南明离火

移动应用检测平台

ANDROID 静态分析报告

暗 香 • v5.0.2

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: 2024-03-31 18:32:39

应用概览

文件名称:	base.apk
文件大小:	41.28MB
应用名称:	暗 香
软件包名:	com.dcwmwmcbpt.pjwwzwkhnn
主活动:	com.rDjAXYof.bAuStdEf.EBDCDRagTXtlpOEM
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:	61/100 (低风险)
杀软检测:	1 个杀毒软件报毒
MD5:	3b3b1c7d895455204fe5b5ff11045ca0
SHA1:	7748cadcc7f380e1db62fc728fb6556bd928d034
SHA256:	d89978a437d7b4d561d7a340458d3eb912db0341498237f52a1023a57e7e6e91

分析结果严重性分布

高危	中危	信息	安全	关注
0	0	1	1	1

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：0个
Receiver组件：4个，其中export的有：2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: False

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

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: 2024-03-24 04:25:22+00:00
有效期至: 2078-12-26 04:25:22+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0xf94e6b9842c7753d
哈希算法: sha256
证书MD5: d0c0a99287d6a2e2a064af985d2ffc83
证书SHA1: de61e8e26dff67f9a4007eef7ad8db66ea493174
证书SHA256: 3a6e0101c4ba57778df3909e7e7350b445522adfef2242675a5dcd1f7698faa9
证书SHA512:
cdc745d3f25ed52e431abf2fcdd33031735214caff597483a5eafa6ddbcf7e0cf9f9ceabb52f05676b39d0cebb41bac531cf8b1805159cd1e54412e64a3c723c

公钥算法: rsa
密钥长度: 2048
指纹: 55491c17fe5eda870156ef1b037d7cd4fcb4d4df33234b440fe0dadc222743c8
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。

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

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.dcwmwmcbpt.pjwwzwkhnn.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: **4** | 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]	警告	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。

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

2	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，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	Broadcast Receiver (com.rDjAXYof.bAuStdEf.SsmsMjJfKOSRzyAp) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。
4	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: **0** | 警告: **1** | 信息: **1** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	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	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

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

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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
www.xiaohongshu.com	安全	是	**IP地址:** 81.69.116.87 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 查看: 高德地图

URL 链接安全分析

URL信息	源码文件
• https://res.wx.qq.com/open/js/jweixin-1.3.2.js • http://es5.github.io/ • http://support.dun.163.com/feedback/captcha • http://es5.github.com/	自研引擎分析结果
• https://www.xiaohongshu.com/experience/home?fullscreen=true	pr2/h.java
• https://www.xiaohongshu.com/api/hawking/h5/redirect?scene_code=cooper_center	pr2/j.java
• www.xiaohongshu.com/user/shopping_cart?isrn=true&rnname=shopping-cart&rnpath=user/shopping_cart	pr2/z.java
• https://www.xiaohongshu.com/login/other/question	te2/n.java
• www.xiaohongshu.com/user/shopping_cart?isrn=true&rnname=shopping-cart&rnpath=user/shopping_cart	tr2/a0.java
• https://www.xiaohongshu.com/experience/home?fullscreen=true	tr2/i.java
• https://www.xiaohongshu.com/api/hawking/h5/redirect?scene_code=cooper_center	tr2/k.java

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

• https://www.xiaohongshu.com/experience/home?fullscreen=true • https://www.xiaohongshu.com/login/otherquestion • www.xiaohongshu.com/user/shopping_cart?isrn=true&rnname=shopping-cart&rnpath=user/shopping_cart • https://www.xiaohongshu.com/api/hawking/h5/redirect?scene_code=cooper_center	自研引擎分析结果

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