南明离火
移动应用检测平台

ANDROID 静态分析报告

ReposPartner • v1.51

分析日期: 2025-07-07 09:40:17

应用概览

文件名称:	ReposPartner.apk
文件大小:	22.83MB
应用名称:	ReposPartner
软件包名:	com.reposenergy.partner
主活动:	com.reposenergy.partner.MainActivity
版本号:	1.51
最小SDK:	26
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:	57/100 (中风险)
跟踪器检测:	3/432
杀软检测:	AI评估：安全
MD5:	99510500c928d093eea3f33b11820faa
SHA1:	3d70e38efa46ab[illegible]257f[illegible]bfb652dbc7c7599703
SHA256:	fe30ba065a4db040a281bc89cef621d040d3a896de49aff244193682a37cca4f

本报告由南明离火移动安全分析平台生成

分析结果严重性分布

高危	中危	信息	安全	关注
0	9	2	1	0

四大组件导出状态统计

Activity组件：7个，其中export的有： 0个
Service组件：7个，其中export的有： 0个
Receiver组件：3个，其中export的有： 1个
Provider组件：2个，其中export的有： 0个

应用签名证书信息

APK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: 2020-03-26 18:51:55+00:00
有效期至: 2050-03-26 18:51:55+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x877083cf738a5f1fcfa2c5679c89534752ceb79d
哈希算法: sha256
证书MD5: 228ab21b2a9107db19a76d145c987c27
证书SHA1: a9d5d59e31ffe301cc003705e9ba75e2bb875c07
证书SHA256: d28f7a3f182c65adf6e0d14568431e6fd464507a132926b047cf7354ce11bfd5
证书SHA512:
60a486184763b8bae7797e9f69def5bf7202363482f0c93b8b2b2c3f1a110f46e1c738949c379d87a3373f96b7407bb82d6439b223ac9a5ddc2838258273472

公钥算法: rsa
密钥长度: 4096
指纹: c1484d6d30b466a318a30a4db8305fd286dd0d1bc3783d3f00d5eed42a8c20e7
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.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.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。
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.repositorynergy.partner.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

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: **0** | 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: **2** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
2	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。

代码安全漏洞检测

高危: **0** | 警告: **4** | 信息: **1** | 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	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	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

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
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
00013	读取文件并将其放入流中	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
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
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
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
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
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
00036	从 res/raw 目录获取资源文件	反射	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	1/30	android.permission.WAKE_LOCK
其它常用权限	5/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.BLUETOOTH 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
repospetrolpump.firebaseio.com	安全	否	**IP地址:** 34.120.160.131 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
drf-media-data.s3.ap-south-1.amazonaws.com	安全	否	**IP地址:** 104.21.48.1 **国家:** 印度 **地区:** 马哈拉施特拉邦 **城市:** 孟买 **纬度:** 19.075975 **经度:** 72.877380 **查看:** Google 地图
reposenergy.com	安全	否	**IP地址:** 104.21.96.1 **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
drf.reposenergy.com	安全	否	**IP地址:** 104.21.96.1 **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

api.mixpanel.com	安全	否	**IP地址:** 35.190.25.25 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://drf.reposenergy.com/	com/reposenergy/partner/BuildConfig.java
• https://api.mixpanel.com	com/mixpanel/android/util/MPConstants.java
• https://reposenergy.com/terms-conditions/	com/reposenergy/partner/ui/referral/ReferralViewModel.java
• https://github.com/mixpanel/mixpanel-android/issues/567	com/mixpanel/android/mpmetrics/AnalyticsMessages.java
• https://reposenergy.com/terms-of-use/	com/reposenergy/partner/ui/pumps/overview/bottomsheets/AutoRateUpdateBottomSheetKt.java
• https://drf-media-data.s3.ap-south-1.amazonaws.com/pump-logos/new_bpcl.png	com/reposenergy/partner/ui/pumps/overview/OverviewRFSKt.java
• https://repospetrolpump.firebaseio.com	自研引擎-S

Firebase 配置安全检测

标题	严重程度	描述信息
应用与Firebase数据库通信	信息	该应用与位于 https://repospetrolpump.firebaseio.com 的 Firebase 数据库进行通信

Firebase远程配置已启用	警告	Firebase远程配置URL （ https://firebaseremoteconfig.googleapis.com/v1/projects/209167714498/namespaces/firebase:fetch?key=AIzaSyBhqsrQj9KpXuIY-HfFEMCIuj_Tbya_UCE ） 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": {
		"app_block_alert_message": "Hello, We have launched our new mobile application with a fresh UI and UX. Please update with our new Repos Petrol Pump app to avoid uninterrupted diesel delivery. Thank you for choosing Repos.",
		"app_block_alert_title": "Alert",
		"ios_alert_title": "Alert",
		"is_Delete_account_ios": "false",
		"is_app_block": "true",
		"is_ios_app_block": "false",
		"is_repos_app_block": "false",
		"new_app_url": "https://play.google.com/store/apps/details?id=com.reposenergy.partner&hl=en",
		"new_ios_app_url": "https://apps.apple.com/us/app/repos-petrol-pump/id1503747830?ls=1",
		"prod_latest_ed_partner_app_version": "39",
		"prod_latest_ed_partner_ios_app_version": "36",
		"prod_latest_ed_repos_partner_app_version": "34",
		"prod_latest_ed_repos_pertrol_pump_ios_app_version": "3.0",
		"prod_min_ed_partner_app_version": "39",
		"prod_min_ed_partner_ios_app_version": "36",
		"prod_min_ed_repos_partner_app_version": "34",
		"prod_min_ed_repos_pertol_pump_ios_app_version": "1.09",
		"update_message": "Hello, We have launched our new mobile application with a fresh UI and UX. Please update with our new Repos Petrol Pump app to avoid uninterrupted diesel delivery. Thank you for choosing Repos."
		},
		"state": "UPDATE",
		"templateVersion": "126"
		}

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。
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
techtest@gmail.com	com/reposenergy/partner/ui/pumps/dispenseReport/OnlineModeDispenseReportItemKt.java

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
MixPanel	Analytics	https://reports.exodus-privacy.eu.org/trackers/118

敏感凭证泄露检测

可能的密钥
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"firebase_database_url" : "https://repospetrolpump.firebaseio.com"
"google_api_key" : "AIzaSyBhqsrQj9KpXuIY-HfFEMCIuj_Tbya_UCE"
"google_app_id" : "1:209167714498:android:7ea4c928ba03aa3efd3f1b"
"google_crash_reporting_api_key" : "AIzaSyBhqsrQj9KpXuIY-HfFEMCIuj_Tbya_UCE"
"turkey" : "Turkije"
"turkey" : "Turki"
"turkey" : "Turquie"
"turkey" : "Turchia"
7b7b5090880094dbff5ab4ae1c274cf5
tvr9ilWoFNnKTkT2XuC54mEuIfon8rfpS2fqVys
ccccc694a29983c6d2252909d0a174d4
a3676a54bb335a2eeb4ef478b2fa8c9b
m167GreyOutlinedTrailingIconTextFieldvs558To

023620d011a70c8114f9c9038dc68154
KxvxDpiasLtCa8hyWZtFBQuDTVnx4PR10z1oLTkxREGgkYQrfzZNIrGWujM9qDfVN4HgpxgoCOBpdjlBTdYTYWqpyiXZ432fqnDezIANbH6zPWROxkaWGp3AIcoCDInj

Google Play 应用市场信息

标题: Repos Petrol Pump

评分: 3.8148148 **安装:** 10,000+ **价格:** 0 **Android版本支持:** **分类:** 办公 **Play Store URL:** com.reposenergy.partner

开发者信息: Repos Energy India Pvt Ltd., Repos+Energy+India+Pvt+Ltd., None, http://www.reposenergy.com/, technology.repos@gmail.com,

发布日期: 2020年3月26日 **隐私政策:** Privacy link

关于此应用:

您可能会问有什么新鲜事？ Repos Energy Partner 应用程序：为您的汽油泵业务加油！ 是时候升级你的座驾了！ Repos Energy Partner 应用程序刚刚进行了重大修改，旨在增强您的汽油泵管理。 做好准备： 即时销售洞察：实时查看您的销售业绩，像业务高手一样做出明智的决策。 轻松订购和付款：以闪电般的速度下订单、接受付款（在线和离线），不再落后。 信贷客户尽在掌握：发送提醒、一键收款，告别逾期麻烦。 现代、直观的设计：该应用程序现在同样时尚且易于使用。 立即更新并推动您的业务成功！ □□

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。