南明离火
移动应用检测平台

ANDROID 静态分析报告

狙击准星助手 • v3.4

分析日期: 2025-08-25 10:27:47

应用概览

文件名称:	jujizhunxingzhushou.apk
文件大小:	2.17MB
应用名称:	狙击准星助手
软件包名:	com.snipehelper.jjzx
主活动:	com.iapp.app.logoActivity
版本号:	3.4
最小SDK:	9
目标SDK:	21
加固信息:	未加壳
开发框架:	iApp(裕语言)
应用程序安全分数:	39/100 (高风险)
杀软检测:	34 个杀毒软件报毒
MD5:	39f0d6f028ccfb745c3feea1e1015994
SHA1:	3db85262ef52c1b12ec02bfb1e6501ca708133e
SHA256:	3c93beb4f614a6[illegible]c3bfa7f562923eb2ec002a2b2a9498248d2002fa9

分析结果严重性分布

高危	中危	信息	安全	关注
4	7	1	1	0

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：0个，其中export的有： 0个
Receiver组件：0个，其中export的有： 0个
Provider组件：0个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: True
v2 签名: False
v3 签名: False
v4 签名: False
主题: C=cn, ST=bj, L=bj, O=ipuser, OU=ipuser, CN=ipuser
签名算法: rsassa_pkcs1v15
有效期自: 2016-07-02 11:43:26+00:00
有效期至: 2098-08-21 11:43:26+00:00
发行人: C=cn, ST=bj, L=bj, O=ipuser, OU=ipuser, CN=ipuser
序列号: 0x3435f5c4
哈希算法: sha256
证书MD5: c118816b9a0f406ba5ba053c67638185
证书SHA1: ae773917cc7a7523b41e1eb95bed61cf0aa8e3b0
证书SHA256: ac0d0777ca24956f8d584c69a7fd5d2e4fb88e276d953aec9e29ceeb9aa78e32
证书SHA512:
4667da273fe54297d8c90136e189f721a4bf15ba360aac00f095756e2ed09e59edcf69e08cddd20c379bff8f2b4d59c0fcb3ad5ed3c93[illegible]472c8a85a40a21f5

共检测到 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.READ_CONTACTS	危险	读取联系人信息	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
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_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.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_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。

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: 1 | 警告: 0 | 信息: 1

标题	严重程度	描述信息

已签名应用	信息	应用已使用代码签名证书进行签名。
存在 Janus 漏洞风险	高危	仅使用 v1 签名方案，Android 5.0-8.0 设备易受 Janus 漏洞影响。若同时存在 v1 和 v2/v3 签名，Android 5.0-7.0 设备同样存在风险。

Manifest 配置安全分析

高危: **0** | 警告: **0** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息

代码安全漏洞检测

高危: **3** | 警告: **7** | 信息: **1** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	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	如果一个应用程序使用WebView的loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
4	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
5	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限

6	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限
7	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
8	默认情况下，调用Cipher.getInstance("AES")将返回AES ECB模式。众所周知，ECB模式很弱，因为它导致相同明文块的密文相同	高危	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	升级会员：解锁高级权限
9	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
10	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限
11	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限

应用行为分析

编号	行为	标签	文件

00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00054	从文件安装其他APK	反射	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
00072	将 HTTP 输入流写入文件	命令 网络 文件	升级会员：解锁高级权限
00108	从给定的 URL 读取输入流	网络 命令	升级会员：解锁高级权限
00183	获取当前相机参数并更改设置	相机	升级会员：解锁高级权限
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00202	打电话	控制	升级会员：解锁高级权限
00080	将录制的音频/视频保存到文件	录制音视频 文件	升级会员：解锁高级权限
00203	将电话号码放入意图中	控制	升级会员：解锁高级权限
00101	初始化录音机	录制音视频	升级会员：解锁高级权限
00199	停止录音并释放录音资源	录制音视频	升级会员：解锁高级权限
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00198	初始化录音机并开始录音	录制音视频	升级会员：解锁高级权限
00136	停止录音	录制音视频 命令	升级会员：解锁高级权限
00194	设置音源（MIC）和录制文件格式	录制音视频	升级会员：解锁高级权限
00090	设置录制的音频/视频文件格式	录制音视频	升级会员：解锁高级权限
00197	设置音频编码器并初始化录音机	录制音视频	升级会员：解锁高级权限
00067	查询IMSI号码	信息收集	升级会员：解锁高级权限
00138	设置音频源（MIC）	录制音视频	升级会员：解锁高级权限
00196	设置录制文件格式和输出路径	录制音视频 文件	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	升级会员：解锁高级权限
00133	开始录音	录制音视频 命令	升级会员：解锁高级权限
00083	查询IMEI号	信息收集 电话服务	升级会员：解锁高级权限

00104	检查给定路径是否是目录	文件	升级会员：解锁高级权限
00041	将录制的音频/视频保存到文件	录制音视频	升级会员：解锁高级权限
00001	初始化位图对象并将数据（例如JPEG）压缩为位图对象	相机	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00094	连接到 URL 并从中读取数据	命令 网络	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
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00153	通过 HTTP 发送二进制数据	http	升级会员：解锁高级权限
00009	将游标中的数据放入JSON对象	文件	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00208	捕获设备屏幕的内容	信息收集 屏幕	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	3/30	android.permission.READ_CONTACTS android.permission.SYSTEM_ALERT_WINDOW android.permission.READ_PHONE_STATE
其它常用权限	3/46	android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.INTERNET

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
iapp.yx93.com	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• http://iapp.yx93.com:8881/	com/iapp/app/dx.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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程序应用。
iApp	iApp	将想法变为现实一款国产手机端可视化编程软件。
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。

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。