南明离火
移动应用检测平台

ANDROID 静态分析报告

无极分享社 • v9.0

本报告由南明离火移动安全分析平台生成

分析日期: 2025-05-17 07:59:58

应用概览

文件名称:	无极分享社.apk
文件大小:	8.18MB
应用名称:	无极分享社
软件包名:	com.wuji
主活动:	com.rjd.ruanjiankv.activity.HomeActivity
版本号:	9.0
最小SDK:	21
目标SDK:	28
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	46/100 (中风险)
杀软检测:	10 个杀毒软件报毒
MD5:	c9a9fa9fd334a2358a28b6bb2e92043a
SHA1:	209734b8620bdbcc49e77c49725f089bf8eb8979
SHA256:	79fa28ddd2c238742b2775602284be1554c092552eb47ddd928d3257189c291a

分析结果严重性分布

高危	中危	信息	安全	关注
4	1	2	2	5

四大组件导出状态统计

Activity组件：3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
签名算法: rsassa_pkcs1v15
有效期自: 2023-09-27 07:02:40+00:00
有效期至: 2048-09-20 07:02:40+00:00
发行人: C=CN
序列号: 0x599b4c5c
哈希算法: sha256
证书MD5: 8ba23712ba4177374b7de38743f9b058
证书SHA1: dd2e75b64622523ca1456385bb8a90f4f3fbc994
证书SHA256: 4f66bd3d4a111a666748415503b86aaf5ed4d605ce57c08f629a92b2445a2537
证书SHA512:
56a323129ec8f79a1de102f51cb9d861087d1d0249b8ec0d2b1a58a3ffac2ba4c42d3564bd1450ee3fd6c8376cb6556877011a1c37cb73dd68d263feaf133c51

公钥算法: rsa
密钥长度: 2048
指纹: eb8394c0ffbab216e67ac0bf7524b6b8a312b1b63e294ae4aaf5a22270975fbb
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.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.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.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
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.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.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.MANAGE_EXTERNAL_STORAGE	危险	广泛的文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。
android.permission.SET_WALLPAPER	普通	设置壁纸	允许应用程序设置壁纸。
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.REORDER_TASKS	危险	对正在运行的应用程序重新排序	允许应用程序将任务移至前端和后台。恶意应用程序可借此强行进入前端，而不受您的控制。
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.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.BIND_VPN_SERVICE	签名	VpnServices 需要进行系统绑定	必须是VpnService, 以确保只有系统可以绑定到它。
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	应用已使用代码签名证书进行签名。

Manifest 配置安全分析

高危: **1** | 警告: **2** | 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	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
3	Activity (com.rjd.ruanjiankv.activity.HomeActivity) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。

代码安全漏洞检测

高危: **3** | 警告: **8** | 信息: **2** | 安全: **1** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-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	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

4	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
5	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
6	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
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	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
9	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
10	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
11	已启用远程WebView调试	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

12	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
13	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
14	该文件是World Writable。任何应用程序都可以写入文件	高危	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

应用行为分析

编号	行为	标签	文件
00014	将文件读入流并将其放入 JSON 对象中	文件	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
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
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入 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
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
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
00023	从当前应用程序启动另一个应用程序	反射 控制	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
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	短信	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
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

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
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
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
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
00163	创建新的 Socket 并连接到它	socket	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
00202	打电话	控制	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
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
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
00034	查询当前数据网络类型	信息收集 网络	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.REQUEST_INSTALL_PACKAGES android.permission.SET_WALLPAPER android.permission.READ_PHONE_STATE
其它常用权限	7/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE android.permission.REORDER_TASKS android.permission.FOREGROUND_SERVICE

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
yymao.pro	安全	否	No Geolocation information available.

static.woozooo.com	安全	是	**IP地址:** 58.221.70.116 **国家:** 中国 **地区:** 江苏 **城市:** 南通 **纬度:** 32.030296 **经度:** 120.874779 **查看:** 高德地图
wwp.lanzout.com	安全	是	**IP地址:** 58.221.70.116 **国家:** 中国 **地区:** 江苏 **城市:** 南通 **纬度:** 32.030296 **经度:** 120.874779 **查看:** 高德地图
img-home.csdnimg.cn	安全	是	**IP地址:** 123.2.116.64 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
aria.laoyuyu.me	安全	否	No Geolocation information available.
t.me	安全	否	**IP地址:** 149.154.167.99 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 英格兰 **城市:** 伦敦 **纬度:** 51.508530 **经度:** -0.125740 **查看:** Google 地图
rjlm.pro	安全	是	**IP地址:** 8.210.81.134 **国家:** 中国 **地区:** 香港 **城市:** 香港 **纬度:** 22.285521 **经度:** 114.157692 **查看:** 高德地图
www.lanzouy.com	安全	是	**IP地址:** 58.221.70.116 **国家:** 中国 **地区:** 江苏 **城市:** 南通 **纬度:** 32.030296 **经度:** 120.874779 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• https://yq7.lanzout.com/b00taxcb9g • https://www.lanzouo.com/b00tayeuva • https://www.lanzouo.com/b00tayxfle • https://wwp.lanzout.com/b00taxcb9g • https://wwp.lanzout.com/b00tapbsfa	自研引擎-A

• https://aria.laoyuyu.me/aria_doc/other/annotaion_invalid.html	com/arialyy/aria/core/upload/UploadReceiver.java
• 104.19.244.87	mirrorb/android/app/job/C0032.java
• 172.64.139.148	mirrorb/android/app/job/C0044.java
• 172.64.139.148	mirrorb/android/app/job/C0029.java
• http://yymao.pro/	com/rjd/ruanjiankv/adapter/HomeAppListAdapter.java
• 162.159.243.215	mirrorb/android/webkit/C0089.java
• 104.19.81.88	mirrorb/android/webkit/C0088.java
• 104.18.124.253	com/cloudinject/customview/C0027.java
• 104.18.124.253	com/cloudinject/customview/C0020.java
• 172.64.197.29	mirrorb/android/media/session/C0048.java
• 162.159.253.217	mirrorb/android/view/accessibility/C0087.java
• 162.159.243.215	mirrorb/android/webkit/C0074.java
• 104.19.81.88	mirrorb/android/webkit/C0073.java
• https://img-home.csdnimg.cn/images/20201124032511.png	com/rjd/ruanjiankv/fragment/BrowserFragment.java
• https://aria.laoyuyu.me/aria_doc/create/any_java.html	com/arialyy/aria/core/Aria.java
• https://wwp.lanzout.com/b00tayekgf • http://rjlm.pro/gx.txt	com/rjd/ruanjiankv/fragment/HomeTwoFragment.java
• http://rjlm.pro/gx.txt	com/rjd/ruanjiankv/fragment/AppListFragment.java
• https://static.woozooo.com/ico	com/rjd/ruanjiankv/adapter/AppListAdapter.java
• 172.64.203.72	mirrorb/android/hardware/display/C0061.java
• 172.64.203.72	mirrorb/android/hardware/display/C0046.java
• 104.21.234.149	mirrorb/android/app/role/C0050.java
• https://aria.laoyuyu.me/aria_doc/other/annotaion_invalid.html	com/arialyy/aria/core/download/DownloadReceiver.java
• 172.64.197.29	mirrorb/android/media/session/C0063.java
• 162.159.253.217	mirrorb/android/view/accessibility/C0072.java

• https://www.lanzouy.com/ajaxm.php	com/rjd/ruanjiankv/utils/LanzouHelper.java
• 172.64.110.164	mirrorb/android/app/servertransaction/C0053.java
• 104.19.109.228	mirrorb/android/net/wifi/C0053.java
• 172.64.110.164	mirrorb/android/app/servertransaction/C0038.java
• 162.159.38.227	mirrorb/android/service/persistentdata/C0068.java
• 104.18.115.242 • 172.64.102.243	mirrorb/android/service/persistentdata/C0067.java
• 104.22.31.162	mirrorb/java/io/C0106.java
• 104.18.115.242 • 172.64.102.243	mirrorb/android/service/persistentdata/C0082.java
• 162.159.38.227	mirrorb/android/service/persistentdata/C0083.java
• 104.19.109.228	mirrorb/android/net/wifi/C0068.java
• 104.22.31.162	mirrorb/java/io/C0091.java
• http://undefined/	org/jsoup/helper/HttpConnection.java
• 104.19.78.48	mirrorb/android/providers/C0059.java
• 104.21.231.104	mirrorb/android/os/storage/C0072.java
• 172.64.109.246	mirrorb/android/bluetooth/C0042.java
• 104.19.78.48	mirrorb/android/providers/C0074.java
• 104.21.234.149	mirrorb/android/app/role/C0035.java
• https://github.com/arialyy/aria/issues/597	com/arialyy/aria/core/download/m3u8/M3U8Option.java
• 1.9.2.6	com/arialyy/aria/http/upload/HttpUThreadTaskAdapter.java
• 172.64.109.246	mirrorb/android/bluetooth/C0057.java
• 104.19.244.87	mirrorb/android/app/job/C0047.java
• http://www.baidu.com/?	com/rjd/ruanjiankv/activity/HomeActivity.java
• 104.21.231.104	mirrorb/android/os/storage/C0057.java
• 172.64.141.217	mirrorb/android/graphics/drawable/C0060.java
• https://static.woozooo.com/ico/	com/rjd/ruanjiankv/adapter/AppHotAdapter.java

• 172.64.141.217	mirrorb/android/graphics/drawable/C0045.java
• 172.64.136.152	mirrorb/android/security/net/config/C0080.java
• 104.18.127.20	mirrorb/android/rms/C0078.java
• 104.19.31.141	mirrorb/android/rms/C0079.java
• 104.18.127.20	mirrorb/android/rms/C0063.java
• 172.64.136.152	mirrorb/android/security/net/config/C0065.java
• 104.19.31.141	mirrorb/android/rms/C0064.java
• https://wwp.lanzout.com/b00tayekgf • https://t.me/dddddffxxr	system/security/Dialogue.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
AgentWeb	Justson	AgentWeb 是一个基于的 Android WebView ， 极度容易使用以及功能强大的库，提供了 Android WebView 一系列的问题解决方案，并且轻量和极度灵活。
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相关的文件。
Jetpack App Startup	Google	App Startup 库提供了一种直接，高效的方法来在应用程序启动时初始化组件。库开发人员和应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。
Picasso	Square	一个强大的 Android 图片下载缓存库。

敏感凭证泄露检测

可能的密钥
4ddc39c1fb01d2864c6485e1e29c470
46a6b6c26f186c30000242d50cf1f9f

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。