com/calintamas/react-native-toast-message/blob/master/README.mdn_url • https://www.sitepoint.com/css3-cursor-styles/n/api/v1/activity/normalUser/status----------start • https://dev.to/li/how-to-requestpermission-for-devicemotion-and-deviceorientation-events-in-ios-13-46g2.29.320682baseUniqrToPathandleTitleLayoutoHexadecimal-paddingHorizontallElementsCreatingNativeWindowssfunction • http://help.dottoro.com/lcrthhhv.phparseFontStringetReactTreehttps • https://www.baidu.com • https://github.com/csstree/csstree/issues • https://github.com/lahmatiy • http://help.dottoro.com/lcbkewgt.phparseJSCHeapCapture.captureHeap • https://github.com/mdn/data/pull/431 • https://github.com/ecomfe/echarts/blob/master/LICENSE.txt • https://play.google.com/store/apps/details?id=com.bitroo.up&hl=en&gl=USDT/7/Day1 • http://help.dottoro.com/lclhnthl.phparseFileSlashouldIgnoreCaseModecodeXMLStrictRNSVGClipPathasUnresolvedRefs.slice • https://docs.swmansion.com/react-native-reanimated/docs/guides/troubleshooting • https://drafts.fxtf.org/css-masking-1 • https://github.com/ecomfe/zrender/blob/master/LICENSE.txt • https://github.com/charpeni/react-native-url-polyfill/issuesopFirebaseJsonLoadingFinishadowRadiuseAnimatedSensorGravitySensortedLastIndexOfirebaseModuleWithArgshouldTestNextLibringsTstrokeCapitalDifferentialDOMTimeStamparseMscrollTojestackRefirefox • http://help.dottoro.com/lcxquvkf.phparseGeckopfirebase.analytics	自研引擎-A
• https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenStackFragment.java
• https://pinterest.com/pin/create/button/?url={url}&media=$media&description={message}	cl/json/social/PinterestShare.java
• https://play.google.com/store/apps/details?id=com.instagram.android	cl/json/social/InstagramStoriesShare.java
• https://play.google.com/store/apps/details?id=com.instagram.android	cl/json/social/InstagramShare.java
• https://www.facebook.com/sharer/sharer.php?u={url}	cl/json/social/FacebookShare.java
• https://in.appcenter.ms	com/microsoft/appcenter/ingestion/AppCenterIngestion.java

• https://www.facebook.com/sharer/sharer.php?u={url}	cl/json/social/FacebookPagesManagerShare.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://mobile.events.data.microsoft.com/onecollector/1.0	com/microsoft/appcenter/ingestion/OneCollectorIngestion.java
• https://github.com/software-mansion/react-native-screens/issues	com/swmansion/rnscreens/utils/ScreenDummyLayoutHelper.java
• https://twitter.com/intent/tweet?text={message}&url={url}	cl/json/social/TwitterShare.java
• 3.0.0.4	com/engagelab/privates/push/platform/vivo/BuildConfig.java
• https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704676	com/swmansion/rnscreens/ScreenFragment.java
• https://codepush.appcenter.ms/	com/microsoft/codepush/react/CodePush.java
• https://docs.swmansion.com/react-native-gesture-handler/docs/guides/migrating-off-rnghenabledroot	com/swmansion/gesturehandler/react/RNGestureHandlerEnabledRootView.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/265290532228/namespaces/firebase:fetch?key=AIzaSyAp17uB9n4iklHZQ1MOrRiIjf1cIa3XMD8 ）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。
HMS Core	Huawei	HMS Core 是华为终端云服务提供的端、云开放能力的合集，助您高效构建精品应用。

Huawei Push	Huawei	华为推送服务（HUAWEI Push Kit）是华为为开发者提供的消息推送平台，建立了从云端到终端的消息推送通道。开发者通过集成 HUAWEI Push Kit 可以实时推送消息到用户终端应用，构筑良好的用户关系，提升用户的感知度和活跃度。
Process Phoenix	JakeWharton	Process Phoenix facilitates restarting your application process.
vivo Push	vivo	vivo 推送是 Funtouch OS 上系统级消息推送平台，帮助开发者在 vivo 平台有效提升活跃和留存。通过和系统的深度结合，建立稳定可靠、安全可控、高性能的消息推送服务，帮助不同行业的开发者挖掘更多的运营价值。
MiPush	Xiaomi	小米消息推送服务在 MIUI 上为系统级通道，并且全平台通用，可以为开发者提供稳定、可靠、高效的推送服务。
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。
Firebase	Google	Firebase 提供了分析、数据库、消息传送和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
AppGallery Connect	Huawei	为开发者提供移动应用全生命周期服务，覆盖全终端全场景，降低开发成本，提升运营效率，助力商业成功。
HMS Core AAID	Huawei	华为推送服务开放能力合集提供的匿名设备标识（AAID）实体类与令牌实体类包。异步方式获取的 AAID 与令牌通过此包内对应的类承载返回。
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。
Meizu Push	Meizu	魅族推送服务是由魅族公司为开发者提供的消息推送服务，开发者可以向集成了魅族 push SDK 的客户端实时地推送通知或者消息，与用户保持互动，提高活跃率。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).
OPPO Push	OPPO	OPPO PUSH 是 ColorOS 上的系统级通道，为开发者提供稳定，高效的消息推送服务。

第三方追踪器检测

名称	类别	网址
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Huawei Mobile Services (HMS) Core	Location, Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/333
Microsoft Visual Studio App Center Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/243
Microsoft Visual Studio App Center Crashes	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/238

敏感凭证泄露检测

可能的密钥
小米推送的=> "XIAOMI_APPKEY" : "MI-您的，对应平台信息"
Engagelab-推送SDK的=> "ENGAGELAB_PRIVATES_CHANNEL" : "bitroo"
小米推送的=> "XIAOMI_APPID" : "MI-您的，对应平台信息"
vivo推送的=> "com.vivo.push.app_id" : "您的，对应平台信息"
OPPO推送的=> "OPPO_APPKEY" : "OP-您的，对应平台信息"
魅族推送的=> "MEIZU_APPID" : "MZ-您的，对应平台信息"
vivo推送的=> "com.vivo.push.api_key" : "您的，对应平台信息"
OPPO推送的=> "OPPO_APPSECRET" : "OP-您的，对应平台信息"
魅族推送的=> "MEIZU_APPKEY" : "MZ-您的，对应平台信息"
荣耀推送的=> "com.hihonor.push.app_id" : "您的，对应平台信息"
Engagelab-推送SDK的=> "ENGAGELAB_PRIVATES_APPKEY" : "8193455208d15f45459[illegible]"
OPPO推送的=> "OPPO_APPID" : "OP-您的，对应平台信息"
vivo推送的=> "local_iv" : "MzMsMzQsMzUsMzYsMzcsMzgsMzksNDAsNDEsMzIsMzgsMzcsMzYsMzUsMzQsMzMsI0AzNCwzMiwzMywzNywzMywzNCwzMiwzMywzMywzMywzNCw0MSwzNSwzNSwzMiwzMiwjQDM1LDM0LDM1LDM2LDM3LDM4LDM5LDQwLDQxLDMyLDM4LDM3LDMzLDM1LDM0LDMzLCNAMzQsMzIsMzMsMzcsMzMsMzQsMzIsMzMsMzMsMzIsMzQsNDEsMzUsMzgsMzI"
"CodePushDeploymentKey" : "gCSA80FK6eR0lAOn-0er[illegible]7hwpTt8COb"
"ENGAGELAB_PRIVATES_CHANNEL_high" : "HIGH"
"ENGAGELAB_PRIVATES_CHANNEL_low" : "LOW"
"ENGAGELAB_PRIVATES_CHANNEL_normal" : "NORMAL"
"ENGAGELAB_PRIVATES_CHANNEL_silence" : "SILENCE"
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"google_api_key" : "AIzaSyAp17uB9n4iklHZQ1MOrRiIjf1cIa3XMD8"
"google_app_id" : "1:265290532226:android:ce37221e04932a8bb7c9d1"
"google_crash_reporting_api_key" : "AIzaSyAp17uB9n4iklHZQ1MOrRiIjf1cIa3XMD8"
3267051002075881697803025130507043184471273380659243275938904335757337482424
6864797660130600812981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028191115057151
109384903807373427451111239076680556993620759895168374899458639449595311615073501601370873757375962324859213229670631330943845253159101291214232748847898598 4
1157920892103562487626974469494075735300861434152903141955336313088670978539 48

