南明离火
移动应用检测平台

ANDROID 静态分析报告

Ibo Player Pro : v3.5

分析日期: 2025-03-11 14:43:53

应用概览

文件名称:	Ibo Player Pro v3.5.apk
文件大小:	9.14MB
应用名称:	Ibo Player Pro
软件包名:	com.flextv.livestore
主活动:	com.flextv.livestore.MainActivity
版本号:	3.5
最小SDK:	21
目标SDK:	32
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	57/100 (中风险)
杀软检测:	AI评估：安全
MD5:	2bbadf924555157a1ab94d4e8ceffd34
SHA1:	eb577cffc36c810e6d58cbe4c1cd04130f210128
SHA256:	fe151cd0f3f1bdb15e1de04cbbd990182a695811c7316b58af03bf42151a2482

分析结果严重性

高危	中危	信息	安全	关注
1	9	1	2	0

四大组件信息

Activity组件：29个，其中export的有：1个
Service组件：2个，其中export的有：1个
Receiver组件：0个，其中export的有：0个
Provider组件：2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=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2022-11-29 15:33:21+00:00
有效期至: 2052-11-29 15:33:21+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xed40f5e8e4294573f208c7d6cb74e58e599929a4
哈希算法: sha256
证书MD5: 72acec29afbc1568de959c2828670989
证书SHA1: 99cf6cf61cdf11333a62149b4e10c5e87b58e5f5
证书SHA256: e5f1268b605aa9e28be9b043394fa1f01834ff5dd3bfc621b6e38cf3246f4b6f
证书SHA512:
8bbb75cd773fe53062d49d2cf773d5c0b20bdf80163dacc4fcd1a59931dc8ddae83f27ae243a165d1bf615d7a0f2443267de180e7efc9020b84b187fbd85fedd

公钥算法: rsa
密钥长度: 4096
指纹: fcb41df25f67edc53bf414ab05235895555ba710e59280a667dd907f04b4eeb4
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.DISABLE_KEYGUARD	危险	禁用键盘锁	允许应用程序停用键盘和任何关联的密码安全设置。例如，在手机上接听电话时停用键锁，在通话结束后重新启用键锁。
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.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.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
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.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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
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）

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.flextv.livestore.MainTVActivity) 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	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) 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。

安全漏洞检测

高危: **1** | 警告: **4** | 信息: **1** | 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	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	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	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	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

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
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
00056	修改语音音量	控制	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
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
00024	Base64解码后写入文件	反射 文件	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
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
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

敏感权限分析

类型	匹配	权限

恶意软件常用权限	3/30	android.permission.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK android.permission.WRITE_SETTINGS
其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_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。

域名检测

域名	状态	中国境内	位置信息
realm.io	安全	否	**IP地址:** 18.164.154.63 **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
docs.mongodb.com	安全	否	**IP地址:** 3.33.186.135 **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
iboproapp.com	安全	否	**IP地址:** 104.22.23.173 **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
i.ytimg.com	安全	否	**IP地址:** 142.250.188.246 **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

URL链接分析

URL信息	源码文件
• http://0.0.0.0:1234	iptv/m3u/parser/M3UParser.java
• http://i.ytimg.com/vi/	at/huber/youtubeExtractor/VideoMeta.java

• https://play.google.com/store/apps/details?id=org.videolan.vlc&hl=en_us • https://play.google.com/store/apps/details?id=com.mxtech.videoplayer.ad	com/flextv/livestore/activities/MovieActivity.java
• https://play.google.com/store/apps/details?id=org.videolan.vlc&hl=en_us • https://play.google.com/store/apps/details?id=com.mxtech.videoplayer.ad	com/flextv/livestore/activities/MovieSecondActivity.java
• https://iboproapp.com/manage-playlists/login/	com/flextv/livestore/apps/Constants.java
• https://play.google.com/store/apps/details?id=org.videolan.vlc&hl=en_us • https://play.google.com/store/apps/details?id=com.mxtech.videoplayer.ad	com/flextv/livestore/activities/SeasonActivity.java
• https://play.google.com/store/apps/details?id=org.videolan.vlc&hl=en_us • https://play.google.com/store/apps/details?id=com.mxtech.videoplayer.ad	com/flextv/livestore/activities/MovieInfoActivity.java
• https://play.google.com/store/apps/details?id=	com/flextv/livestore/activities/SettingActivity.java
• https://realm.io/docs/java/latest/#rxjava	io/realm/RealmObject.java
• https://github.com/realm/realm-java/tree/master/examples/rxjavaexample • https://docs.mongodb.com/realm/sdk/android/install/#customize-dependecies-defined-by-the-realm-gradle-plugin	io/realm/RealmConfiguration.java
• https://github.com/vinc3m1 • https://github.com/vinc3m1/roundedimageview.git • https://github.com/vinc3m1/roundedimageview	自研引擎-S

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。
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。

密钥凭证

可能的密钥
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
d96abf176686[illegible]7b8336a61933

免责声明及风险提示: