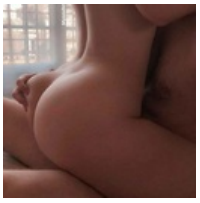
南明离火

移动应用检测平台

ANDROID 静态分析报告



Sexy movie • v1.5.9.9

分析日期: 2025-04-26 21:23:43

应用概览

文件名称:	Sexy movie.apk
文件大小:	3.24MB
应用名称:	Sexy movie□
软件包名:	ir.novinpardaz.kish
主活动:	.main
版本号:	1.5.9.9
最小SDK:	21
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	53/100 (中风险)
跟踪器检测:	1/432
杀软检测:	22 个杀毒软件报毒
MD5:	36222a8dea04684837f68a5defcda6ad
SHA1:	6cbf02e5de7dcbfefc853390c1088bb8d2b01145
SHA256:	ccf3bca23ff3aa4f5a69df17ff60c6689cba4e33c76295e63a306b6e710fdd2d

分析结果严重性

高危	中危	信息	安全	关注
1	22	1	2	0

四大组件信息

Activity组件：3个，其中export的有： 1个
Service组件：9个，其中export的有： 5个
Receiver组件：9个，其中export的有： 7个
Provider组件：1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=5Y, ST=70RHRo, L=ZgQfJE, O=jiUBr8sF0d8c, OU=ZyleZydR, CN=3M3Q5CWZs1
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-23 18:36:31+00:00
有效期至: 2035-04-21 18:36:31+00:00
发行人: C=5Y, ST=70RHRo, L=ZgQfJE, O=jiUBr8sF0d8c, OU=ZyleZydR, CN=3M3Q5CWZs1
序列号: 0xf55795d365fa8531
哈希算法: sha256
证书MD5: 54c420f10891f41c75818e193ac13022
证书SHA1: 0aa99709ec57a7fdc609d89f0aeff31042e7b111
证书SHA256: 67d8de180dc613739d13b31ca6783c5eefb4f759b1f1979a5785e47db2a69cfe
证书SHA512:
636a60e9e5132eec6aee823a8ced0ff0518aaea01363f5a9b0e28efadd1a30d4050e749ef4619f4f0dd185dc890358356dfb141fe491e6f4294ac8d8687db363

公钥算法: rsa
密钥长度: 2048
指纹: d54bff787cf9cafc100c71d3aeb65edf1a0c7f8b198043224f9dcce96deb73ee
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
ir.novinpardaz.kish.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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.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_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.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.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.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.VIBRATE	普通	控制振动器	允许应用程序控制振动器，用于消息通知振动功能。
android.permission.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
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.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。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
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。
ir.novinpardaz.kish.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。

com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。
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。
android.permission.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送短信。恶意应用程序可能会不经您的确认就发送信息，给您带来费用。
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收短信。 恶意程序会在用户未知的情况下监视或删除。
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.FOREGROUND_SERVICE_DATA_SYNC	普通	允许前台服务进行数据同步	允许常规应用程序使用类型为“dataSync”的 Service.startForeground。
android.permission.FOREGROUND_SERVICE_TYPE_REMOTE_MESSAGING	未知	未知权限	来自 android 引用的未知权限。

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: **15** | 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。

3	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
4	Service (com.google.firebase.iid.FirebaseInstanceIdService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
5	Service (anywheresoftware.b4a.objects.FirebaseNotificationsService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
6	Activity-Alias (.settings) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
7	Service (.starter) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
8	Broadcast Receiver (.starter$starter_BR) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
9	Broadcast Receiver (.firebasemessaging) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
10	Service (.iconservice) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
11	Broadcast Receiver (.iconservice$iconservice_BR) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
12	Broadcast Receiver (.sms_receiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
13	Service (.handlingservice) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
14	Broadcast Receiver (.handlingservice$handlingservice_BR) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
15	Broadcast Receiver (.httputil2service) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

本报告由南明离火移动安全分析平台生成

安全漏洞检测

高危: **1** | 警告: **5** | 信息: **1** | 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
2	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
3	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
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	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
6	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
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
8	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

行为分析

编号	行为	标签	文件
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
00204	获取默认铃声	信息收集	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
00146	获取网络运营商名称和 IMSI	电话服务 信息收集	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
00193	发送短信	短信	升级会员：解锁高级权限
00117	获取 IMSI 和网络运营商名称	电话服务 信息收集	升级会员：解锁高级权限
00056	修改语音音量	控制	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
00088	创建到给定主机地址的安全套接字连接	命令 网络	升级会员：解锁高级权限
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	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
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00189	获取短信内容	短信	升级会员：解锁高级权限
00188	获取短信地址	短信	升级会员：解锁高级权限
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	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	9/30	android.permission.CALL_PHONE android.permission.READ_SMS android.permission.READ_CONTACTS android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.GET_ACCOUNTS android.permission.SEND_SMS android.permission.RECEIVE_SMS android.permission.READ_PHONE_STATE
其它常用权限	7/46	android.permission.INTERNET android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.FOREGROUND_SERVICE com.google.android.c2dm.permission.RECEIVE com.google.android.gms.permission.AD_ID com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_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。

域名检测

域名	状态	中国境内	位置信息
google.com	安全	否	**IP地址:** 35.186.236.207 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
xproject-9cb86-default-rtdb.asia-southeast1.firebasedatabase.app	安全	否	**IP地址:** 35.186.236.207 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图

URL链接分析

URL信息	源码文件
• 127.0.0.1	ir/novinpardaz/kish/xclass.java
• 127.0.0.1	anywheresoftware/b4a/objects/SocketWrapper.java
• https://google.com	ir/novinpardaz/kish/main.java
• https://invalid-url/	ir/novinpardaz/kish/httpjob.java
• 127.0.0.1	ir/novinpardaz/kish/utils.java

• https://xproject-9cb86-default-rtdb.asia-southeast1.firebasedatabase.app	自研引擎-S

FIREBASE数据库分析

标题	严重程度	描述信息

Firebase远程配置已禁用	安全	Firebase远程配置URL （https://firebaseremoteconfig.googleapis.com/v1/projects/737288533764/namespaces/firebase:fetch?key=AIzaSyCmDaqLA-_bTS6cqILLFXFvnC5BSEvWAwA ）已禁用。响应内容如下所示:
		{
		"state": "NO_TEMPLATE"
		}

第三方SDK

SDK名称	开发者	描述信息
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。
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。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。

追踪器

名称	类别	网址
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

密钥凭证

可能的密钥
"firebase_database_url" : "https://xproject-9cb86-default-rtdb.asia-southeast1.firebasedatabase.app"
"google_api_key" : "AIzaSyCmDaqLA-_bTS6cqILLFXFvnC5BSEvWAwA"
"google_app_id" : "1:737288533764:android:e8d0b0eabb8ee744a2c251"
"google_crash_reporting_api_key" : "AIzaSyCmDaqLA-_bTS6cqILLFXFvnC5BSEvWAwA"

免责声明及风险提示: