



MoGua

超清直播 9.2.8.APK 分析报告



APP名称:

超清直播

包名:	hutf8.chaoqing.nh4d8
域名线索:	14条
URL线索:	16条
邮箱线索:	4条
分析日期:	2024年10月16日
分析平台:	摸瓜APK反编译平台

文件名: hudf8.chaoqing.nh4d8_9.2.8_1728925908_yecao.apk
文件大小: 15.78MB
MD5值: e4ebca07b268ee36d76c888166f06c92
SHA1值: e3fc843b12cc5b1974aedc6cc0a012396fe33247
SHA256值: 007e0c57c7ee3a2d478ea463504291b011ff57ca8409b058f9ef0f71c6f0c821

i APP 信息

App名称: 超清直播
包名: hudf8.chaoqing.nh4d8
主活动Activity: com.vv.test.SplashActivity
安卓版本名称: 9.2.8
安卓版本: 928

🔍 域名线索

域名	服务器信息
stackoverflow.com	IP: 104.18.32.7 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
feross.org	IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont 纬度: 37.548271 经度: -121.988571
www.openssl.org	IP: 34.49.79.89 所属国家: United States of America 地区: California

	城市: Mountain View 纬度: 37.405991 经度: -122.078514
www.macromedia.com	IP: 23.216.153.92 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
sizzlejs.com	IP: 104.17.99.190 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
facebook.github.io	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
127.0.0.1	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
www.nagasoft.cn	IP: 175.178.176.44 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
jquery.com	IP: 104.18.155.119 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
schemas.xmlsoap.org	IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
fb.me	IP: 157.240.22.35 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.339390 经度: -121.894958
jquery.org	IP: 104.18.159.194 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700

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	摸瓜V2引擎
https://fb.me/invalid-aria-prop	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
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/libp7p.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/libp2p.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/libp5p.so
http://%s/forcelive&begin=%d&count=%d/%s.ts	lib/armeabi-v7a/libp9p.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://www.nagasoftware.cn:8080/iptvauth.jsp	lib/armeabi-v7a/libp2pcore.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/libforcetv.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://%s/forcelive&begin=%d&count=%d/%s.ts	lib/armeabi-v7a/libp4p.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libijkffmpeg.so

 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

 手机线索

 签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=086, ST=江苏, L=常州, O=群众, OU=常州陈迪公司, CN=xkys.keystore
签名算法: rsassa_pkcs1v15
有效期自: 2024-08-28 15:20:54+00:00
有效期至: 2025-08-28 15:20:54+00:00
发行人: C=086, ST=江苏, L=常州, O=群众, OU=常州陈迪公司, CN=xkys.keystore

序列号: 0x7ca9312cf848b40c
哈希算法: sha256
md5值: 8b7d038b5cad732467cce4d01c294f38
sha1值: 7d9ed044de0884acdf86b57f3baf05f6f2048901
sha256值: 503ea1b33179142fcc6635ae0bda7e7d7ec7f0839ef1244ffea6a8a076627a8e
sha512值: 0a9680c56166491dc77cbd3dc2152ed099e829e23e9ea0af010a6dae98a635b7311f6fb7e10eeab2cde41ecb268e50a00ad87e82deb6684c5fc92071d397c8ed
公钥算法: rsa
密钥长度: 1024
指纹: e6e48257c6e830ba7344e0f5252fc050fe48fb5bcfc4434cb1f6287be689a0ee

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"

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

☰ 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

📠 应用内通信