南明离火
移动应用检测平台

ANDROID 静态分析报告

Auto Pay Solution v1.0

分析日期: 2025-04-05 12:06:20

应用概览

文件名称:	APP.apk
文件大小:	6.19MB
应用名称:	Auto Pay Solution
软件包名:	com.sms.worldpay
主活动:	com.sms.worldpay.SplashActivity
版本号:	1.0
最小SDK:	24
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:	41/100 (中风险)
杀软检测:	15 个杀毒软件报毒
MD5:	32b428519a42d3a91a7d484bd86bbd28
SHA1:	ce4f29a6095d669093ca14c4d2e92c18262724fd
SHA256:	939fd722676bcadc6a79d90a38a45cb0dff6f03cba895b04e173ae78f37a0b5

分析结果严重性分布

高危	中危	信息	安全	关注
4	10	1	1	0

四大组件导出状态统计

Activity组件：8个，其中export的有：2个
Service组件：1个，其中export的有：0个
Receiver组件：4个，其中export的有：4个
Provider组件：1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: False

v2 签名: True
v3 签名: False
v4 签名: False
主题: CN=Android Debug, O=Android, C=US
签名算法: rsassa_pkcs1v15
有效期自: 2024-08-24 14:00:27+00:00
有效期至: 2054-08-17 14:00:27+00:00
发行人: CN=Android Debug, O=Android, C=US
序列号: 0x1
哈希算法: sha256
证书MD5: 02d3176c574608c803700468a15aab3c
证书SHA1: 114ca8b0d80391cd36ebdd9cc4fb27255e319ec3
证书SHA256: 7f9fa9fc85b3120e53ec42934dbf234575f2f7f22d6ea621a9ff39fbb8a43795
证书SHA512:
3396319b1454b61b32993cf03328913f5f7487d797880e389b1915f7ceb48252d8301216e0e7818bcb9a3d06b9e2434dbd9a528e41cf506c0530505017181cfa

公钥算法: rsa
密钥长度: 2048
指纹: 5f230b46cdeb997a92ebbbcd9aa152f9c9c8c3e39840107ca779bf7ff7c30e77
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.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.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.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.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.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.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_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.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.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.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.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.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_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.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.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.REQUEST_COMPANION_RUN_IN_BACKGROUND	普通	允许配套应用程序在后台运行	允许配套应用在后台运行。
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.FOREGROUND_SERVICE_LOCATION	普通	允许前台服务与位置使用	允许常规应用程序使用类型为“location”的 Service.startForeground。
android.permission.DUMP	签名(系统)	获得系统内部状态	允许应用程序检索系统的内部状态。恶意应用程序可借此检索它们本不需要的各种保密信息和安全信息。
com.sms.worldpay.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

高危: **2** | 警告: **1** | 信息: **0** | 安全: **0**

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。
2	*	警告	基本配置配置为信任系统证书。
3	*	高危	基本配置配置为信任用户安装的证书。

证书安全合规分析

高危: **1** | 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
应用程序使用了调试证书进行签名	高危	应用程序使用了调试证书进行签名。生产环境的应用程序不能使用调试证书发布。

Manifest 配置安全分析

高危: **1** | 警告: **8** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
2	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。
3	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。它允许在启用了USB调试的用户从设备上复制应用程序数据。
4	Activity (com.sms.worldpay.LoginActivity) 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 (com.sms.worldpay.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。
6	Broadcast Receiver (com.sms.worldpay.BootReceiver) 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。
7	Broadcast Receiver (com.sms.worldpay.NetworkChangeReceiver) 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。
8	Broadcast Receiver (com.sms.worldpay.SmsReceiver) 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。
9	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。
10	高优先级的Intent（2147483647）- {1 个命中 [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。

代码安全漏洞检测

高危: **0** | 警告: **1** | 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	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
00097	获取短信的发送者地址并放入JSON中	信息收集 短信	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	11/30	android.permission.CAMERA android.permission.READ_PHONE_STATE android.permission.READ_SMS android.permission.RECEIVE_SMS android.permission.SEND_SMS android.permission.VIBRATE android.permission.RECEIVE_BOOT_COMPLETED android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.SYSTEM_ALERT_WINDOW android.permission.WAKE_LOCK
其它常用权限	7/46	android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET android.permission.FOREGROUND_SERVICE android.permission.ACCESS_WIFI_STATE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS

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
autopaysolutions.com	安全	否	**IP地址:** 104.21.8.237 **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://autopaysolution.com/api/add-data	com/sms/worldpay/SmsReceiver.java
• https://autopaysolution.com/api/device-connect	com/sms/worldpay/LoginActivity.java
• https://autopaysolution.com/api/add-data	com/sms/worldpay/MyBackgroundService.java

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。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
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。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。