南明离火
移动应用检测平台

ANDROID 静态分析报告

殇痕画质助手 • v9.7.52.0

分析日期: 2025-04-26 07:04:47

应用概览

文件名称:	殇痕画质助手 v9.7.5.apk
文件大小:	18.63MB
应用名称:	殇痕画质助手
软件包名:	com.Wecrane.Scar.pubg
主活动:	com.iapp.app.run.mian
版本号:	9.7.52.0
最小SDK:	25
目标SDK:	31
加固信息:	360加固
开发框架:	iApp(裕语言)
应用程序安全分数:	68/100 (低风险)
杀软检测:	13 个杀毒软件报毒
MD5:	66f70a118e0cf28f40ff979bf51b7c43
SHA1:	e023acb1a44b4e954d4e83fcf80a941a0f0aaf90
SHA256:	656dbe847bebdd0f3f876e11d69dae6966511e38f2c4dcc00b4b9579d8831b7

分析结果严重性

高危	中危	信息	安全	关注
1	2	1	2	0

四大组件信息

Activity组件：10个，其中export的有：0个
Service组件：0个，其中export的有：0个
Receiver组件：0个，其中export的有：0个
Provider组件：2个，其中export的有：1个

证书信息

二进制文件已签名
v1 签名: False

v2 签名: True
v3 签名: True
v4 签名: False
主题: C=CN
签名算法: rsassa_pkcs1v15
有效期自: 2023-01-21 03:35:49+00:00
有效期至: 2048-01-15 03:35:49+00:00
发行人: C=CN
序列号: 0x29e85484
哈希算法: sha256
证书MD5: 984a3354d3ac955dc0ec6da1c288ae53
证书SHA1: e1a48843ea96998029e21c4fce8fb443e3cb558f
证书SHA256: e5a95c01c34cbbd14ee11f48ce35a17e77382fa860b4f2b28ddc18a1ada89387
证书SHA512:
85be9047734162617e8353d1686c24b8dd87bd9af7e896acc7604acc417f947a85f48542d270db61ef2067e48b43e9b9ff5d8716f9dc776a2c62769dceb8148b

公钥算法: rsa
密钥长度: 2048
指纹: 07ca8292238d452c85ab6dfe51cf0c24d338661f3c26b4cc6b4200fbf941d19a
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.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.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.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.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.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.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.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。
moe.shizuku.manager.permission.API_V23	未知	未知权限	来自 android 引用的未知权限。

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: 0 | 警告: 2 | 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	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/APKTOOL_DUPLICATE_xml_0x7f120002]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
3	Content Provider (rikka.shizuku.ShizukuProvider) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.INTERACT_ACROSS_USERS_FULL [android:exported=true]	警告	发现一个 Content Provider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。它受到一个正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: 1 | 警告: 0 | 信息: 1 | 安全: 1 | 屏蔽: 0

序号	问题	等级	参考标准	文件位置
1	启用了调试配置。生产版本不能是可调试的	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	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
3	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限

行为分析

编号	行为	标签	文件
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
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

敏感权限分析

类型	匹配	权限
恶意软件常用权限	1/30	android.permission.SYSTEM_ALERT_WINDOW
其它常用权限	4/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_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。

域名检测

域名	状态	中国境内	位置信息
iappzy.com	安全	否	No Geolocation information available.

URL链接分析

URL信息	源码文件
• https://www.baidu.com • http://xht.ychz.top/upload/202307210006426578.jpg	自研引擎-A
• http://iappzy.com/a.png	com/mx/MainActivity.java

第三方SDK

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，给安卓应用进行深度加密、加壳保护的安全技术产品，可保护应用远离恶意破解、反编译、二次打包，内存抓取等威胁。
AndroLua	mkottman	AndroLua 是基于 LuaJava 开发的安卓平台轻量级脚本编程语言工具，既具有 Lua 简洁优雅的特质，又支持绝大部分安卓 API，可以使你在手机上快速编写小型应用。
android-gif-drawable	koral--	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。
iApp	iApp	将想法变为现实一款国产手机端可视化编程软件。

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。