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

**群晖电视（ 6.3.3.7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 | 群晖电视 |
| 版本 | 6.3.3.7 |
| 包名 | cn.dsmtv.player |
| 域名线索 | 16条 |
| URL线索 | 23条 |
| APP图标 |  |
| 分析日期 | 2025年2月22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 | 群晖直播.apk |
| 文件大小 | 17.55MB |
| MD5值 | bd42059844c78444d70f72a516e66367 |
| SHA1值 | f42db9170b394692a30d87165b223b832da6cf73 |
| SHA256值 | f1187d086badb99c3e67da65a604454ffc95b756098083952be44cbbf2e20731 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 群晖电视 |
| 包名 | cn.dsmtv.player |
| 主活动Activity | com.eztv.powerful.SplashActivity |
| 安卓版本名称 | 6.3.3.7 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| 192.168.31.231 | IP: 192.168.31.231 所属国家: - 地区: - 城市: -  |
| getbootstrap.com | IP: 104.22.58.100 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.nagasoft.cn | IP: 175.178.176.44 所属国家: China 地区: Beijing 城市: Beijing  |
| iptv.cpolar.top | IP: 116.211.150.89 所属国家: China 地区: Hubei 城市: Wuhan  |
| schemas.xmlsoap.org | IP: 13.107.246.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| ...php | 没有服务器地理信息.  |
| mobileso.bz.mgtv.com | IP: 218.12.91.143 所属国家: China 地区: Hebei 城市: Baoding  |
| webapi.miguvideo.com | IP: 117.131.17.8 所属国家: China 地区: Shanghai 城市: Shanghai  |
| irunmyway.github.io | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| www.macromedia.com | IP: 92.122.244.27 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| spk.bobohome.store | IP: 119.98.124.188 所属国家: China 地区: Hubei 城市: Wuhan  |
| www.bilibili.com | IP: 221.204.56.93 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| v.baidu.com | IP: 182.61.129.253 所属国家: China 地区: Beijing 城市: Beijing  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| www.openssl.org | IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://iptv.cpolar.top/iptv  | com/eztv/powerful/SplashActivity.java  |
| https://www.bilibili.com  | com/eztv/powerful/PlayerActivity.java  |
| http://webapi.miguvideo.com/gateway/playurl/v3/play/playurl?contId=63178053220200310002&rateType=3&clientId=196ce291da152c6363c6c26aad4444ba&channelId=0131\_10010001005  | com/eztv/powerful/PlayerActivity.java  |
| http://127.0.0.1:  | com/eztv/powerful/PlayerActivity.java  |
| http://spk.bobohome.store:8880  | com/eztv/powerful/PlayerActivity.java  |
| http://192.168.31.231:20230/iptv/epg/live\_proxy\_weather.php?  | com/eztv/powerful/PlayerActivity.java  |
| http://192.168.31.231:20230/iptv/epg/live\_proxy\_epg.php  | com/eztv/powerful/PlayerActivity.java  |
| https://mobileso.bz.mgtv.com/pc/suggest/v3?q=  | com/eztv/powerful/PlayerActivity.java  |
| http://...php  | com/eztv/powerful/PlayerActivity.java  |
| http://v.baidu.com/commonapi/tvplay2level/?filter=true&  | com/eztv/powerful/recycleview/b/a.java  |
| http://v.baidu.com/commonapi/movie2level/?filter=true&  | com/eztv/powerful/recycleview/b/a.java  |
| http://v.baidu.com/commonapi/tvshow2level/?filter=true&  | com/eztv/powerful/recycleview/b/a.java  |
| http://v.baidu.com/commonapi/comic2level/?filter=true&  | com/eztv/powerful/recycleview/b/a.java  |
| http://v.baidu.com/channel/commonapi/shaoer2level/?filter=true&  | com/eztv/powerful/recycleview/b/a.java  |
| http://v.baidu.com/commonapi/tvplay2level/?filter=true&type=  | com/eztv/powerful/recycleview/b/a.java  |
| http://v.baidu.com/commonapi/movie2level/?filter=true&type=  | com/eztv/powerful/recycleview/b/a.java  |
| https://irunmyway.github.io/2020/06/18/ez/  | com/eztv/powerful/widget/HelpActivity.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/c/a/h.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | com/c/a/h.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | com/c/a/h.java  |
| http://%s:%d/%s  | com/c/a/f.java  |
| http://127.0.0.1:  | net/media/mpc.java  |
| https://github.com/castorflex  | 摸瓜V1引擎  |
| https://github.com/castorflex/SmoothProgressBar  | 摸瓜V1引擎  |
| https://github.com/castorflex/SmoothProgressBar.git  | 摸瓜V1引擎  |
| http://getbootstrap.com)  | 摸瓜V2引擎  |
| 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://%s:%s%s  | lib/armeabi-v7a/libmpc\_jni.so  |
| http://%s:%s  | lib/armeabi-v7a/libmpc\_jni.so  |
| http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd  | lib/armeabi-v7a/libmpc\_jni.so  |
| https://www.openssl.org/docs/faq.html  | lib/armeabi-v7a/libmpc\_jni.so  |
| http://%s/forcelive&begin=%d&count=%d/%s.ts  | lib/armeabi-v7a/libp2p.so  |
| http://www.nagasoft.cn:8080/iptvauth.jsp  | lib/armeabi-v7a/libp2pcore.so  |
| http://%s/forcelive&begin=%d&count=%d/%s.ts  | lib/armeabi-v7a/libp3p.so  |
| http://%s/forcelive&begin=%d&count=%d/%s.ts  | lib/armeabi-v7a/libp4p.so  |
| http://%s/forcelive&begin=%d&count=%d/%s.ts  | lib/armeabi-v7a/libp5p.so  |
| http://%s/forcelive&begin=%d&count=%d/%s.ts  | lib/armeabi-v7a/libp6p.so  |
| http://%s/forcelive&begin=%d&count=%d/%s.ts  | lib/armeabi-v7a/libp7p.so  |
| http://%s/forcelive&begin=%d&count=%d/%s.ts  | lib/armeabi-v7a/libp8p.so  |
| http://%s/forcelive&begin=%d&count=%d/%s.ts  | lib/armeabi-v7a/libp9p.so  |
| http://127.0.0.1:%d/mpegts\_live  | lib/armeabi-v7a/libtvcore.so  |
| http://127.0.0.1:%d/%lu/index.m3u8  | lib/armeabi-v7a/libtvcore.so  |
| http://www.openssl.org/support/faq.html  | lib/armeabi-v7a/libtvcore.so  |
| http://[fe80:  | lib/armeabi-v7a/libtvcore.so  |
| http://schemas.xmlsoap.org/soap/envelope/  | lib/armeabi-v7a/libtvcore.so  |
| http://schemas.xmlsoap.org/soap/encoding/  | lib/armeabi-v7a/libtvcore.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://127.0.0.1:%u/%llu.%s  | lib/armeabi-v7a/libvjplayer\_jni.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com  | com/c/a/h.java  |
| tvb@gmail.com  | net/media/mpc.java  |
| ffmpeg-devel@ffmpeg.org  | lib/armeabi-v7a/libijkplayer.so  |
| ftp@example.com  | lib/armeabi-v7a/libp2pcore.so  |
| ftp@example.com  | lib/armeabi-v7a/libtvcore.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.java  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: True 找到 1 个唯一证书 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 md5值: e89b158e4bcf988ebd09eb83f5378e87 sha1值: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81 sha256值: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc sha512值: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569 公钥算法: rsa 密钥长度: 2048 指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "library\_smoothprogressbar\_author" : "Antoine Merle"  |
| "library\_smoothprogressbar\_authorWebsite" : "https://github.com/castorflex"  |

## **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.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.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.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.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.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.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| android.permission.CHANGE\_CONFIGURATION | 系统需要 | 更改您的 UI 设置 | 允许应用程序更改当前配置,例如语言环境或整体字体大小 |
| android.permission.DOWNLOAD\_WITHOUT\_NOTIFICATION | 未知 | Unknown permission | Unknown permission from android reference |
| 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.WRITE\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |
| 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。 |

## **10. 应用内通信**

**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。**