南明离火
移动应用检测平台

ANDROID 静态分析报告

久爱 • v5.0.2

分析日期: 2024-05-12 22:35:43

应用概览

文件名称:	760482eeff12db5358c2da3ac32142d6.apk
文件大小:	41.24MB
应用名称:	久爱
软件包名:	com.piyknsrtmv.piamihfurt
主活动:	com.vQkHXOkN.NpmcSwlz.OUWzguifRlXuYetK
版本号:	5.0.2
最小SDK:	23
目标SDK:	29
加固信息:	资源混淆
应用程序安全分数:	47/100 (中风险)
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	760482eeff12db5358c2da3ac32142d6
SHA1:	e77a71ec328a00e725beb2eb13a2299316293602
SHA256:	81414c55721d6e593538ec77349f0fcc6c86283204879686ff4898fcd55f96f

分析结果严重性分布

高危	中危	信息	安全	关注
2	9	13	1	4

四大组件导出状态统计

Activity组件：8个，其中export的有：0个
Service组件：2个，其中export的有：1个
Receiver组件：4个，其中export的有：3个
Provider组件：4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: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2024-05-12 13:12:45+00:00
有效期至: 2079-02-13 13:12:45+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0x6fb7e0f3b26b4053
哈希算法: sha256
证书MD5: d0d32f992144059033e9e2975e1bbc74
证书SHA1: f1c4323207c872809f56bea1f6da6b8c7dd21eee
证书SHA256: 11eeea55e07d97f4dfd314241d645f3a1c4539558d54d18008407b71a0cfc46e
证书SHA512:
c269d9cd542225f7733bfdde55c8503ed7aeb8017e4a91d30dcdafc342b897643ba28ed937f5181cc7c9f11fdad6937ae612d87b0f0c2a987a98145e46456593

公钥算法: rsa
密钥长度: 2048
指纹: 305f091ff1ab26b5688f3d99b2d83bb6a94da8a23e16495cfd0bcd3fdae988a4
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.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.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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
android.permission.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
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.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.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
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.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.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.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.PACKAGE_USAGE_STATS	签名	更新组件使用统计	允许修改组件使用情况统计
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.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.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[illegible]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。
com.piyknsrtmv.piamihfurt.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
android.permission.READ_PRIVILEGED_PHONE_STATE	未知	未知权限	来自 android 引用的未知权限。
android.permission.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。

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: **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

Manifest 配置安全分析

高危: **0** | 警告: **6** | 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 6.0-6.0.1, [minSdk=23]	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	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。

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	Broadcast Receiver (com.vQkHXOkN.NpmcSwlz.JhhjRXCJEfNtWsgr) 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。
5	Broadcast Receiver (com.vQkHXOkN.NpmcSwlz.gRgySSeRiUAcaaSM) 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。
6	Service (com.vQkHXOkN.NpmcSwlz.XGwXGeYFbLZAbSlE) 未被保护。 [android:exported=true]	警告	发现 Service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 (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。

代码安全漏洞检测

高危: **2** | 警告: **2** | 信息: **3** | 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
2	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
3	应用程序记录日志信息，不应记录敏感信息	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
4	应用程序可以写入应用程序目录。敏感信息应加密	信息	CWE: CWE-276: 默认权限不正确 OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
5	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	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
7	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	13/30	android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.WRITE_SETTINGS android.permission.WAKE_LOCK android.permission.READ_PHONE_STATE android.permission.GET_TASKS android.permission.RECEIVE_BOOT_COMPLETED android.permission.SYSTEM_ALERT_WINDOW android.permission.REQUEST_INSTALL_PACKAGES android.permission.VIBRATE android.permission.PACKAGE_USAGE_STATS android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION
其它常用权限	9/46	android.permission.READ_EXTERNAL_STORAGE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FLASHLIGHT android.permission.FOREGROUND_SERVICE android.permission.ACCESS_WIFI_STATE android.permission.BLUETOOTH android.permission.CHANGE_NETWORK_STATE

常用: 已知恶意软件经常滥用的权限。

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

apm-native.xiaohongshu.com	安全	是	**IP地址:** 58.222.45.38 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
wiki.xiaohongshu.com	安全	是	**IP地址:** 114.117.3.118 **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
www.xiaohongshu.com	安全	是	**IP地址:** 58.222.45.38 **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
picasso-static.xiaohongshu.com	安全	是	**IP地址:** 58.222.45.38 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• www.xiaohongshu.com	dd0/j.java
• https://www.xiaohongshu.com/hina/matrix	id0/d.java
• https://www.xiaohongshu.com/picasso_pages/author-center/main?fullscreen=true • https://www.xiaohongshu.com/company/home?fullscreen=true • https://www.xiaohongshu.com/creator/comment/list	qh0/d.java
• https://picasso-static.xiaohongshu.com/fe-platform/723b8946ece112aaecc80d591b17f43764cce6d4.png	qh0/g.java
• https://apm-native.xiaohongshu.com/	w90/d.java
• https://apm-native.xiaohongshu.com/api/collect	w90/e.java
• https://wiki.xiaohongshu.com/pages/viewpage.action?pageid=227883302	wb0/a.java
• https://wiki.xiaohongshu.com/pages/viewpage.action?pageid=227883302	wb0/b.java
• https://wiki.xiaohongshu.com/pages/viewpage.action?pageid=227883302	wb0/c.java
• https://wiki.xiaohongshu.com/pages/viewpage.action?pageid=227883302	wb0/d.java
• https://wiki.xiaohongshu.com/pages/viewpage.action?pageid=227883302	wb0/h.java

• www.xiaohongshu.com	yg0/a.java
• https://wiki.xiaohongshu.com/pages/viewpage.action?pageid=227883302 • https://www.xiaohongshu.com/company/home?fullscreen=true • www.xiaohongshu.com • https://www.xiaohongshu.com/picasso_pages/author-center/main?fullscreen=true • https://www.xiaohongshu.com/creator/comment-list • https://apm-native.xiaohongshu.com/api/collect • https://www.xiaohongshu.com/hina/match • https://apm-native.xiaohongshu.com/ • https://picasso-static.xiaohongshu.com/fe-platform/723b8946ece112aaecc80d591b17f43764cce6d4.png	自研引擎-S

邮箱地址敏感信息提取

EMAIL	源码文件
xhs@xhs.com	id0/a.java
xhs@xhs.com	自研引擎-S

敏感凭证泄露检测

可能的密钥
凭证信息=> "com.appinstall.APP_KEY" : "sp8cqc"
723b8946ece112aaecc80d591b17f43764cce6d4

免责声明及风险提示: