



ANDROID 静态分析报告



开运通 • v1.0.8

分析日期: 2024-05-20 15:22:45

i应用概览

文件名称:	CRnBlw3dUjQT5Sc1h1LX.apk
文件大小:	15.15MB
应用名称:	开运通
软件包名:	com.kaidianbao.kyt
主活动:	com.kaidianbao.kyt.login.SplashActivity
版本号:	1.0.8
最小SDK:	19
目标SDK:	26
加固信息:	360加固 加固
应用程序安全分数:	24/100 (重大风险)
跟踪器检测:	1/432
杀软检测:	3 个杀毒软件报毒
MD5:	fdd7ac0ed3a9262567efa3c7f2c8cc5e
SHA1:	d69de8cc0fa3034388c77da4149b71a2dafa039e
SHA256:	536e251170df15293a877fabe2c1b10aa31baac53350b5664d4a9515f5a3d33a

📊分析结果严重性分布

🚨 高危	⚠️ 中危	ℹ️ 信息	✓ 安全	🔍 关注
24	20	2	1	5

📦四大组件导出状态统计

Activity组件: 69个, 其中export的有: 9个
Service组件: 1个, 其中export的有: 0个
Receiver组件: 0个, 其中export的有: 0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: True
v2 签名: False
v3 签名: False
v4 签名: False
主题: C=123, ST=123, L=123, O=123, OU=123, CN=123
签名算法: rsassa_pkcs1v15
有效期自: 2023-05-31 07:14:43+00:00
有效期至: 2048-05-24 07:14:43+00:00
发行人: C=123, ST=123, L=123, O=123, OU=123, CN=123
序列号: 0x6c094ea0
哈希算法: sha256
证书MD5: 615c8fa61feb93255423f0487668dca4
证书SHA1: a93b8878affa74a165e8679a6b9278df8c047dc1
证书SHA256: aca548f93c3e5fc623ad0ba0f2925ba6f59e35a9b65761499a11fc29ac4b999c
证书SHA512:
2437a07cbf50265f4dc0d550f1285777c2a1f64a78a23a18cdcfb4fe8a6eddb912ddca1455070e9447868f10253da9ad7840b041e72490a68a61592135faa4b2

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_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.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.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.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_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.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错略的经纬度信息，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.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。但不被允许拨打紧急电话。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。
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.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.SYSTEM_OVERLAY_WINDOW	未知	未知权限	来自 android 引用的未知权限。

android.permission.KILL_BACKGROUND_PROCESSES	普通	结束进程	允许应用程序结束其他应用程序的后台进程。
android.permission.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.READ_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。
com.work.xxj.permission.JPUSH_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
android.permission.RECEIVE_USER_PRESENT	普通	允许程序唤醒机器	允许应用可以接收点亮屏幕或解锁广播。
android.permission.NFC	危险	控制nfc功能	允许应用程序与支持nfc的物体交互。
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.kaidianbao.kyt.activity.ActivityReal	Schemes: kaixinfu://, Hosts: com.kaidianbao.happypay, Paths: /ActivityReal,
com.kaidianbao.kyt.MainActivity	Schemes: kaixinfu://, Hosts: com.kaidianbao.happypay, Paths: /MainActivity,

网络通信安全风险分析

高危: 1 | 警告: 0 | 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。

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	应用程序已使用代码签名证书进行签名
应用程序存在Janus漏洞	高危	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

Manifest 配置安全分析

高危: 15 | 警告: 10 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 4.4-4.4.4, [minSdk=19]	信息	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	应用程序具有网络安全配置 [android:networkSecurityCo nfig=@xml/net_fonfig]	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。
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。它允许已经启用了USB调试的用户从设备上复制应用程序数据。
4	Activity (com.kaidianbao.kyt.wxapi.WXEntryActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的敏感信息。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
5	Activity (com.kaidianbao.kyt.wxapi.WXEntryActivity) 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为"singleTask"。然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。这使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为"singleInstance"或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。您还可以将应用的目标 SDK 版本 (26) 更新到 28 或更高版本以在平台级别修复此问题。
6	Activity (com.kaidianbao.kyt.wxapi.WXEntryActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为"singleInstance"并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (26) 更新到 29 或更高版本以在平台级别修复此问题。
7	Activity (com.kaidianbao.kyt.wxapi.WXEntryActivity) 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。
8	Activity (com.kaidianbao.kyt.wxapi.WXEntryActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为"singleInstance"并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (26) 更新到 29 或更高版本以在平台级别修复此问题。
9	Activity-Alias (com.kaidianbao.kyt.wxapi.WXEntryActivity) 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。
10	Activity (com.kaidianbao.kyt.wxapi.WXPayEntryActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为"singleInstance"并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (26) 更新到 29 或更高版本以在平台级别修复此问题。
11	Activity (com.kaidianbao.kyt.wxapi.WXPayEntryActivity) 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。

12	Activity (com.kaidianbao.kyt.activity.ReadActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
13	Activity (com.kaidianbao.kyt.activity.ActivityReal) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
14	Activity (com.kaidianbao.kyt.activity.ActivityTempPay) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
15	Activity (com.kaidianbao.kyt.MainActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
16	Activity (com.kaidianbao.kyt.MainActivity) 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为 "singleTask"。然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。这使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为 "singleInstance" 或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。您还可以将应用的目标 SDK 版本 (21) 更新到 28 或更高版本以在平台级别修复此问题。
17	Activity (com.kaidianbao.kyt.MainActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
18	Activity (com.kaidianbao.kyt.login.LoginActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
19	Activity (com.kaidianbao.kyt.login.LoginActivity) 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为 "singleTask"。然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。这使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为 "singleInstance" 或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。您还可以将应用的目标 SDK 版本 (26) 更新到 28 或更高版本以在平台级别修复此问题。
20	Activity (com.alipay.sdk.app.PayResultActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
21	Activity (com.alipay.sdk.app.PayResultActivity) 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。
22	Activity (com.alipay.sdk.app.AlipayResultActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
23	Activity (com.alipay.sdk.app.AlipayResultActivity) 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为 "singleTask"。然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。这使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为 "singleInstance" 或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。您还可以将应用的目标 SDK 版本 (26) 更新到 28 或更高版本以在平台级别修复此问题。

24	Activity (com.alipay.sdk.app .AlipayResultActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity=”)来修复此漏洞。您还可以将应用的目标 SDK 版本 (26) 更新到 29 或更高版本以在平台级别修复此问题。
25	Activity (com.alipay.sdk.app .AlipayResultActivity) 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。
26	Activity (com.mylhyl.acp.AcpActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
27	Activity (com.mylhyl.acp.AcpActivity) 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”，然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。这使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity=”)属性来修复此漏洞。您还可以将应用的目标 SDK 版本 (26) 更新到 28 或更高版本以在平台级别修复此问题。

代码安全漏洞检测

高危: 7 | 警告: 8 | 信息: 2 | 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: M3: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
3	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
4	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
5	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限

6	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击。	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
7	WebView域控制不严格漏洞	高危	CWE: CWE-73: 外部控制文件名或路径	升级会员：解锁高级权限
8	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
9	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
10	已启用远程WebView调试	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M11: Improper Platform Usage OWASP MASVS: MSTG-RSTORAGE-2	升级会员：解锁高级权限
11	该文件是World Readable。任何应用程序都可以读取文件。	高危	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
12	应用程序在加密算法中使用ECB模式。ECB模式是已知的弱模式，因为它对相同的明文块生成相同的密文。	高危	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	升级会员：解锁高级权限
13	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限

14	使用弱加密算法	高危	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
15	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
16	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
17	应用程序创建临时文件。敏感信息永远不应该被写入临时文件	警告	CWE: CWE-276: 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
18	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-BEAT-101-7	升级会员：解锁高级权限

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	RELRO	RP AT H (指定SO搜索路径)	R U N P A T H (指定SO搜索路径)	FORTIFY(常用函数加强检查)	SY M B O L S T R I P P E D (裁剪符号表)
1	arm64-v8a/libtoken.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数：['_memcpy_chk', '_strcat_chk', '_strlen_chk', '_memset_chk', '_strcpy_chk', '_vsprintf_chk', '_memmove_chk']	False warning 符号可用

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 android.permission.CAMERA android.permission.READ_PHONE_STATE android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.CALL_PHONE android.permission.REQUEST_INSTALL_PACKAGES android.permission.READ_CONTACTS android.permission.SYSTEM_ALERT_WINDOW android.permission.MODIFY_AUDIO_SETTINGS android.permission.RECORD_AUDIO

其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE android.permission.FLASHLIGHT
--------	------	--

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
h5.hunanwanxin.com	安全	是	IP地址: 39.104.166.130 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图
txt.go.sohu.com	安全	是	IP地址: 47.110.177.60 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图
kxf-gw.candypay.com	安全	是	IP地址: 47.110.177.60 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图
kxf.hunanwanxin.com	安全	是	IP地址: 47.110.177.60 国家: 中国 地区: 浙江 城市: 杭州 纬度: 30.293650 经度: 120.161583 查看: 高德地图
kf.hunanwanxin.com	安全	是	IP地址: 39.104.67.105 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图

🌐 URL 链接安全分析

URL信息	源码文件
-------	------

- https://testapp.xinhucaifu.com/Public/images/012.png - https://testapp.xinhucaifu.com/Public/images/010.png - https://testapp.xinhucaifu.com/Public/images/006.png - https://testapp.xinhucaifu.com/Public/images/002.png - https://testapp.xinhucaifu.com/Public/images/009.png - https://testapp.xinhucaifu.com/Public/images/016.png - https://testapp.xinhucaifu.com/Public/images/017.png - https://testapp.xinhucaifu.com/Public/images/920.png - https://testapp.xinhucaifu.com/Public/images/007.png - https://testapp.xinhucaifu.com/Public/images/015.png - https://testapp.xinhucaifu.com/Public/images/004.png - https://testapp.xinhucaifu.com/Public/images/005.png - https://testapp.xinhucaifu.com/Public/images/011.png - https://testapp.xinhucaifu.com/Public/images/934.png - https://testapp.xinhucaifu.com/Public/images/003.png - https://testapp.xinhucaifu.com/Public/images/014.png	自研引擎-A
- javascript:webviewjavascriptbridge._fetchqueue - javascript:webviewjavascriptbridge	com.github.lzyzsd/jsbridge/BridgeUtil.java
javascript:webviewjavascriptbridge._fetchqueue	com.github.lzyzsd/jsbridge/BridgeWebView.java
file:anonymous-string	com.hp.hpl.sparta/parser.java
- https://kxf.hunanwanxin.com/qualification/kdb_licence.jpg - https://kxf.hunanwanxin.com/qualification/publicity.jpg - https://kxf.hunanwanxin.com/qualification/soft1.jpg - https://kxf.hunanwanxin.com/qualification/soft2.jpg	com.kaidianbao/kyt/activity/ActivityCompany.java
http://192.168.0.165:8848/kxf_h5_client/client/view/index.html	com.kaidianbao/kyt/activity/WebView1Activity.java
http://192.168.0.165:8848/kxf_h5_client/client/view/index.html	com.kaidianbao/kyt/activity/WebViewActivity.java
- https://kxf-gw.candypay.com - http://kf.hunanwanxin.com/ - https://kxf.hunanwanxin.com/realback.html - https://h5.hunanwanxin.com/kxf_register_15/#/	com.kaidianbao/kyt/config/Api.java
http://txt.go.sohu.com/ip/soip	com.kaidianbao/kyt/config/ApiUtils.java
- https://kxf.hunanwanxin.com/qualification/xieyi3.html - https://kxf.hunanwanxin.com/qualification/xieyi1.html - https://kxf.hunanwanxin.com/qualification/xieyi2.html - https://kxf.hunanwanxin.com/qualification/xieyi4.html	com.kaidianbao/kyt/config/Constant.java
- javascript:live800appconnector.switchtohuman - javascript:live800appconnector.config.closechat - javascript:live800appconnector.closechat	com.kaidianbao/kyt/js/Live800JSBridge.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Fresco	Facebook	Fresco 是一个用于管理图像及其使用的内存的 Android 库。

GIFLIB	GIFLIB	The GIFLIB project maintains the giflib service library, which has been pulling images out of GIFs since 1989. It is deployed everywhere you can think of and some places you probably can't - graphics applications and web browsers on multiple operating systems, game consoles, smartphones, and likely your ATM too.
360 加固	360	360 加固保是基于 360 核心加密技术，给安卓应用进行深度加密、加壳保护的安全技术产品，可保护应用远离恶意破解、反编译、二次打包，内存抓取等威胁。
支付宝 SDK	Alipay	支付宝开放平台基于支付宝海量用户，将强大的支付、营销、数据能力，通过接口等形式开放给第三方合作伙伴，帮助第三方合作伙伴创建更具竞争力的应用。
ZXing Android Embedded	JourneyApps	Barcode scanning library for Android, using ZXing for decoding.
EasyPermissions	Google	EasyPermissions 是一个包装器库，用于简化针对 Android M 或更高版本的基本系统权限逻辑。
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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

🕒 第三方追踪器检测

名称	类别	网址
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116

🔑 敏感凭证泄露检测

可能的密钥
9F090200019F1E083132333435363738
410f9ab135fe779f7c9259cdcfffb87a
f185b71f614c30a396ac4bc44d3269
6X8Y4XdM2Vhvn0KfzcEatGnWaNIk=
64227f56d64e68613955bf11
7E9DF0AC98093B13BBAF0C37057F2F09
7e158509216bb1c3aa4cf72165af043a

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