



ANDROID 静态分析报告



EFFICIENT POS • v1.5.7

分析日期: 2025-08-04 08:00:47

i应用概览

文件名称:	EFFICIENT POS v1.5.7.apk
文件大小:	20.39MB
应用名称:	EFFICIENT POS
软件包名:	dev.gtr.pos
主活动:	dev.gtr.pos.activity.LoginActivity
版本号:	1.5.7
最小SDK:	21
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:	55/100 (中风险)
跟踪器检测:	2/432
杀软检测:	经检测，该文件安全
MD5:	7c1bbe7e6874eb3feb7b2e311f56217c
SHA1:	cf077061ddc2573d42c5a6351dcf07a071ff6b3fa
SHA256:	bc3513767e5672a634b59fef00da5cce6daabd872c92ecc2e029da7f0345d636

分析结果严重性分布

🚨 高危	⚠️ 中危	i 信息	✓ 安全	🔍 关注
0	12	1	1	0

四大组件导出状态统计

Activity组件: 36个，其中export的有: 1个
Service组件: 10个，其中export的有: 1个
Receiver组件: 11个，其中export的有: 1个

Provider组件: 5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: 2021-12-19 10:06:27+00:00

有效期至: 2051-12-19 10:06:27+00:00

发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

序列号: 0x62db8277a4a962656bf52096883802874cdde8c3

哈希算法: sha256

证书MD5: 832bc6fbc4852669e138d548d92b306

证书SHA1: 4776fc08cd5653b71a108885e3a7a7e6fd277a1e

证书SHA256: 5150415f5a547da4d9c2345376a8186ededede96481d6512e4d40bd9f1cb3ab077

证书SHA512: 9693756be7e39dec058c5d5bdb6d46817ca3b2f5a14c5149ce1a8731f7c661a2438f221837f561134c01d1e8fb0f98293da657e305e724241cd1b00fb26d1cf0

公钥算法: rsa

密钥长度: 4096

指纹: 9fdd1a3de96dc3c8a2a84753ced7908f256c42a21345f022b26073c6aeb85925

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.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.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.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.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.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.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_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.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.RECEIVE_BOOT_COMPLETE	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.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.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。
com.android.vending.CHECK_LICENSE	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: 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: 5 | 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、MediaPlayer 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	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。
3	Activity (dev.tr.pps.activity.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。

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。请在权限定义处检查其保护级别。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。请在权限定义处检查其保护级别。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: 5 | 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	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
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	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
5	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

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
7	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

应用行为分析

编号	行为	标签	文件
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
00193	发送短信	短信	升级会员：解锁高级权限
00183	获取当前相机参数并更改设置	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
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	5/30	android.permission.CAMERA android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	7/40	android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE com.google.android.gms.permission.AD_ID

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
pqstec.com	安全	否	IP地址: 36.255.68.97 国家: 孟加拉国 地区: 锡尔赫特 城市: 锡尔赫特 纬度: 24.896669 经度: 91.871674 查看: Google 地图
www.pqstec.com	安全	否	IP地址: 36.255.68.97 国家: 孟加拉国 地区: 锡尔赫特 城市: 锡尔赫特 纬度: 24.896669 经度: 91.871674 查看: Google 地图
journeyapps.com	安全	否	IP地址: 18.231.36 国家: 荷兰(王国) 地区: 北荷兰省 城市: 阿姆斯特丹 纬度: 52.378502 经度: 4.899980 查看: Google 地图

🌐 URL 链接安全分析

URL信息	源码文件
• https://pqstec.com/invoiceapps/home/signup	dev/gtr/pos/activity/LoginActivity.java
• https://www.pqstec.com/invoiceapps/home/loginapi?email=	dev/gtr/pos/fragment/DynamicMenuFragment.java
• https://www.pqstec.com/invoiceapps/	dev/gtr/pos/api/ApiClient.java
• 1.2.3.2	com/xiaofeng/flowlayoutmanager/BuildConfig.java
• https://journeyapps.com/ • https://github.com/journeyapps/zxing-android-embedded	自研引擎-S

☞ 第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。

ZXing Android Embedded	JourneyApps	Barcode scanning library for Android, using ZXing for decoding.
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，可帮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。
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。

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

敏感凭证泄露检测

可能的密钥
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"library_zxingandroidembedded_authors" : "JourneyApps"
"library_zxingandroidembedded_authorsWebsite" : "https://journeyapps.com/"

Google Play 应用市场信息

标题: Efficient POS
评分: 5 安装: 500+ 价格: 0 Android版本支持: 分类: 办公 Play Store URL: [dev.gtr.pos](#)
开发者信息: Genuine Technology & Research Limited, Genuine+Technology+%26+Research+Limited, None, https://www.pqstec.com/InvoiceApps_gtrltdbd@gmail.com,
发布日期: 2021年12月19日 隐私政策: [Privacy link](#)

关于此应用:

在 Pqstec.com/InvoiceApps 拥有帐户的用户 .. 他可以通过提供有效的用户 ID 和密码来使用此应用程序。

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，深入扫描软件中潜在的漏洞和安全隐患。

© 2025 南明离火 - 移动安全分析平台自动生成