南明离火
移动应用检测平台

ANDROID 静态分析报告

CleanTube • v0.9.5

分析日期: 2025-10-12 17:09:41

应用概览

文件名称:	2cc38e1f8965bbddf28d9cb57bbd5683dcf39f8bf068a77b92841ba422b68728.apk
文件大小:	6.37MB
应用名称:	CleanTube
软件包名:	com.sgebrelibanos.aderaser
主活动:	com.sgebrelibanos.aderaser.MainActivity
版本号:	9.9.5
最小SDK:	24
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:	67/100 (低风险)
杀软检测:	经检测，该文件安全
MD5:	c733017a07ea2926fd17ca2821e5de4a
SHA1:	98d6d6b2daddffc8c67632b13c[illegible]d32f4fcd
SHA256:	2cc38e1f8965bbddf28d9cb57bbd5683dcf39f8bf068a77b92841ba422b68728

分析结果严重性分布

高危	中危	信息	安全	关注
0	0	1	3	0

四大组件导出状态统计

Activity组件：10个，其中export的有： 0个
Service组件：3个，其中export的有： 0个
Receiver组件：2个，其中export的有： 1个
Provider组件：1个，其中export的有： 0个

应用签名证书信息

APK已签名

v1 签名: False
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2022-06-14 20:22:00+00:00
有效期至: 2052-06-14 20:22:00+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xfcb91b6fd24b6da6cb45923967d01918816bb4dd
哈希算法: sha256
证书MD5: bd9f4bb3bdb600ff42796cd8a62912e9
证书SHA1: 871a7d51a5a396d8b888d245079dfc3aae1bdd49
证书SHA256: 59aebd8592222800f4c64af6c90982feb853b54ffc77d9a145771cb6903fa221
证书SHA512:
bcdc4b63471b41d460477d4c4bd9d1ea05627ce4aac5f099f1fbd31509ac786f3a7f3142aad45e6c314ae4abff373f5d082b86b4aa0d5a764ee1c50d06a256ca

公钥算法: rsa
密钥长度: 4096
指纹: e8e7ae0989637235e9eb6a5185cf595c0afe24bcc2241d069e94c0b7336ffafc
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
com.android.vending.BILLING	普通	应用程序具有应用内购买	允许应用程序从 Google Play 进行应用内购买。
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.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.CHANGE_WIFI_MULTICAST_STATE	危险	允许接收WLAN多播	允许应用程序接收并非直接向您的设备发送的数据包。这样在查找附近提供的服务时很有用。这种操作所耗电量大于非多播模式。
android.permission.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.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.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_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。
com.sgebrelibanos.aderaser.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
com.android.vending.CHECK_LICENSE	未知	未知权限	来自 android 引用的未知权限。

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全合规分析

高危: **0** | 警告: **0** | 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: **4** | 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=@7F150002]	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 设置了 TaskAffinity 属性 (com.sgebrelibanos.aderaser.MainActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
5	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 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。

代码安全漏洞检测

高危: **0** | 警告: **5** | 信息: **1** | 安全: **2** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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

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	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
4	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
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	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
7	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-4	升级会员：解锁高级权限
8	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

应用行为分析

编号	行为	标签	文件
00163	创建新的 Socket 并连接到它	socket	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
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00026	方法反射	反射	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
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
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00114	创建到代理地址的安全套接字连接	网络 命令	升级会员：解锁高级权限
00161	对可访问性节点信息执行可访问性服务操作	无障碍服务	升级会员：解锁高级权限
00173	获取 AccessibilityNodeInfo 屏幕中的边界并执行操作	无障碍服务	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	1/30	android.permission.RECORD_AUDIO
其它常用权限	6/46	android.permission.FOREGROUND_SERVICE android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
returnyoutubedislikeapi.com	安全	否	**IP地址:** 188.114.96.0 **国家:** 美国 **地区:** 印第安纳州 **城市:** 弗朗西斯科 **纬度:** 38.333290 **经度:** -87.447083 **查看:** Google 地图
api.glassfy.io	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• https://api.glassfy.io	io/glassfy/androidsdk/internal/GManager.java
• 239.255.255.250 • 239.255.255.246	R2/a.java

• https://returnyoutubedislikeapi.com/votes?videoid=','options','queryselector','getboundingclientrect','click','fetching	com/sgebrelibanos/aderaser/MainActivity.java
• https://play.google.com/store/apps/details?id=com.sgebrelibanos.aderaser	W0/C0448t0.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Google Play Billing	Google	Google Play 结算服务可让您在 Android 上销售数字内容。本文档介绍了 Google Play 结算服务解决方案的基本构建基块。要决定如何实现特定的 Google Play 结算服务解决方案，您必须了解这些构建基块。
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 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。
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。
Picasso	Square	一个强大的 Android 图片下载缓存库。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
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。

邮箱地址敏感信息提取

EMAIL	源码文件
this@abstracttypeconstructor.parameters this@abstracttypeconstructor.builtins	H2/AbstractC1050f.java
this@createcapturedifneeded.type	H2/AbstractC0821d.java

Google Play 应用市场信息

标题: CleanTube - No Ad Videos

评分: 4.6042194 **安装:** 1,000,000+ **价格:** 0 **Android版本支持:** **分类:** 娱乐 **Play Store URL:** com.sgebrelibanos.aderaser

开发者信息: S & G Apps, 5133884515122653280, None, https://clean-tube.com, summon@clean-tube.com,

发布日期: None **隐私政策:** Privacy link

关于此应用:

CleanTube 是一款无广告应用，让您可以聆听音乐、观看您喜爱的频道的高清（4K）视频，并在使用其他应用时在屏幕上方观看视频。 CleanTube 是您手机上必备的无广告流媒体应用，原因如下。 视频广告屏蔽： - 任何情况下，都不会出现中断您视频播放的干扰性广告。 - 浮动视频播放器也没有任何广告。 登录您的帐户： - 安全登录您之前的帐户，您创建的所有视频和播放列表都将在 CleanTube 中供您使用。 弹出式视频播放器 Tube 允许您以“浮动”模式播放视频。现在，您可以玩游戏、看电影以及执行其他任务。 此模式下无广告！ - 您可以调整视频播放器的大小，并将其移动到手机的任何角落。 观看高品质的搞笑短视频。 - 以

4K 分辨率播放数百万个热门视频。您还可以调整视频播放速度。 - 音乐播放器允许您收藏喜爱的视频并将其添加到您自己的播放列表中。 ********** 网站：https://clean-tube.com 隐私政策：https://clean-tube.com/privacy.html ********** 联系我们： CleanTube 团队期待您的反馈！ 有任何反馈或需要帮助？请发送电子邮件至 help.cleantube@gmail.com 即将推出的功能 - 投射到电视应用 CleanTube™ 是 S 的商标& G Apps 有限责任公司

免责声明及风险提示: