南明离火
移动应用检测平台

ANDROID 静态分析报告

HK Pay • v6.1.4

分析日期: 2025-05-10 08:06:28

应用概览

文件名称:	HK Pay v6.1.4.apk
文件大小:	31.75MB
应用名称:	HK Pay
软件包名:	com.hk2025.droid
主活动:	crc64b09eeb05163e43a8.SplashScreen
版本号:	6.1.4
最小SDK:	21
目标SDK:	33
加固信息:	未加壳
开发框架:	Xamarin
应用程序安全分数:	61/100 (低风险)
杀软检测:	23 个杀毒软件报毒
MD5:	93d77c729fde806acbdc7412fd6e87dd
SHA1:	92977387b1565909156f63289[illegible]60bc5584c2b0f
SHA256:	29ee32f095977fa1f896[illegible]0e2584709539b22e702cd8b12b2997849ca3204b612

分析结果严重性分布

高危	中危	信息	安全	关注
0	5	1	1	0

四大组件导出状态统计

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

二进制文件已签名
v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: CN=hk2025_04
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-04 09:40:13+00:00
有效期至: 2050-03-29 09:40:13+00:00
发行人: CN=hk2025_04
序列号: 0x1
哈希算法: sha256
证书MD5: 74993065c433ea75ded6bc7adab2b13c
证书SHA1: 1e93382aca755d0632c4d766cd06e7d5775c12a3
证书SHA256: 1994ac243196b6861fd1d9b22cca8b93146ebebd1dd2f9aa596afaf1aed7c210
证书SHA512:
72044da58aee86bb633718b37b53893d69e5138706817c3f5a4173b4efba0e67d1b0960c6672d43e9a2ada410ec6a60e49d43e5321be5833ad6138ec2367adb4

公钥算法: rsa
密钥长度: 2048
指纹: f52a4375195a85fb4f92bb59cfc920d85851ff716e53e95c081e797ade15637d
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.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_MEDIA_LOCATION	危险	访问取照片的地址信息	更换头像，聊天图片等图片的地址信息被读取。
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.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.BIND_ACCESSIBILITY_SERVICE	签名	AccessibilityServices 需要进行系统绑定	必须由 AccessibilityService要求，以确保只有系统可以绑定到它。
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.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_CONTACTS	危险	读取联系人信息	允允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
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.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.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_BACKGROUND_LOCATION	危险	获取后台定位权限	允许应用程序访问后台位置。如果您正在请求此权限，则还必须请求ACCESS COARSE LOCATION或ACCESS FINE LOCATION。单独请求此权限不会授予您位置访问权限。
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.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.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
com.hk2025.droid.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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
crc64b09eeb05163e43a8.SchemeActivity	Schemes: hkwallet://,

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	应用程序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	Service (crc64b0136e1ff02eb898.DataFindAccessibilityService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_ACCESSIBILITY_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	Activity (crc64b09eeb05163e43a8.SchemeActivity) 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。
5	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: **0** | 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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	8/30	android.permission.SYSTEM_ALERT_WINDOW android.permission.READ_PHONE_STATE android.permission.READ_CONTACTS android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.READ_SMS android.permission.SEND_SMS android.permission.RECEIVE_SMS

本报告由南明离火移动安全分析平台生成

其它常用权限	7/46	android.permission.INTERNET android.permission.READ_MEDIA_IMAGES android.permission.FOREGROUND_SERVICE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_BACKGROUND_LOCATION

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 链接安全分析

URL信息	源码文件
• https://rapi.mobikwik.com/recharge/connections?categoryId=mobile • https://www.mobikwik.com • https://www.freecharge.in	自研引擎-A

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Xamarin	Microsoft	Xamarin 是一个跨平台开发软件，通过使用 C# 共享的代码库，开发人员可以使用 Xamarin 工具，使用本地用户界面编写原生的 Android、iOS 和 Windows 应用程序，并跨多个平台（包括 Windows 和 MacOS）共享代码。
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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
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。