南明离火
移动应用检测平台

ANDROID 静态分析报告

jasmin • v5.1.9

分析日期: 2025-05-01 09:42:50

应用概览

文件名称:	jasmin v5.1.9.apk
文件大小:	25.54MB
应用名称:	jasmin
软件包名:	cl.l1Yc81xE.N1L81M1f
主活动:	.main
版本号:	5.1.9
最小SDK:	22
目标SDK:	31
加固信息:	NP管理器VMP
开发框架:	Java/Kotlin
应用程序安全分数:	45/100 (中风险)
杀软检测:	12 个杀毒软件报毒
MD5:	6bf93406ff786b7b85ac7a7deba2b75c
SHA1:	6077795e1dd1f4f3e847592ae17742722d36ee47
SHA256:	ad21b9567cf72bdcf720de50bc8[illegible]d9265785403561227c38f1f0fa378c25e33

分析结果严重性

高危	警告	信息	安全	关注
4	[illegible]	2	2	0

四大组件信息

Activity组件：17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：2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=VYU7LBlP8ouKNiOS, ST=RAm5T4A5AxcfrkFm, L=zFj5y5E1KReUlIWN, O=pdm1745233320079, OU=qwOln1745233320079, CN=W8i1745233320079
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-21 11:02:00+00:00
有效期至: 2075-04-21 11:02:00+00:00
发行人: C=VYU7LBlP8ouKNiOS, ST=RAm5T4A5AxcfrkFm, L=zFj5y5E1KReUlIWN, O=pdm1745233320079, OU=qwOln1745233320079, CN=W8i1745233320079
序列号: 0x950054710c2e9575
哈希算法: sha256
证书MD5: a586ed21b45bf46220f78c7ed16d1fca
证书SHA1: b8bc631399ec92910ac33a0987500c54d036aff2
证书SHA256: e9b9d7ec73aeb179880881853b9bbedadc3cda78bc2581f80ddd8939f57cc26e
证书SHA512: 4ca2ebe4cbcbd0941905bfc7a1f4515d3c8b3d33a90627baa688382d9322cd7e601bf973772dcad5524f01621257b584b58d60[illegible]68ca185424b008eb8f778

公钥算法: rsa
密钥长度: 2048
指纹: da9ee26f0340c4a80400996e560f33a5ac7ada35b236a3ce7b0d55f6ffe9d16c
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.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.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.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_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
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_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录
android.permission.READ_CONTACTS	危险	读取联系人信息	允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.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
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。
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.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。

网络通信安全

高危: 1 | 警告: 0 | 信息: 0 | 安全: 0

序号	范围	严重级别	描述

1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。

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: **1** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序具有网络安全配置[android:networkSecurityConfig=@xml/network_config]	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。
2	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，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: **3** | 警告: **6** | 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
3	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
4	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

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	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
8	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
9	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
10	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
11	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
12	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

本报告由南明离火移动安全分析平台生成

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
00039	启动网络服务器	控制 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
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
00195	设置录制文件的输出路径	录制音视频 文件	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
00007	Use absolute path of directory for the output media file path	文件	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
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
00162	创建 InetSocketAddress 对象并连接到它	socket	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
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
00054	从文件安装其他APK	反射	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
00067	查询IMSI号码	信息收集	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
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
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
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
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
00209	从最新渲染图像中获取像素	信息收集	升级会员：解锁高级权限
00210	将最新渲染图像中的像素复制到位图中	信息收集	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
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
00012	读取数据并放入缓冲流	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

敏感权限分析

类型	匹配	权限
恶意软件常用权限	5/30	android.permission.READ_PHONE_STATE android.permission.ACCESS_FINE_LOCATION android.permission.READ_CALL_LOG android.permission.READ_CONTACTS android.permission.READ_SMS
其它常用权限	4/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_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。

URL链接分析

URL信息	源码文件
• https://github.com/kongzue/dialogx	com/kongzue/dialogx/interfaces/BaseDialog.java
• https://github.com/kongzue/dialogx/wiki	com/kongzue/dialogx/DialogX.java
• 127.0.0.1	i/app/C0389.java
• 127.0.0.1	i/app/ServerSocket.java

• 127.0.0.1	i/app/C0004.java
• https://github.com/kongzue/dialogx	com/kongzue/dialogx/impl/ActivityLifecycleImpl.java

第三方SDK

SDK名称	开发者	描述信息
android-gif-drawable	koral--	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。
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 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。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

免责声明及风险提示: