Evaluation Warning: The document was created with Spire.Doc for Python.

**91看电视HD（ 1.3.0版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 91看电视HD |
| 版本 | 1.3.0 |
| 包名 | com.kaixinhd.player |
| 域名线索 | 4条 |
| URL线索 | 6条 |
| APP图标 |  |
| 分析日期 | 2025年6月24日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | com.91kds.apk |
| 文件大小 | 10.9MB |
| MD5值 | f0367afe5a37fb336f9acc78516b53c0 |
| SHA1值 | c50c6722ca4e7ec8588f1daba673a13d4366c12a |
| SHA256值 | 30916029df4753e877dd227d675ae457692d9c0c0691d1c491bf932eecc2b78d |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 91看电视HD |
| 包名 | com.kaixinhd.player |
| 主活动Activity | com.kaixinhd.player.activity.StartActivity |
| 安卓版本名称 | 1.3.0 |
| 安卓版本 | 130 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| www.openssl.org | IP: 104.71.138.221 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| apkprotect.baidu.com | IP: 112.80.255.132 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| www.nagasoft.cn | IP: 175.178.176.44 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://%1$s:%2$d  | Mogua Engine V1  |
| https://apkprotect.baidu.com/apklog  | lib/armeabi-v7a/libbaiduprotect.so  |
| http://127.0.0.1:%d/1.flv  | lib/armeabi-v7a/libvjplayer\_jni.so  |
| http://127.0.0.1:%d/1.ts  | lib/armeabi-v7a/libvjplayer\_jni.so  |
| http://127.0.0.1:%d/1.%s  | lib/armeabi-v7a/libvjplayer\_jni.so  |
| http://%s/forcelive&begin=%d&count=%d/%s.ts  | lib/armeabi-v7a/libforcetv.so  |
| http://www.openssl.org/support/faq.html  | lib/armeabi-v7a/libijkffmpeg.so  |
| http://www.nagasoft.cn:8080/iptvauth.jsp  | lib/armeabi-v7a/libp2pcore.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| ffmpeg-devel@ffmpeg.org  | lib/armeabi-v7a/libijkplayer.so  |
| ftp@example.com  | lib/armeabi-v7a/libp2pcore.so  |

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: False v3 签名: False 找到 1 个唯一证书 主题: C=yuhua, ST=jiangsu, L=nanjing, O=keke\_studio, OU=keke\_studio, CN=keke\_studio 签名算法: rsassa\_pkcs1v15 有效期自: 2013-11-17 08:01:18+00:00 有效期至: 3013-03-20 08:01:18+00:00 发行人: C=yuhua, ST=jiangsu, L=nanjing, O=keke\_studio, OU=keke\_studio, CN=keke\_studio 序列号: 0x528877ce 哈希算法: sha1 md5值: 400db4e82d6a536e3182ff07b89c0058 sha1值: d280819e2e658aabd73e8fc9c9520b7a834d9892 sha256值: 374c49a48589310f13267ddfd2288c63ef64e930a231e620308ad9362e78124e sha512值: 8dc3f77da1d872f8eaeb34f74523371d0d2f86bc938684d6927c173ed0eadbebab1492e07a9777065ec42dae91b733c70201b27396316154608785865ae34ea2**

## **6. 硬编码敏感信息**

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 此APP的危险动作**

| 向手机申请的权限 | 是否危险 | 类型  | 详细情况 |
| --- | --- | --- | --- |
| android.permission.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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 | 读取外部存储器内容 | 允许应用程序从外部存储读取 |
| android.permission.ACCESS\_WIFI\_STATE | 正常 | 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 | 正常 | 查看网络状态 | 允许应用程序查看所有网络的状态 |
| android.permission.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| android.permission.CHANGE\_WIFI\_STATE | 正常 | 更改Wi-Fi状态 | 允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改 |
| android.permission.WAKE\_LOCK | 正常 | 防止手机睡眠  | 允许应用程序防止手机进入睡眠状态 |
| android.permission.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| android.permission.REQUEST\_INSTALL\_PACKAGES | 危险 | 允许应用程序请求安装包。 | 恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。 |
| android.permission.READ\_PHONE\_STATE | 危险 | 读取电话状态和身份 | 允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等 |
| android.permission.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.kaixinhd.player.activity.StartActivity | **Schemes**: kdshd://, **Hosts:** 91kds.com,  |

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**