本报告由南明离火移动安全分析平台生成

383F2407-53F9-475B-87BD-6D2F1CE12105
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
55066263022277343669578718895168534326250603453777594175500187360389116729240
27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575
36134250956749795798585127919587881956611106672985015071877198253568414405109
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371361321113864768612440380340372808892707005449
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316
26617408020502170632287687167233609607298591687569731477066713684188029449964278084915450806277719028520942412250655586621571135455709168141616373158959998 46
375718002577002046354550722449118360359445513476976248669456777961554447744055631669123446501294553956214444453381428522585666729196580810124344277578376784
1157920892373161954235709850086879078532699846656405640394575840079088346716 63
39402006196394479212279040100143613805079739270465446667946905279627659399 1 3 3 6 3 5 6 9 3 9 8 9 5 6 3 0 8 1 5 2 2 9 4 2 1 7 5 5 4 3 3 6 5 3 9 4 2 6 4 3
26247035095799689268623156744566981891852923491109213387815615900926 5 1 8 8 5 4 7 3 8 0 5 0 0 8 9 0 2 2 3 8 8 0 5 3 5 9 7 9 1 9 7 8 6 6 5 0 8 7 2 4 7 6 7 3 2 0 8 7
39402006196394479212279040100143613805079739270465446667948293404245 2 1 7 7 1 4 9 6 8 7 0 3 2 9 0 4 7 6 6 0 8 8 2 5 8 9 3 8 0 0 1 8 6 1 6 0 6 9 7 3 1 1 2 3 1 9
1157920892373161954235709850086879078528375642790749048 2 6 0 1 4 3 1 4 1 5 1 8 1 6 1 4 9 4 3 3 7
4105836372515214212932612978004726840911444101599372 5 5 4 9 8 3 5 2 5 6 3 1 4 0 3 9 4 6 7 4 0 1 2 9 1
484395612939064517590525852527979142027629499260417479958440807170824046 85286
8325710961489029985546751289520108179287 5 3 0 4 8 8 6 1 3 1 5 5 9 4 7 0 9 2 0 5 9 0 2 4 8 0 5 1 3 1 9 9 8 8 4 4 1 9 2 2 4 4 3 8 6 4 3 7 6 0 3 9 2 9 4 7 3 3 3 0 7 8 0 8 6 5 1 1 6 2 7 8 7 1
1157920892103562487626974469494075125299969552241357605424221990610685120 44369
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999971664381257402829111505714 8

Google Play 应用市场信息

标题: Bitroo-BTC比特币算力租赁挖矿平台

评分: 2.5142858 **安装:** 10,000+ **价格:** 0 **Android版本支持:** **分类:** 财务 **Play Store URL:** com.bitroo.up

开发者信息: Bitroo, Bitroo, None, https://bitroo.com, app@bitroo.com,

发布日期: None **隐私政策:** Privacy link

关于此应用:

Bitroo 是一个专注于让普通用户更轻松地参与比特币挖矿的平台。我们提供便捷的比特币算力租赁和转售服务，专业的比特币矿机售卖、维护和托管服务，以及相关数字资产金融服务。我们致力于让挖矿更简单，让用户收益最大化，通过专业、诚信、创新、热情的态度服务好平台的每一位用户。 作为全球领先的算力租赁服务商，上线有经典模式、加速回本模式等多种算力租赁套餐，价格极具优势，一流的北美及中亚矿场，能够满足算力租赁的大额需要；团队拥有专业的技术和管理经验，使得设备能够以最高效的方式运作。 邀请好友超高返佣比例，无论好友购买算力租赁，还是购买矿机托管一站式服务，均可享有佣金返还，佣金每日结算，在这里不只是挖矿，还能赚钱！ 比特袋鼠（Bitroo）聚合了全球优秀矿池，如 BTC.com矿池、Antpool蚂蚁矿池、F2Pool鱼池、

免责声明及风险提示: