南明离火
移动应用检测平台

ANDROID 静态分析报告

O3joba TV • v1.0

分析日期: 2025-03-10 17:19:26

应用概览

文件名称:	dc2a874315830adbb8b7d6ed2d1c74c757b25b0aadc8f589ff1818d327168d60.apk
文件大小:	10.89MB
应用名称:	O3joba TV
软件包名:	com.o3joba.tv09
主活动:	.MainActivity
版本号:	1.0
最小SDK:	21
目标SDK:	28
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	52/100 (中风险)
跟踪器检测:	3/432
杀软检测:	9 个杀毒软件报毒
MD5:	5d09ebbcd1c6a4187a959fd93885[illegible]2f
SHA1:	90e9795f4222fa85317fc9a2a[illegible]e6f0a02b84432
SHA256:	dc2a874315830adbb[illegible]2d1c74c757b25b0aadc8f589ff1818d327168d60

分析结果严重性

高危	中危	信息	安全	关注
2	16	3	2	1

四大组件信息

Activity组件：18个，其中export的有： 0个
Service组件：4个，其中export的有： 0个
Receiver组件：2个，其中export的有： 2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=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:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569

公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75
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.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。

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	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	Broadcast Receiver (com.startapp.sdk.adsbase.remoteconfig.BootCompleteListener) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。

安全漏洞检测

高危: **2** | 警告: **10** | 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	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	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
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	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

6	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
7	SHA-1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	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
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	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
11	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
12	SSL的不安全实现。信任所有证书或接受自签名证书是一个关键的安全漏洞。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
13	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

14	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
15	此应用程序可能会请求root（超级用户）权限	警告	CWE: CWE-250: 以不必要的权限执行 OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限

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
00013	读取文件并将其放入流中	文件	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
00137	获取设备的最后已知位置	位置 信息收集	升级会员：解锁高级权限
00115	获取设备的最后已知位置	信息收集 位置	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00014	将文件读入流并将其放入 JSON 对象中	文件	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入 JSON 对象	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
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
00092	发送广播	命令	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	升级会员：解锁高级权限
00025	监视要执行的一般操作	反射	升级会员：解锁高级权限
00023	从当前应用程序启动另一个应用程序	反射 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
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
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
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
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00110	查询ICCID号码	信息收集 电话服务	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
00147	获取当前位置的时间	信息收集 位置	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
00078	获取网络运营商名称	信息收集 电话服务	升级会员：解锁高级权限
00034	查询当前数据网络类型	信息收集 网络	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
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00121	创建目录	文件 命令	升级会员：解锁高级权限
00104	检查给定路径是否是目录	文件	升级会员：解锁高级权限
00064	监控来电状态	控制	升级会员：解锁高级权限
00123	连接到远程服务器后将响应保存为 JSON	网络 命令	升级会员：解锁高级权限
00046	方法反射	反射	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	1/30	android.permission.WAKE_LOCK
其它常用权限	3/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE com.google.android.c2dm.permission.RECEIVE

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
config.unityads.unitychina.cn	安全	是	**IP地址:** 180.97.228.82 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
geoip.api.p3insight.de	安全	否	No Geolocation information available.
o3jobatv-142b3-default-rtdb.firebaseio.com	安全	否	**IP地址:** 35.190.39.113 **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
daneden.me	安全	否	**IP地址:** 76.76.21.142 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 核桃 **纬度:** 34.015400 **经度:** -117.858223 **查看:** Google 地图
d2to8y50b3n6dq.cloudfront.net	安全	否	**IP地址:** 13.226.255.57 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
www.com.startapp.com	安全	否	No Geolocation information available.
config.unityads.unity3d.com	安全	否	**IP地址:** 34.110.229.214 **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
awsdus.api.p3insight.de	安全	否	No Geolocation information available.
d1byvlfiet2h9d.cloudfront.net	安全	否	**IP地址:** 3.167.217.17 **国家:** 美国 **地区:** 华盛顿 **城市:** 西雅图 **纬度:** 47.627499 **经度:** -122.346199 **查看:** Google 地图

infoevent.startappservice.com	安全	否	**IP地址:** 132.145.167.65 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
t.me	安全	否	**IP地址:** 76.76.21.142 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 英格兰 **城市:** 伦敦 **纬度:** 51.508530 **经度:** -0.125740 **查看:** Google 地图
geoip.api.c0nnectthed0ts.com	安全	否	**IP地址:** 34.250.243.49 **国家:** 爱尔兰 **地区:** 都柏林 **城市:** 都柏林 **纬度:** 53.344151 **经度:** -6.267249 **查看:** Google 地图
imp.startappservice.com	安全	否	**IP地址:** 129.213.102.0 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
req.startappservice.com	安全	否	**IP地址:** 132.145.167.65 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
info.startappservice.com	安全	否	**IP地址:** 132.145.167.65 **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
support.startapp.com	安全	否	**IP地址:** 132.145.167.65 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
ul.api.c0nnectthed0ts.com	安全	否	**IP地址:** 34.250.243.49 **国家:** 爱尔兰 **地区:** 都柏林 **城市:** 都柏林 **纬度:** 53.344151 **经度:** -6.267249 **查看:** Google 地图

adsmetadata.startappservice.com	安全	否	**IP地址:** 132.145.167.65 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
lh6.ggpht.com	安全	否	**IP地址:** 142.251.40.33 **国家:** 美国 **地区:** 纽约 **城市:** 纽约市 **纬度:** 40.713192 **经度:** -74.006065 **查看:** Google 地图

URL链接分析

URL信息	源码文件
• https://www.google.com	com/o3joba/tv09/MatchActivity.java
• https://play.google.com/store/apps/details?id=com.instantbits.cast.webvideo	com/o3joba/tv09/ExoplayerActivity.java
• http://play.google.com • https://play.google.com	com/startapp/sdk/adsbase/a.java
• https://t.me/o3jobatv • https://www.facebook.com/profile.php?id=100067048238075 • https://www.google.com	com/o3joba/tv09/HomeActivity.java
• https://www.google.com/	com/o3joba/tv09/MainActivity.java
• https://infoevent.startappservice.com/tracking/infoevent	com/startapp/sdk/adsbase/infoevents/AnalyticsConfig.java
• https://geoip.api.p3insight.de/geoip/ • https://d2to8y50b3n6dq.cloudfront.net/truststores/	com/startapp/sdk/insight/NetworkTestsMetaData.java
• javascript:splash_fadeout • https://daneden.me/animate • https://lh6.ggpht.com/vo9wbihc9bbdbwfhuezqzoqpkmfkjsatibvwk3qxpbvjwcr8i79evui0ab41a-je7x-6=w200	com/startapp/sdk/ads/splash/SplashHtml.java
• https://www.com.startapp.com/policy/sdk-policy/ • https://info.startappservice.com/inapp/resources/info_l.png • https://d1byvmei2h9q.cloudfront.net/inapp/resources/adinformationdialog3.html	com/startapp/sdk/adsbase/adinformation/AdInformationConfig.java
• javascript:window.nativebridge.receiveevent	com/unity3d/services/ads/webplayer/WebPlayerView.java
• https://imp.startappservice.com/tracking/adimpression	com/startapp/sdk/adsbase/AdsConstants.java
• https://support.startapp.com/hc/en-us/articles/360002411114	com/startapp/sdk/adsbase/k.java
• https://aw-us.api.p3insight.de/isupload/upload_check_lumen.php • https://ul.api.c0nnectthed0ts.com/ul/v3/ • https://geoip.api.c0nnectthed0ts.com/geoip/ • https://d2to8y50b3n6dq.cloudfront.net/truststores/	com/startapp/networkTest/a.java

• 1.9.0.4	com/o3joba/tv09/WebviewActivity.java
• https://req.startappservice.com/1.5/ • https://adsmetadata.startappservice.com/1.5/	com/startapp/sdk/adsbase/remoteconfig/MetaData.java
• 127.0.0.1	com/startapp/networkTest/d/a/b.java
• https://www.google.com	com/o3joba/tv09/ChannelsActivity.java
• 10.0.2.15	com/startapp/a/a/a.java
• javascript:startappbackpressed	com/startapp/sdk/adsbase/consent/ConsentActivity.java
• https://config.unityads.unitychina.cn/webview/ • https://config.unityads.unity3d.com/webview/	com/unity3d/services/core/properties/SdkProperties.java
• https://geoip.api.c0nnectthed0ts.com/geoip/ • https://d2to8y50b3n6dq.cloudfront.net/truststores/	com/startapp/networkTest/startapp/NetworkTester.java
• https://o3jobatv-142b3-default-rtdb.firebaseio.com/	自研引擎-S

FIREBASE数据库分析

标题	严重程度	描述信息
应用与Firebase数据库通信	信息	该应用与位于 https://o3jobatv-142b3-default-rtdb.firebaseio.com/ 的 Firebase 数据库进行通信

Firebase远程配置已禁用	安全	Firebase远程配置URL（https://firebaseremoteconfig.googleapis.com/v1/projects/994941029102/namespaces/firebase:fetch?key=AIzaSyDzkTv5rMlXvBbMIa_gK7MKTBdHuLdfdF8 ） 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。
Unity Ads	Unity Technologies	Unity Ads SDK 由领先的移动游戏引擎创建，无论您是在 Unity、xCode 还是 Android Studio 中进行开发，都能为您的游戏提供全面的变现服务框架。
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。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

邮箱

EMAIL	源码文件
o3jobatv@gmail.com	com/o3joba/tv09/HomeActivity.java

追踪器

名称	类别	网址
IAB Open Measurement	Advertisement, Identification	https://reports.exodus-privacy.eu.org/trackers/328
Startapp	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/195
Unity3d Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/121

密钥凭证

可能的密钥
"firebase_database_url" : "https://o3jobatv-142b3-default-rtdb.firebaseio.com/"
"google_api_key" : "AIzaSyDzkTv5rMlXvBbMIa_gK7MKTBdHuLdfdF8"
"google_app_id" : "1:994941029102:android:64fdff65784132eaed81ff"
FJKgMHk72Lw8N35HyJbksY7PMmNDfDO9N0bBld7EL7bSTU7ziVi9
3A757365722F72656C656173652D6B657973
2F73797374656D2F6C69622F6C696272656666572656E63652D72696C2E736F
APA91bEiyoUzQu4FCddBpZaxmmSk1QHQIOIcnlQaC5vh5qeU
com/Vo9wbFH89BbDbWFhUezQZOGPKmfkJSAtIbVWk3QxPbvJwcR8I79EVd0aB41a

---

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患。