南明离火
移动应用检测平台

ANDROID 静态分析报告

心跳 • v5.0.7

分析日期: 2025-03-10 16:48:20

应用概览

文件名称:	f54d76b7a05c5c383c1d7543011334a4f8ff229bc13019b99cee2d76a896ecc7.apk
文件大小:	40.34MB
应用名称:	心 跳
软件包名:	com.vnpqkfmmdm.xqlumzlqeq
主活动:	com.nTFlImPo.FiPOlhtD.NisYncufDyxnrZTI
版本号:	5.0.2
最小SDK:	16
目标SDK:	27
加固信息:	未加壳
开发框架:	Flutter
应用程序安全分数:	42/100 (中风险)
杀软检测:	3 个杀毒软件报毒
MD5:	8afc70bff6d23529167afe9268005220
SHA1:	f91f3a2a62745b35121d9bfb3268092f48df2cfc
SHA256:	f54d76b7a05c5c383c1d7543011334a4f8ff229bc13019b99cee2d76a896ecc7

分析结果严重性

高危	中危	信息	安全	关注
3	6	1	1	0

四大组件信息

Activity组件：8个，其中export的有：5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

证书信息

二进制文件已签名
v1 签名: False

本报告由南明离火移动安全分析平台生成

v2 签名: True
v3 签名: False
v4 签名: None
主题: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2023-12-04 16:01:27+00:00
有效期至: 2078-09-06 16:01:27+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0xfc2637f59fed8ba3
哈希算法: sha256
证书MD5: 2d0d53ed93ef11f4692c6ebdf194894e
证书SHA1: 6e4121f44bcdd1dd9530fe1219f97bc46e612404
证书SHA256: 202638e9f530bffa01ed6b26ba3445fbce62f33919a55f4f3eb28207b84a82bc
证书SHA512:
53884ff42872132ed93608b1af2a1ec91fba22840df24db1310f41ce4720bbfe02997a1af8fe3d496548d1f1acc0c8624b14ce06e105d9d79aa1155291d35bea

公钥算法: rsa
密钥长度: 2048
指纹: b2319e687ad99f824bdb0836f4b51be10f80919896697ea5238553e904061edf
找到 1 个唯一证书

应用权限

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.startForegr ound，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。
com.vnpqkfmmdm.xqlumzlqeq.DYNAMIC_RECEIV ER_NOT_EXPORTED_PERMISSION	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

序号	范围	严重级别	描述

证书安全分析

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	应用程序使用代码签名证书进行签名

MANIFEST分析

高危: **3** | 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。
2	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。

3	Activity (com.nTFlImPo.FiPOlhtD.NisYncufDyxnrZTI) 容易受到StrandHogg 2.0的攻击	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 (27) 更新到 29 或更高版本以在平台级别修复此问题。
4	Broadcast Receiver (com.nTFlImPo.FiPOlhtD.BoirgTQonzEvwlZI) 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.nTFlImPo.FiPOlhtD.IqgzZcYMuwsaIjlP) 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.nTFlImPo.FiPOlhtD.LmdqnOXwQKunbhIc) 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	Activity (com.nTFlImPo.FiPOlhtD.JelocycBwxsVdfev) 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。
8	Activity (com.nTFlImPo.FiPOlhtD.wkRpjnEEnXEYdBdJ) 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。
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。

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

行为分析

编号	行为	标签	文件
00102	将手机扬声器设置为打开	命令	升级会员：解锁高级权限
00028	从assets目录中读取文件	文件	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

00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限

敏感权限分析

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。

密钥凭证

可能的密钥
凭证信息=> "com.appinstall.APP_KEY": "kn0b2v"

免责声明及风险提示: