南明离火
移动应用检测平台

ANDROID 静态分析报告

2112小工具 • v1.0

分析日期: 2025-11-21 23:14:56

应用概览

文件名称:	2112小工具 v1.0.apk
文件大小:	4.39MB
应用名称:	2112小工具
软件包名:	site.xgj
主活动:	com.iapp.app.run.mian
版本号:	1.0
最小SDK:	15
目标SDK:	31
加固信息:	未加壳
开发框架:	iApp
应用程序安全分数:	60/100 (低风险)
杀软检测:	22 个杀毒软件报毒
MD5:	553fb5f69d1be3dedd8a03f5be4b7f97
SHA1:	d7ba030287512ed5d11c8e3[illegible]a4c743e79a
SHA256:	897de9e8dd9f0804fe07bc[illegible]8a095a3bc52ea37375c6e[illegible]8931e8cb3bc3a043

分析结果严重性分布

高危	危	信息	安全	关注
1	6	2	2	0

四大组件导出状态统计

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：1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: True
v3 签名: True
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:
4667da273fe54297d8c90136e189f721a4bf15ba360aac00f095756e2ed09e59edcf69e08cddd20c379bff78f3b4d59c0fcb3ad5ed3b93dc472c8a85a40a21f5

公钥算法: rsa
密钥长度: 2048
指纹: 8bbf61332bce2af8264b5b6a580609a347650411f6732d955346f9f5fe76cf86
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
i.app	未知	未知权限	来自 android 引用的未知权限。
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.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.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.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。

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全分析

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: **1** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	应用已配置网络安全策略 [android:networkSecurityConfig=@7F120002]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。

代码安全漏洞检测

高危: **1** | 警告: **5** | 信息: **2** | 安全: **1** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	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
3	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
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	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限

7	如果一个应用程序使用WebView.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
8	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
9	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-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
00054	从文件安装其他APK	反射	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
00036	从 res/raw 目录获取资源文件	反射	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
00091	从广播中检索数据	信息收集	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
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
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
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
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
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
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
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
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
00101	初始化录音机	录制音视频	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
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
00025	监视要执行的一般操作	反射	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
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
00182	打开相机	相机	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
00133	开始录音	录制音视频 命令	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
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
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
00160	使用辅助服务执行通过视图 ID 获取节点信息的操作	无障碍服务	升级会员：解锁高级权限
00161	对可访问性节点信息执行可访问性服务操作	无障碍服务	升级会员：解锁高级权限
00159	使用辅助服务执行通过文本获取节点信息的操作	无障碍服务	升级会员：解锁高级权限
00173	获取 AccessibilityNodeInfo 屏幕中的边界并执行操作	无障碍服务	升级会员：解锁高级权限
00019	从给定的类名中查找方法，通常用于反射	反射	升级会员：解锁高级权限
00046	方法反射	反射	升级会员：解锁高级权限
00026	方法反射	反射	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
00030	通过给定的 URL 连接到远程服务器	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

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
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
00029	动态初始化类对象	反射	升级会员：解锁高级权限
00039	启动网络服务器	控制 网络	升级会员：解锁高级权限
00002	打开相机并拍照	相机	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	1/30	android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	3/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE

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.objectweb.org	安全	否	**IP地址:** 87.228.10.221 **国家:** 俄罗斯联邦 **地区:** 桑克-彼得堡 **城市:** 圣彼得堡 **纬度:** 59.894440 **经度:** 30.264200 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• www.objectweb.org	bsh/ClassGeneratorUtil.java
• www.objectweb.org	自研引擎-S

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。
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。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

邮箱地址敏感信息提取

EMAIL	源码文件
pat@pat.net	bsh/Interpreter.java
pat@pat.net	自研引擎-S

免责声明及风险提示: