南明离火
移动应用检测平台

ANDROID 静态分析报告

PetTaxi • v1.92

分析日期: 2025-04-30 20:51:57

应用概览

文件名称:	PetTaxi v1.9.2.apk
文件大小:	7.95MB
应用名称:	PetTaxi
软件包名:	com.delviskesyty.PatTaxiTrack
主活动:	com.delviskesyty.PatTaxiTrack.ActivityPermission
版本号:	1.9.2
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:	47/100 (中风险)
杀软检测:	25 个杀毒软件报毒
MD5:	0decccеac663867bac1c032224041505
SHA1:	fe36dd5b0241960dce7e44cb0adf97c9cc6f92c8
SHA256:	0efc05c66d016f90b016612c8552d6950c66201d0b4b72c413e54c4ec2ff979e

分析结果严重性

高危	中危	信息	安全	关注
2	21	1	1	0

四大组件信息

Activity组件：6个，其中export的有：4个
Service组件：2个，其中export的有：1个
Receiver组件：2个，其中export的有：1个
Provider组件：1个，其中export的有：0个

证书信息

二进制文件已签名
v1 签名: False

v2 签名: False
v3 签名: True
v4 签名: False
主题: C=US, ST=Test, L=Test, O=Test, OU=Test, CN=Test
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-24 11:59:51+00:00
有效期至: 2052-09-09 11:59:51+00:00
发行人: C=US, ST=Test, L=Test, O=Test, OU=Test, CN=Test
序列号: 0xbcb332df175dd02b
哈希算法: sha256
证书MD5: 33585ec8b06d5f05676cd54a30f0e060
证书SHA1: 2e4c6668e464042898ce31d6848e00f0256aba82
证书SHA256: ebf37c54e7babfbecf918b02084bf006bfb6779ec16c8f9d034fbba8fe696b8d
证书SHA512:
7bce0c5514df40812a5832a44b375207f11ef59f750012d907932d56993ebdbbfc7bfb22a2917b6071c9fae0e263fc0485e2984b[illegible]e05e9f2a02dd971663c76e6

公钥算法: rsa
密钥长度: 2048
指纹: 72abb224436cec8ec9cdd3b340d7c8d237bb0fb2e6b64a156ee22bb5b85e7b4f
找到 1 个唯一证书

☰ 应用权限

权限名称	安全等级	权限内容	权限描述
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。
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.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收短信。 恶意程序会在用户未知的情况下监视或删除。
android.permission.BIND_NOTIFICATION_LISTENER_SERVICE	签名	NotificationListenerServices 需要用于系统绑定	必须是NotificationListenerService, 以确保只有系统可以绑定到。
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.SEND_SMS	危险	发送短信	允许应用程序发送短信。恶意应用程序可能会不经您的确认就发送信息，给您带来费用。
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。
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.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.RECEIVE_USSD_RESPONSE	未知	未知权限	来自 android 引用的未知权限。
android.permission.FOREGROUND_SERVICE_DATA_SYNC	普通	允许前台服务进行数据同步	允许常规应用程序使用类型为“dataSync”的 Service.startForeground。
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_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.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。
com.delviskesyty.PatTaxiTrack.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

序号	范围	严重级别	描述

证书安全分析

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	应用程序使用代码签名证书进行签名

MANIFEST分析

高危: **1** | 警告: **7** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	程序可被任意调试 [android:debuggable=true]	高危	应用可调试标签被开启，这使得逆向工程师更容易将调试器挂接到应用程序上。这允许导出堆栈跟踪和访问调试助手类。
2	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。
3	Activity (com.delviskesyty.PatTaxiTrack.MainActivity) 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	Activity (com.delviskesyty.PatTaxiTrack.ActivityPermission) 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。

5	Activity-Alias (com.delviskesyty.PatTaxiTrack.AlternativeIcon) 未被保护。[android:exported=true]	警告	发现 Activity-Alias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。
6	Activity-Alias (com.delviskesyty.PatTaxiTrack.StandardIcon) 未被保护。[android:exported=true]	警告	发现 Activity-Alias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。
7	Service (com.delviskesyty.PatTaxiTrack.MyNotificationListenerService) 受权限保护，但是应该检查权限的保护级别。Permission: android.permission.BIND_NOTIFICATION_LISTENER_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。
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。

</> 安全漏洞检测

高危: **1** | 警告: **4** | 信息: **1** | 安全: **0** | 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	应用了调试配置。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

5	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
6	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

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
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
00153	通过 HTTP 发送二进制数据	http	升级会员：解锁高级权限
00151	通过互联网发送电话号码	实时 隐私	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	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
00193	发送短信	短信	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
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
00191	获取短信收件箱中的消息	短信	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
00162	创建 InetSocketAddress 对象并连接到它	socket	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	7/30	android.permission.CALL_PHONE android.permission.READ_PHONE_STATE android.permission.READ_SMS android.permission.RECEIVE_SMS android.permission.SEND_SMS android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED

其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.FOREGROUND_SERVICE android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES

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。

URL链接分析

URL信息	源码文件
• 127.0.0.1	com/mongodb/gridfs/CLI.java
• 127.0.0.1	com/mongodb/ServerAddress.java

第三方SDK

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。
Jetpack ProfileInstaller	Google	以库能够提前预填充要由 ART 实现的编译轨迹。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).

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。对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。