南明离火
移动应用检测平台

ANDROID 静态分析报告

西游记 • v1.0.8

分析日期: 2025-07-05 13:30:26

应用概览

文件名称:	74ca491d689de22b99f989cc1286a1ce9055762f5e139ee6f889dd500858b64b.apk
文件大小:	22.19MB
应用名称:	西游记
软件包名:	com.sex.love
主活动:	com.sex.hv_launch.OpenScreenActivity
版本号:	1.0.8
最小SDK:	23
目标SDK:	29
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	47/100 (中风险)
跟踪器检测:	3/432
杀软检测:	5 个杀毒软件报毒
MD5:	d24af3507987145d4f4de6e85f3b3800
SHA1:	f1f4ced7c2e97e1[illegible]a04ac3300912ca786
SHA256:	74ca491d689de22b99f989cc1286a1ce9055762f5e139ee6f889dd500858b64b

分析结果严重性分布

高危	中危	信息	安全	关注
1	18	2	0	2

四大组件导出状态统计

Activity组件：[illegible]个，其中export的有： 9个
Service组件：6个，其中export的有： 1个
Receiver组件：8个，其中export的有： 1个

Provider组件：8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=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
证书MD5: e89b158e4bcf988ebd09eb83f5378e87
证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
证书SHA512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640[illegible]053abfea303977272d[illegible]9[illegible]704d89b7711292a4569

公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75
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.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.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.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.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
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.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。

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.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
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。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。

网络通信安全风险分析

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: **0** | 警告: **13** | 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=@xml/jz_network_security_config]	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。
3	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。
4	Activity (com.sex.hv_hhlz.ui.activity.BaseSearchActivity) 未受保护。[android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。

5	Activity (com.sex.hv_hhlz.ui.activity.ReadComicActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
6	Activity (com.sex.hv_hhlz.ui.activity.SectionMoreActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
7	Activity (com.sex.hv_hhlz.ui.activity.ReadNovelActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
8	Activity (com.sex.hv_md.ui.SearchActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
9	Activity (com.sex.hv_md.ui.PlayVideoActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
10	Activity (com.sex.hv_md.ui.ClassifyDetailActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
11	Activity (com.sex.hv_md.ui.MainActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
12	Activity (com.sex.hv_byfm.ui.MainActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
13	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
14	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

本报告由南明离火移动安全分析平台生成

代码安全漏洞检测

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

序号	问题	等级	参考标准	文件位置
1	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
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	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
5	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

应用行为分析

编号	行为	标签	文件
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
00024	Base64解码后写入文件	反射 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
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

00036	从 res/raw 目录获取资源文件	反射	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	4/30	android.permission.READ_PHONE_STATE android.permission.WAKE_LOCK android.permission.ACCESS_FINE_LOCATION android.permission.CALL_PHONE
其它常用权限	9/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.FOREGROUND_SERVICE android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.READ_EXTERNAL_STORAGE com.google.android.gms.permission.AD_ID

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
cns.killcovid2021.com	安全	是	**IP**地址: 194.53.53.249 国家: 中国 地区: 江苏 城市: 无锡 纬度: 31.569349 经度: 120.288788 查看: 高德地图
d.njsfcw.cn	安全	否	No Geolocation information available.
e.njsfcw.cn	安全	否	No Geolocation information available.
zltzjiami.dq59k.com	安全	是	**IP**地址: 194.53.53.249 国家: 中国 地区: 江苏 城市: 无锡 纬度: 31.569349 经度: 120.288788 查看: 高德地图

tvv.zjqfart.cn	安全	否	**IP地址:** 194.53.53.249 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289987 **经度:** 103.850281 **查看:** Google 地图
api.madou21.tv	安全	否	No Geolocation information available.
meexx.top	安全	否	No Geolocation information available.
tz.lailujuan.com	安全	否	**IP地址:** 154.17.[illegible].180 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.05[illegible]986 **经度:** -118.263687 **查看:** Google 地图
mhasd.xyz	安全	否	**IP地址:** 82.192[illegible].225 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.3[illegible]502 **经度:** 4.899980 **查看:** Google 地图
b.aisxdz.cn	安全	否	No Geolocation information available.
s1.328888.xyz	安全	否	No Geolocation information available.
yuepmaa.space	安全	否	**IP地址:** 104.21.53.165 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
api.xxxtik.com	安全	否	**IP地址:** 162.159.140.98 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
grcom.xyz	安全	否	**IP地址:** 66.29.129.4 **国家:** 美国 **地区:** 佐治亚州 **城市:** 亚特兰大 **纬度:** 33.727291 **经度:** -84.425377 **查看:** Google 地图
b.rmzx.net	安全	否	No Geolocation information available.

pv-oa-huawei.cgshjx.com	安全	否	No Geolocation information available.
android.pv123.app	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• http://127.0.0.1:%s%s	com/sex/hv_m91/ui/activity/PlayVideoActivity.java
• https://github.com/l-jinbin/apksignaturekillerex	bin/mt/signature/KillerApplication.java
• https://zltzjiami.dq59k.com/	com/sex/hv_zlt/adapter/VideosAdapter.java
• https://zltzjiami.dq59k.com/	com/sex/hv_zlt/adapter/TopicAdapter.java
• https://zltzjiami.dq59k.com/	com/sex/hv_zlt/adapter/ActorAdapter.java
• https://d.njsfcw.cn	com/sex/hv_mmmh/adapter/ReadComicAdapter.java
• https://d.njsfcw.cn	com/sex/hv_mmmh/adapter/ComicPageAdapter.java
• https://d.njsfcw.cn	com/sex/hv_mmmh/ui/fragment/ComicChildFragment.java
• https://meexx.top/	com/sex/hv_pdl/ui/PlayVideoActivity.java
• https://b.aisxdz.cn	com/sex/hv_mmmh/adapter/AnimPageAdapter.java
• https://b.rmzx.net	com/sex/hv_mmmh/ui/fragment/AnimChildFragment.java
• http://127.0.0.1:%s%s	com/sex/hv_m91/ui/activity/PlayShortVideoActivity.java
• https://e.njsfcw.cn	com/sex/hv_mmmh/ui/activity/ReadNovelActivity.java
• https://tvv.zjqfart.cn/ • https://api.maobu21.cn/	com/sex/hv_md/net/MDViewModel.java
• https://zltzjiami.dq59k.com/	com/sex/hv_zlt/ui/activity/PlayVideoActivity.java

• http://127.0.0.1:%s%s	com/sex/hv_mmmh/ui/activity/PlayAnimActivity.java
• http://127.0.0.1:%s%s	com/sex/hv_m91/adapter/ChoiceAdapter.java
• https://yuepmaa.space/mainview	com/sex/hv_yxfm/ui/fragment/YxFmBaseListFragment.java
• https://yuepmaa.space/radioalbum/	com/sex/hv_yxfm/ui/activity/RadioDetailActivity.java
• http://119.8.107.122:81/	com/sex/hv_avp/adapter/LabelAdapter.java
• https://api.xxxtik.com/util/source?path=	com/sex/hv_tik/adapter/VideosAdapter.java
• https://api.xxxtik.com/util/source?path=	com/sex/hv_tik/adapter/TikAdapter.java
• https://yuepmaa.space/radioalbum/	com/sex/hv_yxfm/ui/activity/AuthorDetailActivity.java
• http://tz.lailujuan.com/xs.txt	com/quanhuang/size.java
• https://cns.killcovid2021.com	com/sex/hv_m91porn/ui/PlayVideoActivity.java
• https://grcom.xyz/ • https://mhasd.xyz/	com/sex/hv_hmh/ui/MainActivity.java
• https://grcom.xyz/	com/sex/hv_hmh/ui/PlayMp3Activity.java
• https://s1.328888.xyz/	com/sex/hv_lf/ui/LFActivity.java
• https://yuepmaa.space/mainview	com/sex/hv_yxfm/ui/fragment/YxFmRankListChildFragment.java
• https://android.pv123.app • https://pv-oa-hua[illegible].cgshjx.com	com/sex/comment/video/JZMediaExo.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
C++ 共享库	Android	在 Android 应用中运行原生代码。
OpenSSL	OpenSSL	OpenSSL 是用于传输层安全性协议（TLS）和安全套接字层（SSL）协议的功能强大的，商业级且功能齐全的工具包。
IJKPlayer	Bilibili	IJKPlayer 是一款基于 FFmpeg 的轻量级 Android/iOS 视频播放器，具有 API 易于集成、编译配置可裁剪、支持硬件加速解码、DanmakuFlameMaster 架构清晰、简单易用等优势。

MMKV	Tencent	MMKV 是基于 mmap 内存映射的 key-value 组件，底层序列化/反序列化使用 protobuf 实现，性能高，稳定性强。
OpenCV	OpenCV	OpenCV 是一个跨平台的计算机视觉库，可用于开发实时的图像处理、计算机视觉以及模式识别程序。
RenderScript	Android	RenderScript 是用于在 Android 上以高性能运行计算密集型任务的框架。RenderScript 主要用于数据并行计算，不过串行工作负载也可以从中受益。RenderScript 运行时可在设备上提供的多个处理器（如多核 CPU 和 GPU）间并行调度工作。这样您就能够专注于表达算法而不是调度工作。RenderScript 对于执行图像处理、计算摄影或计算机视觉的应用来说尤其有用。
Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
Jetpack Lifecycle	Google	生命周期感知型组件可执行操作来响应另一个组件（如 Activity 和 Fragment）的生命周期状态的变化。这些组件有助于您写出更有条理且往往更精简的代码，这样的代码更易于维护。
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 WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
DRouter	Didi	DRouter 是 18 年滴滴乘客端自研的一套 Android 路由框架，基于平台化解耦的思想，为组件间通信服务。该项目以功能全面、易用为原则，支持各种路由场景，在页面路由、服务获取和过滤、跨进程及应用、VirtualApk 插件支持等方面都能提供多样化的服务。目前已在滴滴乘客端、顺风车、单车、国际化、滴滴定制车等十多个滴滴的 app 内使用，得到各种场景的验证。
AndroidAutoSize	JessYanCoding	今日头条屏幕适配方案终极版，一个极低成本的 Android 屏幕适配方案。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。

第三方追踪器检测

名称	类别	网址
Flurry	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/25
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

敏感凭证泄露检测

可能的密钥
AdMob广告平台的=> "com.google.android.gms.ads.APPLICATION_ID" : "ca-app-pub-6643150985989435~1140987084"
nx15lSjB7OdaJiaHvqjZ/elSWJ0aEdzSttjLmxWLAsUgxIaQMB8t1YJD8byFmgjvAPC1w9EweGEKX
nsiLXOX5P7cpvFUX7krS8cFwFhnnBG2me8tpHC5l2arZ7Idpv
nzjCH6n1sDma8EtSJPyHLib6qL78RAsSLiRpq0zQr9Z8092p7Kc5o+PBcEDQFh13TNYocsNVB0Leb
nVKULS52fwz6BEex1/+4qI2LD3k+cGuWOdgenUd2Rd0ZXhnRd31UnPR4QdqrnIm7jFBRNeAPulKyR
MIIDdzCCAl+gAwIBAgIEEAgHSTANBgkqhkiG9w0BAQsFADBsMRAwDgYDVQQGEwdzZXhsb3ZlMRAw
nTw8ipI8X71pLRW6HOPHXqOMCBN3zcf820+CDRMXvHFti05QzmIwr3qvSb0TGbkgP33cHN6w3VtiF
nFVjlb2baUyHPIP25MhabvxF00zEMw2a7RE0ztaF4WxguKCeJq3JhCznIW2tA09tYhmifgbtxM0sy
nVQQLEwdzZXhsb3ZlMRAwDgYDVQQDEwdzZXhsb3ZlMB4XDTIyMTAyMzA0MjQxNloXDTQ3MTAxNzA0
nZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJTIHXFT2cir/8dSmdOpox3DA2cW93kx
npOz47nUCAwEAAaMhMB8wHQYDVR0OBBYEFPyjixn9a6VYl+n2fMIyVVMLPuXyMA0GCSqGSIb3DQEB
nCwUAA4IBAQACZRqi05LNXdmCPfS3RPI8Pw5etHuw8X456mp5fXGWEocNMXOVfpXJp2RzEIGtRi8H

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。