南明离火
移动应用检测平台

ANDROID 静态分析报告

尾巴漫画 • v1.0.1

分析日期: 2025-05-01 22:23:21

应用概览

文件名称:	尾巴漫画.apk
文件大小:	1.91MB
应用名称:	尾巴漫画
软件包名:	com.es.reader.v9152063.r3644
主活动:	com.example.myapplication.MainActivity
版本号:	1.0.1
最小SDK:	23
目标SDK:	30
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	67/100 (低风险)
杀软检测:	9 个杀毒软件报毒
MD5:	43e5294662c50e19225469af0803db70
SHA1:	f0f0f04a4603b1531079f0dcd64fd98ba235838
SHA256:	84b90645b085f99ddb8d6821b3136668027a1064a31e1af907d821b6a0e3ea12

分析结果严重性

高危	中危	信息	安全	关注
0	6	2	2	1

四大组件信息

Activity组件：3个，其中export的有：1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

证书信息

二进制文件已签名
v1 签名: True

v2 签名: True
v3 签名: True
v4 签名: False
主题: C=CN, ST=China, L=Shanghai, O=Chen, OU=Chen, CN=Chen
签名算法: rsassa_pkcs1v15
有效期自: 2024-12-21 20:00:11+00:00
有效期至: 2052-05-08 20:00:11+00:00
发行人: C=CN, ST=China, L=Shanghai, O=Chen, OU=Chen, CN=Chen
序列号: 0x50150da3
哈希算法: sha256
证书MD5: 4e8932e72f34b22d80df1e614451806c
证书SHA1: 16e347c024df58c3c676dc671d767c150952c069
证书SHA256: eac05120ef8b8d264caf0edc90eef5e4b8c5ba883cac53f1cafa283b6b595c07
证书SHA512:
f915150ac59bd2b15d655cd825de3e2c4d9d8d2c59e65d1af5e9d545bce356981bc4b5a8dc21181179117cce539ff6c177bd13f5cdf56f83b107154baaaa69ce

公钥算法: rsa
密钥长度: 2048
指纹: 3eba9a031b27bbe27afe292365779042b9f977272039ef07e7158baee9eca360
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.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.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。

可浏览的Activity组件

ACTIVITY	INTENT
com.example.myapplication.MainActivity	Schemes: reader://, Hosts: comic.esmh.com,

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: **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	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过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。

</> 安全漏洞检测

高危: **0** | 警告: **4** | 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	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
3	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
4	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
5	应用程序可以写入应用程序目录。敏感信息应加密	信息	CWE: CWE-276: 默认权限不正确 OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
6	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
7	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

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
00114	创建到代理地址的安全套接字连接	网络 命令	升级会员：解锁高级权限
00162	创建 InetSocketAddress 对象并连接到它	socket	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
00075	获取设备的位置	信息收集 位置	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
00024	Base64解码后写入文件	反射 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	0/30	
其它常用权限	3/46	android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE 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。

域名检测

域名	状态	中国境内	位置信息
kf.wbgoodmh.top	安全	是	**IP地址:** 103.135.101.5 **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

URL链接分析

URL信息	源码文件
• http://kf.wbgoodmh.top/tour?kefu_id=tlmh&invite=	com/example/myapplication/LoadingActivity.java

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。