南明离火
移动应用检测平台

ANDROID 静态分析报告

影视免费看 • v2.7.1

分析日期: 2024-05-30 03:31:08

应用概览

文件名称:	爱加密2019.11.22日样本.apk
文件大小:	4.06MB
应用名称:	影视免费看
软件包名:	com.example.jingbin.webviewstudy
主活动:	com.example.jingbin.webviewstudy.MainActivity
版本号:	2.7.1
最小SDK:	14
目标SDK:	28
加固信息:	爱加密企业版 加固
应用程序安全分数:	45/100 (中风险)
杀软检测:	AI评估：可能有安全隐患
MD5:	6a055040e637414066c42c37154becf8
SHA1:	0d29c249d5604c6291af9e8fec8d590939928efb
SHA256:	52f0142e0be35d7a4b638e175ff[illegible]12e0d3a0da7d744a0bd093c2dfcc493b

分析结果严重性分布

高危	中危	信息	安全	关注
2	4	10	1	9

四大组件导出状态统计

Activity组件：4个，其中export的有：2个
Service组件：0个，其中export的有：0个
Receiver组件：0个，其中export的有：0个
Provider组件：0个，其中export的有：0个

应用签名证书信息

二进制文件已签名
v1 签名: True
v2 签名: False

v3 签名: False
v4 签名: False
主题: C=US, O=Android, CN=Android Debug
签名算法: rsassa_pkcs1v15
有效期自: 2012-06-27 04:40:33+00:00
有效期至: 2042-06-20 04:40:33+00:00
发行人: C=US, O=Android, CN=Android Debug
序列号: 0x4fea8ec1
哈希算法: sha1
证书MD5: 9e0f030537038bbf1493402a80f47239
证书SHA1: 03495b5729e6121bee74a57a54b2f9c7ed6bcf31
证书SHA256: 52fa8791a4420e506b1035ae60e5f7d458709971f9205df75d1688a6b642a311
证书SHA512:
0bedfc369d68dd30eb489d6f115c63393e08f93614820d1fc9dcedf12c3e1bc68e63bf1bd1bb54e3ad0c60e7926ec022f2a1b426f78258c3e2aadce091dca179

找到 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.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.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.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户错略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
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.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.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
android.permission.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
android.permission.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.example.jingbin.webviewstudy.WebViewActivity	Schemes: https://,
com.example.jingbin.webviewstudy.DeepLinkActivity	Schemes: will://, Hosts: link,

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: **2** | 警告: **0** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序已使用代码签名证书进行签名
应用程序存在Janus漏洞	高危	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。
应用程序使用了调试证书进行签名	高危	应用程序使用了调试证书进行签名。生产环境的应用程序不能使用调试证书发布。

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	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 4.0-4.0.2, [minSdk=14]	信息	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	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。
3	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。
4	Activity (com.example.jingbin.webviewstudy.WebViewActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity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Activity是显式导出的。
5	Activity (com.example.jingbin.webviewstudy.DeepLinkActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity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Activity是显式导出的。

代码安全漏洞检测

序号	问题	等级	参考标准	文件位置

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED(裁剪符号表)
1	armeabi/libibs.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出覆盖返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	No RELRO high 此共享对象未启用 RELRO。整个 GOT（.got 和 .got.plt）都是可写的。如果没有此编译器标志，全局变量上的缓冲区溢出可能会覆盖 GOT 条目。使用选项 -z,relro,-z,now 启用完整 RELRO，仅使用 -z,relro 启用部分 RELRO。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	8/30	android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.READ_PHONE_STATE android.permission.SYSTEM_ALERT_WINDOW android.permission.GET_TASKS android.permission.RECORD_AUDIO android.permission.CAMERA android.permission.MODIFY_AUDIO_SETTINGS
其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FOREGROUND_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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
mctool.cn	安全	是	**IP地址:** 154.210.49.239 **国家:** 中国 **地区:** 香港 **城市:** 香港 **纬度:** 22.285521 **经度:** 114.157692 **查看:** 高德地图
m.youku.com	安全	是	**IP地址:** 58.215.190.101 **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
vip.iqiyi.com	安全	是	**IP地址:** 58.215.190.101 **国家:** 中国 **地区:** 山东 **城市:** 济南 **纬度:** 36.668331 **经度:** 116.997223 **查看:** 高德地图
www.66zhibo.net	安全	是	**IP地址:** 43.129.165.37 **国家:** 中国 **地区:** 香港 **城市:** 香港 **纬度:** 22.285521 **经度:** 114.157692 **查看:** 高德地图

www.hanjutv.com	安全	是	**IP地址:** 210.56.51.192 **国家:** 中国 **地区:** 香港 **城市:** 香港 **纬度:** 22.285521 **经度:** 114.157692 **查看:** 高德地图
note.youdao.com	安全	是	**IP地址:** 58.215.190.101 **国家:** 中国 **地区:** 江苏 **城市:** 南通 **纬度:** 32.030296 **经度:** 120.874779 **查看:** 高德地图
m.tv.sohu.com	安全	是	**IP地址:** 58.215.190.101 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
m.mgtv.com	安全	是	**IP地址:** 58.215.190.101 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
m.pptv.com	安全	是	**IP地址:** 58.215.190.101 **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
jx.drgxj.com	安全	否	**IP地址:** 50.28.56.190 **国家:** 美利坚合众国 **地区:** 密歇根 **城市:** 兰辛 **纬度:** 42.733280 **经度:** -84.637764 **查看:** Google 地图

URL链接安全分析

URL信息	源码文件
• http://taoyanranduapp.com/kaws/salvation/salvation.html • https://github.com/youlookwhat/WebViewStudy • http://taoyanran.duapp.com/kaws/salvation/images/kaxws_qrcode.png • https://github.com/youlookwhat/MaterialDesign/raw/master/app/release/app-release.apk • https://v4-image-api.kangaiweishi.com/v4/articles/fa1ffcd611934e80bb6e490bed15efb8.html • http://custom.transaction • http://support.kangaiweishi.com/wx_api	自研引擎-A

• file:unexpect • http://debugtbs.qq.com • www.qq.com • http://mqqad.html5.qq.com/adjs • https://m.pptv.com/?location=m_channel_vip • https://note.youdao.com/yws/public/note/5d3587dc1179b82f0fdce87bc36c1b27 • javascript:document.body.innerhtml= • https://vip.iqiyi.com/ • http://www.hanjutv.com/ • https://www.baidu.com/s?ie=utf-8&wd= • http://pms.mb.qq.com/rsp204 • https://github.com/youlookwhat/webviewstudy • http://wup.imtt.qq.com:8080 • https://film.qq.com/weixin/all.html • www.le • http://jx.drgxj.com/?url= • https://m.youku.com/ • http://debugtbs.qq.com?10000 • http://mdc.html5.qq.com/mh?channel_id=50079&u= • http://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_debugplugin_debugplugin.tbs • https://m.tv.sohu.com/film • http://cfg.imtt.qq.com/tbs?v=2&mk= • http://www.66zhibo.net/ • www.mgtv • http://mctool.cn/music/ • https://m.mgtv.com/channel/vip/ • http://debugx5.qq.com • www.iqiyi	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
爱加密	北京智游网安科技有限公司	针对目前移动应用普遍存在的破解、篡改、劫持、盗版、数据窃取、钓鱼欺诈等各类安全风险，通过业界领先的第六代加固技术，为用户提供全面的移动应用加固加密技术和攻击防范服务。
腾讯浏览服务（TBS）	Tencent	腾讯浏览服务，依托 X5 内核强大的能力，致力于提供优化移动端浏览体验的整套解决方案。
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。

免责声明及风险提示: