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

**直播电视（ VIP20241010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 | 直播电视 |
| 版本 | VIP20241010 |
| 包名 | com.zb.test |
| 域名线索 | 20条 |
| URL线索 | 18条 |
| APP图标 |  |
| 分析日期 | 2025年7月5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 | zbds.apk |
| 文件大小 | 13.08MB |
| MD5值 | 480c604092ab677b05cbc097d4305a3e |
| SHA1值 | ea28105d9f50be42753c4b0dd8b1b291725d181a |
| SHA256值 | a4be363924d243da6e429dc41643cc76058ddddb5ec908d49197951a7fcda95d |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 直播电视 |
| 包名 | com.zb.test |
| 主活动Activity | com.vv.test.SplashActivity |
| 安卓版本名称 | VIP20241010 |
| 安卓版本 | 13 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| c.appjiagu.com | IP: 106.63.25.12 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.openssl.org | IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View  |
| jquery.com | IP: 104.18.156.119 所属国家: United States of America 地区: California 城市: San Francisco  |
| schemas.xmlsoap.org | IP: 13.107.246.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| feross.org | IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont  |
| stackoverflow.com | IP: 104.18.32.7 所属国家: United States of America 地区: California 城市: San Francisco  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| sizzlejs.com | IP: 104.17.99.190 所属国家: United States of America 地区: California 城市: San Francisco  |
| fb.me | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| gcc.gnu.org | IP: 8.43.85.97 所属国家: United States of America 地区: North Carolina 城市: Raleigh  |
| www.nagasoft.cn | IP: 175.178.176.44 所属国家: China 地区: Beijing 城市: Beijing  |
| jquery.org | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| www.macromedia.com | IP: 104.75.169.27 所属国家: Japan 地区: Osaka 城市: Osaka  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| upload.ffmpeg.org | IP: 213.36.253.119 所属国家: France 地区: Ile-de-France 城市: Paris  |
| live-1253296737.file.myqcloud.com | IP: 116.131.57.65 所属国家: China 地区: Beijing 城市: Beijing  |
| zb.zhoujie218.top | IP: 101.132.153.183 所属国家: China 地区: Shanghai 城市: Shanghai  |
| curl.haxx.se | IP: 151.101.90.49 所属国家: United States of America 地区: California 城市: San Francisco  |
| facebook.github.io | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| 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://jquery.com/  | 摸瓜V2引擎  |
| http://sizzlejs.com/  | 摸瓜V2引擎  |
| http://jquery.org/license  | 摸瓜V2引擎  |
| https://fb.me/react-spread-deprecation  | 摸瓜V2引擎  |
| http://facebook.github.io/react/docs/error-decoder.html?invariant=  | 摸瓜V2引擎  |
| https://fb.me/react-special-props)  | 摸瓜V2引擎  |
| https://github.com/facebook/react/issues/3236).  | 摸瓜V2引擎  |
| https://fb.me/react-legacyfactory  | 摸瓜V2引擎  |
| https://fb.me/react-warning-keys  | 摸瓜V2引擎  |
| https://fb.me/react-warning-dont-call-proptypes  | 摸瓜V2引擎  |
| https://fb.me/react-devtools  | 摸瓜V2引擎  |
| https://fb.me/react-minification  | 摸瓜V2引擎  |
| https://fb.me/react-warning-polyfills  | 摸瓜V2引擎  |
| https://fb.me/react-event-pooling  | 摸瓜V2引擎  |
| https://fb.me/react-refs-must-have-owner).  | 摸瓜V2引擎  |
| https://fb.me/react-invariant-dangerously-set-inner-html  | 摸瓜V2引擎  |
| https://fb.me/react-controlled-components  | 摸瓜V2引擎  |
| https://fb.me/react-unknown-prop%s  | 摸瓜V2引擎  |
| https://fb.me/invalid-aria-prop%s  | 摸瓜V2引擎  |
| https://github.com/zertosh/loose-envify)  | 摸瓜V2引擎  |
| http://stackoverflow.com/questions/30030031)  | 摸瓜V2引擎  |
| https://github.com/reactjs/react-redux/releases/tag/v2.0.0  | 摸瓜V2引擎  |
| http://feross.org>  | 摸瓜V2引擎  |
| ftp://upload.ffmpeg.org/incoming/  | 摸瓜V3引擎  |
| http://%s:%d/force&begin=%lld&count=%lld/%s.ts  | 摸瓜V3引擎  |
| http://www.nagasoft.cn:8080/iptvauth.jsp&stream=live&cgi=msgpeeroffpeerget  | 摸瓜V3引擎  |
| http://127.0.0.1:%d/mpc\_start\_play.m3u8  | 摸瓜V3引擎  |
| http://httpsfastopenijkapplicationAppleCoreMedia/1.0.0.9A405  | 摸瓜V3引擎  |
| http://127.0.0.1:%d/cid.m3u8  | 摸瓜V3引擎  |
| http://127.0.0.1:%d/1.flv  | 摸瓜V3引擎  |
| http://127.0.0.1:%d/1.%sRange:bytes=%llu-%lluIf-Modified-Since:If-None-Match:ETag:CVodSession::  | 摸瓜V3引擎  |
| https://github.com/castorflex/SmoothProgressBar  | 摸瓜V3引擎  |
| http://www.nagasoft.cn:8080/iptvauth.jsp  | 摸瓜V3引擎  |
| http://127.0.0.1:%d/1.tsSendData  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |
| http://c.appjiagu.com/apk/cr.html  | 摸瓜V3引擎  |
| http://sizzlejs.com/  | 摸瓜V3引擎  |
| https://github.com/castorflex  | 摸瓜V3引擎  |
| http://127.0.0.1:%d/1.ts  | 摸瓜V3引擎  |
| http://schemas.xmlsoap.org/soap/envelope/  | 摸瓜V3引擎  |
| www.googleapis.com  | 摸瓜V3引擎  |
| http://jquery.com/  | 摸瓜V3引擎  |
| https://www.openssl.org/docs/faq.html  | 摸瓜V3引擎  |
| http://127.0.0.1:%d/%lu/index.m3u8hlsOnPrepared:  | 摸瓜V3引擎  |
| http://curl.haxx.se/rfc/cookie\_spec.html  | 摸瓜V3引擎  |
| http://c.appjiagu.com/apk/cr.html0%.0f%e%f  | 摸瓜V3引擎  |
| http://live-1253296737.file.myqcloud.com/code.json  | 摸瓜V3引擎  |
| http://127.0.0.1:%d/1.%s  | 摸瓜V3引擎  |
| http://www.openssl.org/support/faq.html/var/run/egd-pool/dev/egd-pool/etc/egd-pool/etc/entropy/dev/r  | 摸瓜V3引擎  |
| https://curl.haxx.se/docs/http-cookies.html  | 摸瓜V3引擎  |
| http://%s/forcelive&begin=%d&count=%d/%s.tsnew  | 摸瓜V3引擎  |
| http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd  | 摸瓜V3引擎  |
| http:///cgi-bin/live.fcgitype=live&cid=&begin=&time=start/cgi-bin/vod.fcgitype=vod&cid=&hash=&mime=&  | 摸瓜V3引擎  |
| http://feross.org  | 摸瓜V3引擎  |
| http://schemas.xmlsoap.org/soap/encoding/  | 摸瓜V3引擎  |
| play.googleapis.com  | 摸瓜V3引擎  |
| http://www.openssl.org/support/faq.html  | 摸瓜V3引擎  |
| infinitedata-pa.googleapis.com  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto  | 摸瓜V3引擎  |
| http://jquery.org/license  | 摸瓜V3引擎  |
| http://%s:%d/forcelive&begin=loading&count=0/%s.ts  | 摸瓜V3引擎  |
| http://127.0.0.1:%d/%lu/index.m3u8  | 摸瓜V3引擎  |
| http://gcc.gnu.org/bugs.html):  | 摸瓜V3引擎  |
| https://github.com/castorflex/SmoothProgressBar.git  | 摸瓜V3引擎  |
| http://127.0.0.1:%u/%llu.%sEnter  | 摸瓜V3引擎  |
| http://127.0.0.1:%d/mpegts\_livehttp  | 摸瓜V3引擎  |
| http://127.0.0.1:%d/1.flvvector::\_M\_insert\_auxvector::\_M\_fill\_inserterase  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto99fr.castorflex.android.smoothprogressbar.SmoothProgressBar  | 摸瓜V3引擎  |
| zb.zhoujie218.top  | 摸瓜V3引擎  |
| http://www.openssl.org/support/faq.htmldual  | 摸瓜V3引擎  |
| http://%s/forcelive&begin=%d&count=%d/%s.ts  | 摸瓜V3引擎  |
| http://127.0.0.1:%u/%llu.%s  | 摸瓜V3引擎  |
| http://127.0.0.1:%d/mpegts\_live  | 摸瓜V3引擎  |
| http://%s/forcelive&begin=%d&count=%d/%s.ts  | lib/armeabi-v7a/libforcetv.so  |
| http://live-1253296737.file.myqcloud.com/code.json  | lib/armeabi-v7a/libgetName.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 |
| --- | --- |
| feross@feross.org  | 摸瓜V2引擎  |
| 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**

## **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=cn, ST=jx, L=nc, O=zhou, OU=zhou, CN=zhoujie 签名算法: rsassa\_pkcs1v15 有效期自: 2024-10-11 07:12:07+00:00 有效期至: 2052-02-27 07:12:07+00:00 发行人: C=cn, ST=jx, L=nc, O=zhou, OU=zhou, CN=zhoujie 序列号: 0x8a7d620e270ca038 哈希算法: sha384 md5值: f2d3ea049cc4bba89a0f153641eb409c sha1值: 1de40728d059fac1f6a5581975ff40d134b9a034 sha256值: f8837ba71980c71bc87a7ca72a2aa4eef08a25cd6ebbc5b9f402483a37a4ff4e sha512值: 0462102d4d2f064796fcacc79664179ec11b842314c5dc12444730aaa067bf0df5b3e860bb636dab72a2beaeeb9eb2c220eb3b466b98993d1800410e54aec850 公钥算法: rsa 密钥长度: 2048 指纹: 08698bfd6b10bbc862972bbf6baf93e7cb56c1d9d2b1cbb0841a02f6a6969ce2**

## **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 |

## **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。**