



## ANDROID 静态分析报告



◆ 爱春 · v8.0.8

本报告由南明离火移动安全分析平台生成  
本报告由南明离火移动安全分析平台生成

分析日期: 2025-03-11 10:07:32

## i应用概览

文件名称:	2gfJREFnMT_2.apk
文件大小:	48.99MB
应用名称:	爱春
软件包名:	cww.eqjhsuzhmnjlk.ogywn.my2yt
主活动:	ouldnsrm.euyqess.c6kyyyg.ey5w1jk.jfd4bjj.MainActivity
版本号:	8.0.8
最小SDK:	24
目标SDK:	34
加固信息:	未加壳
开发框架:	Flutter
应用程序安全分数:	64/100 (低风险)
杀软检测:	AI评估: 很危险, 请谨慎安装
MD5:	12b0b5f2aa7417feec73dabb16b3fa57
SHA1:	31c8607973401d9926e07aaf51790f45106248ee
SHA256:	496e29d2e04307103abf381ddbe1a52ab3f06daa014f095cd25f14d1dde1a903

## 分析结果严重性

高危	中危	信息	安全	关注
0	4	0	1	0

## 四大组件信息

Activity组件: 40个, 其中export的有: 0个
Service组件: 5个, 其中export的有: 1个
Receiver组件: 2个, 其中export的有: 1个
Provider组件: 1个, 其中export的有: 0个

## 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=CN, ST=Beijing, L=Beijing, O=XQJZnkSZ, OU=dXxAYsYB, CN=IExQnRaQ  
 签名算法: dsa  
 有效期自: 2025-03-10 01:30:13+00:00  
 有效期至: 2026-12-31 01:30:13+00:00  
 发行人: C=CN, ST=Beijing, L=Beijing, O=XQJZnkSZ, OU=dXxAYsYB, CN=IExQnRaQ  
 序列号: 0x2f665dae  
 哈希算法: sha256  
 证书MD5: d46642f05b1f55d94d6c5f229b0e0f61  
 证书SHA1: 6bb569421540e3c89541f5ce1c93d7a8662acae6  
 证书SHA256: 49080b877ac9204ad0d5abe3fcc6e2b9f543d614a17133818cde3cc6e0d9bdbb  
 证书SHA512: 3f88f76ba68ca922d70e157234f0c9f2908d7521f54f7994b9a06dd9b695e0299bf6e717a2e8a8f4ac3f712b9f802e49644281f0c91770bc6bbb9fe1e0d75da5  
 公钥算法: dsa  
 密钥长度: 2048  
 指纹: c0a639dc043f0eb08082c00545e708bf61d03c2894811f178965ee6c921c9597  
 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_MEDIA_VISUAL_USER_SELECTED	危险	允许从外部存储读取用户选择的图像或视频文件	允许应用程序从用户通过权限提示照片选择器选择的外部存储中读取图像或视频文件。应用程序可以检查此权限以验证用户是否决定使用照片选择器，而不是授予对 READ_MEDIA_IMAGES 或 READ_MEDIA_VIDEO 的访问权限。它不会阻止应用程序手动访问标准照片选择器。应与 READ_MEDIA_IMAGES 和/或 READ_MEDIA_VIDEO 一起请求此权限，具体取决于所需的媒体类型。
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.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.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
android.permission.READ_MEDIA_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。
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立即自行启动。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	Android 8.0 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.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.POST_NOTIFICATIONS	危险	发送通知的运行权限	允许应用发布通知，Android 13 引入的新权限。
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.FOREGROUND_SERVICE_MEDIA_PLAYBACK	普通	启用用于媒体播放的前台服务	允许常规应用程序使用类型为“mediaPlayback”的 Service.startForeground。
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.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。
cwv.eqjbsvwhnrljlk.ogywn.my2yt.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
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。
android.permission.READ_PRIVILEGED_PHONE_STATE	签名(系统)	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。



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: 0 | 警告: 3 | 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	Broadcast Receiver (androidx.profileinstaller.ProfileInstallerReceiver) 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。它列出了一个在分析的应用程序中未定义的权限的保护，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。
3	Service (mhpmbdbm.nhm5mgu.k0nziH.BgTasksUp) 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。

## 安全漏洞检测

序号	问题	等级	参考标准	文件位置
----	----	----	------	------

## 动态库分析

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	RELRO	RPATH (指定SO搜索路径)	RUNPATH (指定SO搜索路径)	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED (裁剪符号表)
1	armeabi-v7a/libluibwunsemMAoBm.so	True <b>info</b> 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。	动态共享对象(DSO) <b>info</b> 共享库是使用-fPIC标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程(ROP)攻击更难可靠地执行。	True <b>info</b> 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 <b>info</b> 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 <b>info</b> 二进制文件没有设置运行时搜索路径或RPATH	None <b>info</b> 二进制文件没有设置RUNPATH	False <b>warning</b> 二进制文件没有任何加固函数。加固函数提供了针对glibc的常见不安全函数(如strcpy, gets等)的缓冲区溢出检查。使用编译选项-D_FORTIFY_SOURCE=2来加固函数。这个检查对于Dart/Flutter库不适用	True <b>info</b> 符号被剥离

### :::敏感权限分析

类型	匹配	权限
----	----	----

恶意软件常用权限	14/30	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 android.permission.MODIFY_AUDIO_SETTINGS
其它常用权限	12/46	android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.READ_MEDIA_AUDIO android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FLASHLIGHT android.permission.FOREGROUND_SERVICE android.permission.BLUETOOTH android.permission.ACCESS_WIFI_STATE 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=> "org.patess.subbad.sional.Pxphgeg.apikcy" : "qj1lrcS3ltLztp0YqYtfmWd7teTHesFwiFeUo0wL2"
凭证信息=> "com.appinstall.APP_KEY" : "w6v148bp"
凭证信息=> "CjEv5ZzdyKKey" : "HlwTrQITPpytlGy8Q7gqfcz3SUPph7Q"
凭证信息=> "GPAIWiltWKey" : "EnhJ80JXWwCU56u6A0zEXc3V9FwiEKWT49q"
凭证信息=> "org.wzr.phosere.etrotue.Gdnucpdocpcj.apikcy" : "9chqMWHI7aWi41BnlZHPbmpweOq1z6oWWzR"
凭证信息=> "z3x9PDW8C9UKey" : "9BvmpF1AaVoSMOkqz5REKqj8Kagn2YFa6R1Ep"
"agora_app_id" : "0b01e68e03524c1b920d5c9c2e3185e0"

## 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

本报告由南明离火移动安全分析平台生成

本报告由南明离火移动安全分析平台生成