南明离火
移动应用检测平台

ANDROID 静态分析报告

锐公考 • v3.1.0

分析日期: 2024-07-16 13:37:42

应用概览

文件名称:	锐公考.apk
文件大小:	14.81MB
应用名称:	锐公考
软件包名:	com.hanzi.ruigongkao
主活动:	com.hanzi.ruigongkao.ui.launch.LaunchActivity
版本号:	3.1.0
最小SDK:	19
目标SDK:	28
加固信息:	360加固 加固
应用程序安全分数:	60/100 (低风险)
杀软检测:	14 个杀毒软件报毒
MD5:	50a72e98504a3c5b4e040afc62f3c910
SHA1:	3577e5c9c21b3dfe6b37aa91f84920810a25d2fc
SHA256:	93aa237074a7b9dc8d61b41a39a[illegible]3461400e67dce78763d0a37ac2511e7c3d1

分析结果严重性分布

高危	中危	信息	安全	关注
0	6	0	1	0

四大组件导出状态统计

Activity组件：[illegible]，其中export的有：3个
Service组件：3个，其中export的有：0个
Receiver组件：1个，其中export的有：1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: True
v3 签名: False

v4 签名: False
主题: C=cn, ST=gd, L=gz, O=cn, OU=hanzi, CN=hjq
签名算法: rsassa_pkcs1v15
有效期自: 2017-12-20 07:43:44+00:00
有效期至: 2042-12-14 07:43:44+00:00
发行人: C=cn, ST=gd, L=gz, O=cn, OU=hanzi, CN=hjq
序列号: 0x133dba48
哈希算法: sha256
证书MD5: fdbe86a88ca02dd8b0312ea7977d9de4
证书SHA1: 6b20f0804bfbb96de4c4e2bfb2e52373397fffdb
证书SHA256: 77dc5803cd34f06eafda3d51d3bede708730ec7c03017d462100bdedb890823e
证书SHA512:
841f9fa4ced537835a4a54cd1d69b4ee2ae08710529692ad4360a64aba2a5213719aa676e472c813291d293e5d5902d58e5b227edfd49f1[illegible]63afa81b78fd4e

公钥算法: rsa
密钥长度: 2048
指纹: 3aceb99f5fe5487001551d8c6927120a592ee97fd1ebcd9ae04002d8a0403e7e
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.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.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.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.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.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.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.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.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.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.tencent.tauth.AuthActivity	Schemes: tencent1106505850://,

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: **1** | 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: **5** | 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.hanzi.ruigongkao.receiver.DownloadApkReceiver) 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	Activity (com.tencent.tauth.AuthActivity) 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。
5	Activity (com.sina.weibo.sdk.share.WbShareTransActivity) 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。
6	Activity (com.sina.weibo.sdk.share.WbShareToStoryActivity) 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。

代码安全漏洞检测

序号	问题	等级	参考标准	文件位置

敏感权限滥用分析

类型	匹配	权限

恶意软件常用权限	4/30	android.permission.READ_PHONE_STATE android.permission.CAMERA android.permission.SYSTEM_ALERT_WINDOW android.permission.WRITE_SETTINGS
其它常用权限	6/46	android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.CHANGE_WIFI_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。

URL 链接安全分析

URL信息	源码文件
• https://github.com/vinc3m1 • https://github.com/vinc3m1/roundedimageview • https://github.com/vinc3m1/roundedimageview.git	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
360 加固	360	360 加固保是基于 360 核心加密技术，对安卓应用进行深度加密、加壳保护的安全技术产品，可保护应用远离反编译破解、反编译、二次打包、内存抓取等威胁。
LibVLC	VideoLAN	VLC 是一款免费、自由、开源的跨平台多媒体播放器及框架，可播放大多数多媒体文件，以及各类流媒体协议。
微博 SDK	Weibo	微博 Android 平台 SDK 为第三方应用提供了简单易用的微博 API 调用服务，使第三方客户端无需了解复杂的验证机制即可进行授权登陆，并提供微博分享功能，可直接通过微博官方客户端分享微博。

敏感凭证泄露检测

可能的密钥
友盟统计的=> "UMENG_CHANNEL" : "qh360"
友盟统计的=> "UMENG_APPKEY" : "5a5643d2b27b0a59c70000f3"
凭证信息=> "WEIBO_APPKEY" : "947632163"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"

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隐患。