



MoGua

九洲 8.0.8.APK 分析报告



APP名称:

九洲

包名: smlszv.piouswog.uwogvh.zdvhnd

域名线索: 18条

URL线索: 12条

邮箱线索: 1条

分析日期: 2025年5月9日

分析平台: [摸瓜APK反编译平台](#)

文件名: 1wedmTGk0m_1.apk
文件大小: 78.51MB
MD5值: c43033ce17416741dd226f64d4d0e54e
SHA1值: 9be333b754b325a65b22d0419925f7804d24aea3
SHA256值: d8d6adfde85e7b721dbd10ec83b5698155f4d6a75e301c3df0c2eb1579b4ecb7

i APP 信息

App名称: 九洲
包名: smlszv.piouswog.uwogvh.zdvhnd
主活动Activity: at1jey9e.bbsj2oibr.tyxydhpd.qkzegfos9.rph7gfdvt.MainActivity
安卓版本名称: 8.0.8
安卓版本: 1

🔍 域名线索

域名	服务器信息
dartbug.com	IP: 216.239.34.21 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
flutter.dev	IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
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
www.gnu.org	IP: 209.51.188.116 所属国家: United States of America 地区: Massachusetts 城市: Somerville 纬度: 42.387600 经度: -71.099503
paulbakaus.com	IP: 167.172.18.193 所属国家: United States of America 地区: New Jersey 城市: Clifton 纬度: 40.858585 经度: -74.163605
www.ibm.com	IP: 23.1.167.82 所属国家: Japan 地区: Osaka 城市: Ibaraki 纬度: 34.816425 经度: 135.568909
www.webrtc.org	IP: 172.217.14.206 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
www.ietf.org	IP: 104.16.45.99 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

www.unicode.org	IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas 纬度: 32.814899 经度: -96.879204
developer.mozilla.org	IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
dev.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
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
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
docs.flutter.dev	IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View

	纬度: 37.405991 经度: -122.078514
api.flutter.dev	IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
ns.adobe.com	没有服务器地理信息.
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
aomediadecodec.github.io	IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724

 URL线索

URL信息	Url所在文件
https://github.com/richtr/NoSleep.js/issues/15	摸瓜V2引擎
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released	摸瓜V2引擎
">https://www.gnu.org/licenses/> .	摸瓜V2引擎

https://www.gnu.org/licenses/ >.	摸瓜V2引擎
https://www.gnu.org/licenses/ >.	摸瓜V2引擎
http://paulbikaus.com/tutorials/html5/web-audio-on-ios/	摸瓜V2引擎
http://stackoverflow.com/questions/24119684	摸瓜V2引擎
https://github.com/nodeca/pica	摸瓜V2引擎
http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrext/playout-delay	lib/armeabi-v7a/libliteavsdk.so
http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrext/meta-data-01	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrext/meta-data-02	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrext/meta-data-03	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrext/decoding-timestamp	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrext/video-composition-time	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrext/video-frame-type	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrext/transport-wide-cc-02	lib/armeabi-v7a/libliteavsdk.so
https://aomediacodec.github.io/av1-rtp-spec/	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor-00	lib/armeabi-v7a/libliteavsdk.so

http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrext/video-content-type	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrext/video-timing	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrext/color-space	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrext/inband-cn	lib/armeabi-v7a/libliteavsdk.so
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libimagepipeline.so
http://www.unicode.org/copyright.html	lib/armeabi-v7a/libflutter.so
https://docs.flutter.dev/release/breaking-changes/android-surface-plugins	lib/armeabi-v7a/libflutter.so
https://github.com/flutter/flutter/issues	lib/armeabi-v7a/libflutter.so
https://dartbug.com/52121	lib/armeabi-v7a/libflutter.so
http://127.0.0.1:%d/proxy/%d/%d/vod_%d.m3u8?play_id=%d&clip_id=%d&force_online=0	lib/armeabi-v7a/libdownloadproxy.so
http://127.0.0.1:%d/proxy/%d/%d/%s?play_id=%d&clip_id=%d&force_online=0%s	lib/armeabi-v7a/libdownloadproxy.so
http://127.0.0.1:%d/proxy/%d/%d/master.m3u8?play_id=%d&clip_id=%d&force_online=0	lib/armeabi-v7a/libdownloadproxy.so
http://127.0.0.1:%d/proxy/%d/%d/vod.mp4?play_id=%d&clip_id=%d&force_online=0	lib/armeabi-v7a/libdownloadproxy.so
http://127.0.0.1:%d/proxy/%d/%d/%s.mpd_tp_dl_autotype?play_id=%d&clip_id=%d&force_online=0	lib/armeabi-v7a/libdownloadproxy.so
http://127.0.0.1:%d/proxy/%d/%d/%s_tp_dl_autotype?play_id=%d&clip_id=%d&force_online=0	lib/armeabi-v7a/libdownloadproxy.so
http://127.0.0.1:%d/proxy/%d/%d/%s?play_id=%d&clip_id=%d&force_online=0	lib/armeabi-v7a/libdownloadproxy.so
http://127.0.0.1:%d/proxy/%d/%d/vod.m3u8?play_id=%d&clip_id=%d&force_online=0	lib/armeabi-v7a/libdownloadproxy.so

http://127.0.0.1:%d/proxy/%d/%d/live.m3u8?play_id=%d&clip_id=%d&force_online=0	lib/armeabi-v7a/libdownloadproxy.so
http://127.0.0.1:%d/proxy/%d/1/%s.flv?play_id=%d&clip_id=1&force_online=0	lib/armeabi-v7a/libdownloadproxy.so
http://127.0.0.1:%d/proxy/%d/%d/loop.m3u8?play_id=%d&clip_id=%d&force_online=0	lib/armeabi-v7a/libdownloadproxy.so
http://127.0.0.1:	lib/armeabi-v7a/libapp.so
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so
http://127.0.0.1:88888/	lib/armeabi-v7a/libapp.so
http://kiwi_live/tunnel/a033b072?z=1&nobase64=1	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.	lib/armeabi-v7a/libapp.so
http://kiwi_install	lib/armeabi-v7a/libapp.so
http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor	lib/armeabi-v7a/libagora-rtc-sdk.so
http://s	lib/armeabi-v7a/libagora-rtc-sdk.so

 邮箱线索

邮箱地址	所在文件
_growablelist@0150898._literal _typeerror@0150898._create _xfa@56287047.wqd _bytebuffer@7027147._new lib/armeabi-v7a/libapp.so	

```
_double@0150898.frominteg  
_immutablelist@0150898.tk  
_assertionerror@0150898._create
```

手机线索

✿ 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=CN, ST=Beijing, L=Beijing, O=cVRiZsEC, OU=XxwJNTwZ, CN=qAfpOtLi

签名算法: dsa

有效期自: 2025-03-25 09:35:54+00:00

有效期至: 2031-03-18 09:35:54+00:00

发行人: C=CN, ST=Beijing, L=Beijing, O=cVRiZsEC, OU=XxwJNTwZ, CN=qAfpOtLi

序列号: 0x1514cce8

哈希算法: sha256

md5值: d0c1ace015a619372c14c5570ce4deae

sha1值: 2d731605781d6199d9c9913832718916464b69f3

sha256值: c5321921e4f756cefd1280c3ddc8107b4c92166afe0f8e84c63c67d746995aa5

sha512值: 278620efc60d75ae51f6015729a89de8f6310e6e246bb5c8a87caa3b3127484e7d233d300f6ebaad654891c82104142f608688ace66f83a56887fdef7a146cdc

硬编码敏感信息

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.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference
android.permission.INTERNET	正	互联网接入	

	常		允许应用程序创建网络套接字
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.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
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.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.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
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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.PACKAGE_USAGE_STATS	合法	更新组件使用统计	允许修改收集的组件使用统计。不供普通应用程序使用
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	未知	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由

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
smlszv.piouswog.uwogvh.zdvhnd.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
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.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference

应用内通信