南明离火
移动应用检测平台

ANDROID 静态分析报告

悦诚 • v1.0.77

分析日期: 2025-03-11 10:35:01

应用概览

文件名称:	base.apk
文件大小:	11.46MB
应用名称:	悦诚
软件包名:	com.aa9m47vo.android
主活动:	com.cola.sprite.activity.MainActivity
版本号:	1.0.77
最小SDK:	21
目标SDK:	33
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	60/100 (低风险)
杀软检测:	AI评估：安全
MD5:	882d74e80cb93df2235adcdbbaa555be
SHA1:	220a0f63de831a8f6b78c8a4cbd1649e53895935
SHA256:	7967ed6d7d87a28830fbb1bb2ff217b73133a63c5a60da94caa780c44e72975a

分析结果严重性

高危	中危	信息	安全	关注
0	1	2	2	3

四大组件信息

Activity组件：6个，其中export的有：1个
Service组件：2个，其中export的有：0个
Receiver组件：1个，其中export的有：1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: False
v4 签名: False
主题: O=aa9m47vo, OU=aa9m47vo, CN=aa9m47vo
签名算法: rsassa_pkcs1v15
有效期自: 2021-06-04 09:09:27+00:00
有效期至: 2046-05-29 09:09:27+00:00
发行人: O=aa9m47vo, OU=aa9m47vo, CN=aa9m47vo
序列号: 0x5e6696dc
哈希算法: sha256
证书MD5: 65c9b7ff8f46cb1f7667a2417599d5c2
证书SHA1: 7e83950cbffea8ddb57f75c896f25771c24f7720
证书SHA256: c21cd1b95b931d841aac4732b8193f021bd26883ac04883ec4058f50d6bb314b
证书SHA512:
772d44267f436f1deabbe56750db4cf4561e51e9f7d7b29435ba014762cd9ded642e43a38821019356ca58fbcac046e44d5eef3d99f6bbb0bc21b7c846573347

公钥算法: rsa
密钥长度: 2048
指纹: 8afa6ab9c18a33ab49672fe0f17aa6e798cb4fbe0d0524e940d34adfbf704486
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.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.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.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.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.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.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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
android.permission.READ_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
android.permission.INSTALL_PACKAGES	签名(系统)	请求安装APP	允许应用程序安装全新的或更新的 Android 包。恶意应用程序可能会借此添加其具有任意权限的新应用程序。
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。
com.aa9m47vo.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
android.permission.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。

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: **4** | 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。
3	Activity (com.canhub.cropper.CropImageActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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。
4	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.DUMP [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。

安全漏洞检测

高危: **0** | 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	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	此文件没有使用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
3	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

4	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	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
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
7	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
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	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

行为分析

编号	行为	标签	文件
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
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
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
00091	从广播中检索数据	信息收集	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
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
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限
00052	删除内容 URI 指定的媒体（SMS、CALL_LOG、文件等）	短信	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	3/30	android.permission.VIBRATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.WAKE_LOCK
其它常用权限	8/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE

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
www.sy001.store	安全	否	No Geolocation information available.
www.zyz550.top	安全	否	No Geolocation information available.
google.com	安全	否	**IP地址:** 142.250.176.14 **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
www.xfcyp.top	安全	否	No Geolocation information available.
www.cmpay.com	安全	是	**IP地址:** 114.230.95.19 **国家:** 中国 **地区:** 江苏 **城市:** 扬州 **纬度:** 32.397221 **经度:** 119.435600 **查看:** 高德地图
kfghetsdf.com	安全	否	No Geolocation information available.

tempuri.org	安全	否	**IP地址:** 20.76.201.171 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
www.xmmenggou.com	安全	是	**IP地址:** 61.160.192.102 **国家:** 中国 **地区:** 江苏 **城市:** 常州 **纬度:** 31.783331 **经度:** 119.966667 **查看:** 高德地图
material.io	安全	否	**IP地址:** 216.239.36.21 **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
www.zzha.vip	安全	否	**IP地址:** 206.238.197.27 **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
www.shouyinbei.net	安全	是	**IP地址:** 121.41.10.35 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图

URL链接分析

URL信息	源码文件
• https://kfghetsdf.com/ • wss://kfghetsdf.com/cable • https://oss-cn-shenzhen.aliyuncs.com:443	com/cola/sprite/BuildConfig.java
• https://kfghetsdf.com/ • https://oss-cn-shenzhen.aliyuncs.com:443 • wss://kfghetsdf.com/cable	com/cola/sprite/dagger/NetworkModule.java
• www.sy001.store • www.zyz550.top • www.xfcyp.top • www.cmpay.com • www.xmmenggou.com • www.shouyinbei.net • www.zzha.vip • www.alipay.com	com/cola/sprite/app/LegacyPaymentSettingsQRCodeValidator.java

• https://github.com/airbnb/epoxy/wiki/avoiding-memory-leaks	com/airbnb/epoxy/EpoxyController.java
• https://material.io/design/components/dialogs.html#actions	com/afollestad/materialdialogs/MaterialDialog.java
• https://google.com	com/tonyodev/fetch2core/FetchCoreUtils.java
• http://tempuri.org/	com/cola/sprite/utils/Router.java

第三方SDK

SDK名称	开发者	描述信息
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。
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。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个对象层，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。

密钥凭证

可能的密钥
2cjTlnrZEe1IQocQoGV4fJkpOyeuw6
460643a974555d792b8f5a6e1e5d323c
946eca6b182e63ebe50cf82e483715bf

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。