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

**应急通（ 1.0.2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 | 应急通 |
| 版本 | 1.0.2 |
| 包名 | io.zzsf.app.enterprisechat |
| 域名线索 | 45条 |
| URL线索 | 46条 |
| APP图标 |  |
| 分析日期 | 2024年9月14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 | zzsf\_release.apk |
| 文件大小 | 79.9MB |
| MD5值 | c45bc335d95641d45dd69a97e02ef124 |
| SHA1值 | 8b698e1fa29250fff30f6e3d9978559b47af09f8 |
| SHA256值 | ecf7d520fbeb304bc19036a52dc51e57a17338cc1bd174ee8ffed13e59ed7453 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 应急通 |
| 包名 | io.zzsf.app.enterprisechat |
| 主活动Activity | io.zzsf.app.enterprisechat.MainActivity |
| 安卓版本名称 | 1.0.2 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| apps.samsung.com | IP: 103.254.189.69  所属国家: China  地区: Beijing  城市: Beijing |
| ru.register.xmpush.global.xiaomi.com | IP: 107.155.52.56  所属国家: Russian Federation  地区: Moskva  城市: Moscow |
| schemas.microsoft.com | IP: 13.107.213.49  所属国家: United States of America  地区: Washington  城市: Redmond |
| resolver.msg.xiaomi.net | IP: 183.84.5.221  所属国家: China  地区: Beijing  城市: Beijing |
| www.baidu.com | IP: 110.242.68.3  所属国家: China  地区: Hebei  城市: Baoding |
| astat.bugly.qcloud.com | IP: 150.109.27.253  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.example.com | IP: 93.184.216.34  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| webrd01.is.autonavi.com | IP: 36.102.212.90  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| exoplayer.dev | IP: 185.199.108.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| maps.apple.com | IP: 103.254.191.161  所属国家: China  地区: Beijing  城市: Beijing |
| flutter.dev | IP: 151.101.65.195  所属国家: United States of America  地区: California  城市: San Francisco |
| dashif.org | IP: 185.199.108.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| play.google.com | IP: 172.217.160.78  所属国家: United States of America  地区: California  城市: Mountain View |
| xmlpull.org | IP: 74.50.61.58  所属国家: United States of America  地区: Texas  城市: Dallas |
| github.com | IP: 20.205.243.166  所属国家: United States of America  地区: Washington  城市: Redmond |
| android.bugly.qq.com | IP: 109.244.244.137  所属国家: China  地区: Beijing  城市: Beijing |
| ce3e75d5.jpush.cn | IP: 183.232.58.242  所属国家: China  地区: Guangdong  城市: Guangzhou |
| register.xmpush.global.xiaomi.com | IP: 47.88.199.5  所属国家: Singapore  地区: Singapore  城市: Singapore |
| schemas.android.com | 没有服务器地理信息. |
| astat.bugly.cros.wr.pvp.net | IP: 170.106.135.32  所属国家: United States of America  地区: California  城市: San Francisco |
| www.jivesoftware.com | IP: 35.238.7.255  所属国家: United States of America  地区: Iowa  城市: Council Bluffs |
| yjj-zzszfxportal.z.digitalcnzz.com | IP: 42.228.55.222  所属国家: China  地区: Henan  城市: Zhengzhou |
| xml.org | IP: 104.239.240.11  所属国家: United States of America  地区: Texas  城市: Windcrest |
| aomediacodec.github.io | IP: 185.199.108.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| developer.android.com | IP: 172.217.163.46  所属国家: United States of America  地区: California  城市: Mountain View |
| www.w3.org | IP: 128.30.52.100  所属国家: United States of America  地区: Massachusetts  城市: Cambridge |
| maps.google.com | IP: 142.251.42.238  所属国家: United States of America  地区: California  城市: Mountain View |
| fr.register.xmpush.global.xiaomi.com | IP: 3.65.144.146  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| crbug.com | IP: 216.239.32.29  所属国家: United States of America  地区: California  城市: Mountain View |
| api-push.meizu.com | IP: 125.94.213.129  所属国家: China  地区: Guangdong  城市: Guangzhou |
| yjj-zzszfxim.z.digitalcnzz.com | IP: 42.228.55.222  所属国家: China  地区: Henan  城市: Zhengzhou |
| store.hispace.hicloud.com | IP: 49.4.32.127  所属国家: China  地区: Beijing  城市: Beijing |
| www.ietf.org | IP: 104.16.44.99  所属国家: United States of America  地区: Texas  城市: Dallas |
| apis.map.qq.com | IP: 109.244.244.223  所属国家: China  地区: Beijing  城市: Beijing |
| share.here.com | IP: 54.171.147.76  所属国家: Ireland  地区: Dublin  城市: Dublin |
| www.webrtc.org | IP: 172.217.160.78  所属国家: United States of America  地区: California  城市: Mountain View |
| resolver.msg.global.xiaomi.net | IP: 47.241.56.51  所属国家: Singapore  地区: Singapore  城市: Singapore |
| cn.register.xmpush.xiaomi.com | IP: 203.100.92.32  所属国家: China  地区: Beijing  城市: Beijing |
| idmb.register.xmpush.global.xiaomi.com | IP: 13.234.36.106  所属国家: India  地区: Maharashtra  城市: Mumbai |
| ns.adobe.com | 没有服务器地理信息. |
| norma-external-collect.meizu.com | IP: 113.106.27.98  所属国家: China  地区: Guangdong  城市: Zhongshan |
| api.flutter.dev | IP: 199.36.158.100  所属国家: United States of America  地区: California  城市: Mountain View |
| appgallery.cloud.huawei.com | IP: 49.4.35.33  所属国家: China  地区: Beijing  城市: Beijing |
| api-push.in.meizu.com | IP: 206.161.233.191  所属国家: United States of America  地区: Virginia  城市: Herndon |
| journeyapps.com | IP: 13.225.165.91  所属国家: Japan  地区: Tokyo  城市: Tokyo |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://android.bugly.qq.com/rqd/async | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java |
| https://astat.bugly.qcloud.com/rqd/async | com/tencent/bugly/crashreport/common/strategy/c.java |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async | com/tencent/bugly/crashreport/common/strategy/c.java |
| http://www.example.com | com/pichillilorenzo/flutter\_inappwebview/chrome\_custom\_tabs/CustomTabsHelper.java |
| https://github.com/pichillilorenzo/flutter\_inappwebview#important-note-for-android | com/pichillilorenzo/flutter\_inappwebview/in\_app\_webview/FlutterWebView.java |
| https://github.com/flutter/flutter/wiki/Upgrading-pre-1.12-Android-projects | com/pichillilorenzo/flutter\_inappwebview/in\_app\_webview/FlutterWebView.java |
| https://api-push.meizu.com/garcia/api/client/ | com/meizu/cloud/pushsdk/platform/a/a.java |
| https://api-push.in.meizu.com/garcia/api/client/ | com/meizu/cloud/pushsdk/platform/a/a.java |
| https://api-push.meizu.com/garcia/api/client/log/upload | com/meizu/cloud/pushsdk/platform/a/a.java |
| https://api-push.meizu.com/garcia/api/server/getPublicKey | com/meizu/cloud/pushsdk/constants/PushConstants.java |
| https://api-push.in.meizu.com | com/meizu/cloud/pushsdk/constants/PushConstants.java |
| https://api-push.meizu.com | com/meizu/cloud/pushsdk/constants/PushConstants.java |
| https://norma-external-collect.meizu.com/android/exchange/getpublickey.do | com/meizu/cloud/pushsdk/constants/PushConstants.java |
| https://norma-external-collect.meizu.com/push/android/external/add.do | com/meizu/cloud/pushsdk/constants/PushConstants.java |
| http://xml.org/sax/features/namespaces | com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java |
| http://xml.org/sax/features/validation | com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java |
| http://xml.org/sax/features/namespaces | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xml.org/sax/features/namespace-prefixes | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xml.org/sax/features/validation | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xml.org/sax/features/external-general-entities | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xml.org/sax/features/external-parameter-entities | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xml.org/sax/features/string-interning | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java |
| http://xmlpull.org/v1/doc/features.html#process-namespaces | com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java |
| http://xmlpull.org/v1/doc/features.html#report-namespace-prefixes | com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java |
| http://xmlpull.org/v1/doc/features.html#process-docdecl | com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java |
| http://xmlpull.org/v1/doc/features.html#validation | com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java |
| http://xmlpull.org/v1/doc/features.html#process-namespaces | com/xiaomi/push/gp.java |
| http://xmlpull.org/v1/doc/features.html#process-namespaces | com/xiaomi/push/gd.java |
| http://www.jivesoftware.com/xmlns/xmpp/properties | com/xiaomi/push/ha.java |
| http://xmlpull.org/v1/doc/features.html#process-namespaces | com/xiaomi/push/hi.java |
| http://xmlpull.org/v1/doc/features.html#process-namespaces | com/xiaomi/push/hh.java |
| https://%1$s/gslb/?ver=4.0 | com/xiaomi/push/cu.java |
| https://resolver.msg.global.xiaomi.net/psc/?t=a | com/xiaomi/push/service/bt.java |
| https://resolver.msg.xiaomi.net/psc/?t=a | com/xiaomi/push/service/bt.java |
| https://cn.register.xmpush.xiaomi.com | com/xiaomi/push/service/s.java |
| https://register.xmpush.global.xiaomi.com | com/xiaomi/push/service/s.java |
| https://fr.register.xmpush.global.xiaomi.com | com/xiaomi/push/service/s.java |
| https://ru.register.xmpush.global.xiaomi.com | com/xiaomi/push/service/s.java |
| https://idmb.register.xmpush.global.xiaomi.com | com/xiaomi/push/service/s.java |
| www.baidu.com:80 | com/xiaomi/push/service/an.java |
| https://ce3e75d5.jpush.cn/wi/cjc4sa | cn/jiguang/au/c.java |
| https://ce3e75d5.jpush.cn/wi/d8n3hj | cn/jiguang/au/c.java |
| http://apps.samsung.com/appquery/appDetail.as?appId= | cn/jpush/android/af/f.java |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread | f/h/a/b/g2.java |
| https://x | f/h/a/b/v3/g0.java |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense | f/h/a/b/v3/h0.java |
| http://dashif.org/guidelines/trickmode | f/h/a/b/b4/a1/f.java |
| http://dashif.org/guidelines/last-segment-number | f/h/a/b/b4/a1/m/d.java |
| http://dashif.org/guidelines/trickmode | f/h/a/b/b4/a1/m/d.java |
| http://ns.adobe.com/xap/1.0/ | f/h/a/b/w3/i0/a.java |
| http://www.w3.org/ns/ttml#parameter | f/h/a/b/c4/s/c.java |
| http://ns.adobe.com/xap/1.0/ | d/m/a/a.java |
| http://schemas.android.com/apk/res/android | d/i/b/e/i.java |
| https://github.com/flutter/flutter/issues/2897).It | io/flutter/plugin/platform/PlatformViewsController.java |
| https://developer.android.com/guide/topics/permissions/overview | io/flutter/plugin/platform/PlatformPlugin.java |
| https://developer.android.com/reference/javax/net/ssl/SSLSocket | io/flutter/plugins/videoplayer/VideoPlayerPlugin.java |
| https://play.google.com/store/apps/details?id= | Android String Resource |
| https://appgallery.cloud.huawei.com | Android String Resource |
| https://journeyapps.com/ | Android String Resource |
| https://github.com/journeyapps/zxing-android-embedded | Android String Resource |
| https://store.hispace.hicloud.com/hwmarket/api/ | Android String Resource |
| http://www.w3.org/XML/1998/namespace | lib/armeabi-v7a/libflutter.so |
| http://www.w3.org/2000/xmlns/ | lib/armeabi-v7a/libflutter.so |
| https://www.w3.org/Style/CSS/Test/Fonts/Ahem/). | lib/armeabi-v7a/libflutter.so |
| https://github.com/flutter/flutter/issues. | lib/armeabi-v7a/libflutter.so |
| https://yjj-zzszfxportal.z.digitalcnzz.com:20017/app/register/user/avatar/update | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxportal.z.digitalcnzz.com:20017/pai/pai-sso/msg/register/sendMessage | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxim.z.digitalcnzz.com:20013/friend/import\_friend | lib/armeabi-v7a/libapp.so |
| https://webrd01.is.autonavi.com/appmaptile?lang=zh\_cn&size=1&scale=1&style=8&x={x}&y={y}&z={z} | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxportal.z.digitalcnzz.com:20017/app/register/administrative/division/list | lib/armeabi-v7a/libapp.so |
| https://share.here.com/l/ | lib/armeabi-v7a/libapp.so |
| https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxim.z.digitalcnzz.com:20013/manager/get\_all\_users\_uid | lib/armeabi-v7a/libapp.so |
| http://maps.apple.com/maps | lib/armeabi-v7a/libapp.so |
| https://apis.map.qq.com/ws/staticmap/v2/?center=%s&zoom=18&size= | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxim.z.digitalcnzz.com:20013/auth/verify | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxim.z.digitalcnzz.com:20013/auth/password | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxim.z.digitalcnzz.com:20013/office/get\_user\_tags | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxportal.z.digitalcnzz.com:20017/pai/pai-sso/msg/register/checkCode | lib/armeabi-v7a/libapp.so |
| https://api.flutter.dev/flutter/material/Scaffold/of.html | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxportal.z.digitalcnzz.com:20017 | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxim.z.digitalcnzz.com:20013/third/minio\_upload | lib/armeabi-v7a/libapp.so |
| https://github.com/flutter/flutter/issues/new. | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxim.z.digitalcnzz.com:20013/auth/reset\_password | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxim.z.digitalcnzz.com:20013/office/create\_tag | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxim.z.digitalcnzz.com:20013/office/delete\_tag | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxportal.z.digitalcnzz.com:20017/app/register/dept/treeselect | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxim.z.digitalcnzz.com:20013/user/get\_users\_online\_status | lib/armeabi-v7a/libapp.so |
| https://apis.map.qq.com/tools/locpicker?search=1&type=0&backurl= | lib/armeabi-v7a/libapp.so |
| http://maps.google.com/maps | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxportal.z.digitalcnzz.com:20017/api/ztcp/zhsf-person/oauth/pc/queryDutyPersonTypeDetail/ | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxportal.z.digitalcnzz.com:20017/app/register/user | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxim.z.digitalcnzz.com:20013/auth/code | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxportal.z.digitalcnzz.com:20017/app/register/dept/add | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxim.z.digitalcnzz.com:20013/group/invite\_user\_to\_group | lib/armeabi-v7a/libapp.so |
| http://callback | lib/armeabi-v7a/libapp.so |
| https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android. | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxportal.z.digitalcnzz.com:20017/app/api/checkversion | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxportal.z.digitalcnzz.com:20017/app/register/default/topMessage | lib/armeabi-v7a/libapp.so |
| https://yjj-zzszfxportal.z.digitalcnzz.com:20017/api/ztcp/zhsf-person/oauth/pc/queryDutyPersonType | lib/armeabi-v7a/libapp.so |
| https://crbug.com/1053756 | lib/armeabi-v7a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time | lib/armeabi-v7a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time | lib/armeabi-v7a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-content-type | lib/armeabi-v7a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-timing | lib/armeabi-v7a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor-00 | lib/armeabi-v7a/libjingle\_peerconnection\_so.so |
| https://aomediacodec.github.io/av1-rtp-spec/#dependency-descriptor-rtp-header-extension | lib/armeabi-v7a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-layers-allocation00 | lib/armeabi-v7a/libjingle\_peerconnection\_so.so |
| http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01 | lib/armeabi-v7a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/transport-wide-cc-02 | lib/armeabi-v7a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/playout-delay | lib/armeabi-v7a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/color-space | lib/armeabi-v7a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-frame-tracking-id | lib/armeabi-v7a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/inband-cn | lib/armeabi-v7a/libjingle\_peerconnection\_so.so |
| https://www.w3.org/Style/CSS/Test/Fonts/Ahem/). | lib/x86\_64/libflutter.so |
| https://github.com/flutter/flutter/issues. | lib/x86\_64/libflutter.so |
| http://www.w3.org/XML/1998/namespace | lib/x86\_64/libflutter.so |
| http://www.w3.org/2000/xmlns/ | lib/x86\_64/libflutter.so |
| https://crbug.com/1053756 | lib/x86\_64/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time | lib/x86\_64/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time | lib/x86\_64/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-content-type | lib/x86\_64/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-timing | lib/x86\_64/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor-00 | lib/x86\_64/libjingle\_peerconnection\_so.so |
| https://aomediacodec.github.io/av1-rtp-spec/#dependency-descriptor-rtp-header-extension | lib/x86\_64/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-layers-allocation00 | lib/x86\_64/libjingle\_peerconnection\_so.so |
| http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01 | lib/x86\_64/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/transport-wide-cc-02 | lib/x86\_64/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/playout-delay | lib/x86\_64/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/color-space | lib/x86\_64/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-frame-tracking-id | lib/x86\_64/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/inband-cn | lib/x86\_64/libjingle\_peerconnection\_so.so |
| https://crbug.com/1053756 | lib/x86/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time | lib/x86/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time | lib/x86/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-content-type | lib/x86/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-timing | lib/x86/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor-00 | lib/x86/libjingle\_peerconnection\_so.so |
| https://aomediacodec.github.io/av1-rtp-spec/#dependency-descriptor-rtp-header-extension | lib/x86/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-layers-allocation00 | lib/x86/libjingle\_peerconnection\_so.so |
| http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01 | lib/x86/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/transport-wide-cc-02 | lib/x86/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/playout-delay | lib/x86/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/color-space | lib/x86/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-frame-tracking-id | lib/x86/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/inband-cn | lib/x86/libjingle\_peerconnection\_so.so |
| http://www.w3.org/XML/1998/namespace | lib/arm64-v8a/libflutter.so |
| http://www.w3.org/2000/xmlns/ | lib/arm64-v8a/libflutter.so |
| https://www.w3.org/Style/CSS/Test/Fonts/Ahem/). | lib/arm64-v8a/libflutter.so |
| https://github.com/flutter/flutter/issues. | lib/arm64-v8a/libflutter.so |
| https://crbug.com/1053756 | lib/arm64-v8a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time | lib/arm64-v8a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time | lib/arm64-v8a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-content-type | lib/arm64-v8a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-timing | lib/arm64-v8a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor-00 | lib/arm64-v8a/libjingle\_peerconnection\_so.so |
| https://aomediacodec.github.io/av1-rtp-spec/#dependency-descriptor-rtp-header-extension | lib/arm64-v8a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-layers-allocation00 | lib/arm64-v8a/libjingle\_peerconnection\_so.so |
| http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01 | lib/arm64-v8a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/transport-wide-cc-02 | lib/arm64-v8a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/playout-delay | lib/arm64-v8a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/color-space | lib/arm64-v8a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-frame-tracking-id | lib/arm64-v8a/libjingle\_peerconnection\_so.so |
| http://www.webrtc.org/experiments/rtp-hdrext/inband-cn | lib/arm64-v8a/libjingle\_peerconnection\_so.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| \_httpparser@13463476.responsepa  storationinformation@922124995.fromserial  x\_internetaddress@14069316.fixed  .\_future@4048458.immediate  \_growablelist@0150898.\_literal  \_link@14069316.fromrawpat  c\_growablelist@0150898.withcapaci  \_receiveportimpl@1026248.fromrawrec  m\_growablelist@0150898.\_literal2  g\_bigintimpl@0150898.from  \_list@0150898.empty  \_directory@14069316.fromrawpat  r\_growablelist@0150898.empty  \_colorfilter@16065589.srgbtoline  q\_imagefilter@16065589.blur  \_growablelist@0150898.\_literal4  x\_growablelist@0150898.of  3\_list@0150898.\_ofimmutab  k\_colorfilter@16065589.lineartosr  \_list@0150898.of  \_list@0150898.generate  n\_typeerror@0150898.\_create  lectiontoolbarbutton@543392285.text  \_list@0150898.\_ofgrowabl  \_list@0150898.\_ofefficie  \_socket@14069316.\_readpipe  \_list@0150898.\_ofother  eo\_bytebuffer@7027147.\_new  av\_nativesocket@14069316.normal  j\_filestream@14069316.forstdin  qd\_growablelist@0150898.\_literal8  \_future@4048458.zonevalue  \_double@0150898.fromintege  \_growablelist@0150898.\_literal6  z\_timer@1026248.periodic  \_casterror@0150898.\_create  l\_invocationmirror@0150898.\_withtype  \_colorfilter@16065589.mode  i\_rawsocket@14069316.\_writepipe  \_growablelist@0150898.\_literal1  4\_uri@0150898.file  bb\_growablelist@0150898.\_ofgrowabl  erflowindicatormixin@827204652.mixin  v\_utf8encoder@9003594.withbuffer  \_nativesocket@14069316.pipe  \_growablelist@0150898.\_ofimmutab  \_cookie@13463476.fromsetcoo  authenticationscheme@13463476.fromstring  \_growablelist@0150898.\_withdata  \_growablelist@0150898.\_literal3  u\_growablelist@0150898.\_ofother  lectiontoolbarbutton@659113492.text  \_list@0150898.\_oflist  \_timer@1026248.\_internal  \_growablelist@0150898.\_literal5  \_rawsocket@14069316.\_readpipe  gz\_routedata@1565504625.ofroute  ngstreamsubscription@4048458.zoned  \_assertionerror@0150898.\_create  \_uri@0150898.directory  v\_file@14069316.fromrawpat  gh\_growablelist@0150898.generate  \_uri@0150898.notsimple  7u\_growablelist@0150898.\_literal7  \_\_growablelist@0150898.\_ofefficie  \_future@4048458.immediatee  m\_growablelist@0150898.\_oflist | lib/armeabi-v7a/libapp.so |
| appro@openssl.org | lib/arm64-v8a/libflutter.so |
| appro@openssl.org | lib/arm64-v8a/libjingle\_peerconnection\_so.so |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17512775099 | f/h/b/c/a.java |
| 13918588195 | lib/armeabi-v7a/libapp.so |
| 18349115126 | lib/armeabi-v7a/libapp.so |
| 18666662412 | lib/armeabi-v7a/libapp.so |

## **5. 签名证书**

**APK is signed v1 signature: True v2 signature: True v3 signature: False Found 1 unique certificates Subject: C=000000, ST=openim, L=openim, O=openim, OU=openim, CN=openim Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2021-10-26 08:47:56+00:00 Valid To: 2046-10-20 08:47:56+00:00 Issuer: C=000000, ST=openim, L=openim, O=openim, OU=openim, CN=openim Serial Number: 0x19e05291 Hash Algorithm: sha256 md5: 05d03bd8459d4a87134eb128e3dab5fd sha1: 57ce8b8feb004052692f721f7ffa52be51def128 sha256: 1f38a82fb3c33be7951fb5d964ef5bd9c6c9bfc084ae1e2a8a40a0d1f44ae1fe sha512: 797e3ccaf31be41cfce915486e9027118413d22103ba02737cf0ae37904874a7791ab675fb4508cf7b9edfa6044393cb1e282f99eb133f515fe1afdc2447cc0d PublicKey Algorithm: rsa Bit Size: 2048 Fingerprint: 0b749ba3321060732b29f063fbabeb507e14e7e949653bdabdbd3bd3139c14e2**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "google\_api\_key" : "AIzaSyC\_Bx0ewCxYvM5Qfy7uueBrjTF55ZYur\_Y" |
| "google\_crash\_reporting\_api\_key" : "AIzaSyC\_Bx0ewCxYvM5Qfy7uueBrjTF55ZYur\_Y" |
| "library\_zxingandroidembedded\_author" : "JourneyApps" |
| "library\_zxingandroidembedded\_authorWebsite" : "https://journeyapps.com/" |

## **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.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.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.ACCESS\_MEDIA\_LOCATION | 危险 | 访问的任何地理位置 | 允许应用程序访问的任何地理位置持久保存在用户的共享集合 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.CHANGE\_WIFI\_MULTICAST\_STATE | 正常 | 允许Wi-Fi多播接收 | 允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率 |
| 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.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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS | 正常 |  | 应用程序必须持有的权限才能使用 Settings.ACTION\_REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS。 |
| android.permission.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| 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.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.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\_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\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| 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.ACCESS\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |
| 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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.VIDEO\_CAPTURE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.AUDIO\_CAPTURE | 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.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。 |
| android.permission.BLUETOOTH\_CONNECT | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.USE\_FULL\_SCREEN\_INTENT | 正常 |  | 针对想要使用通知全屏意图的 Build.VERSION\_CODES.Q 的应用程序是必需的 |
| android.permission.SCHEDULE\_EXACT\_ALARM | 正常 |  | 允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| 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。 |
| io.zzsf.app.enterprisechat.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| io.zzsf.app.enterprisechat.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| io.zzsf.app.enterprisechat.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| com.meizu.flyme.permission.PUSH | 未知 | Unknown permission | Unknown permission from android reference |
| com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.heytap.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.sec.android.provider.badge.permission.READ | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sec.android.provider.badge.permission.WRITE | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.UPDATE\_SHORTCUT | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonyericsson.home.permission.BROADCAST\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonymobile.home.permission.PROVIDER\_INSERT\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.anddoes.launcher.permission.UPDATE\_COUNT | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或徽章 |
| com.majeur.launcher.permission.UPDATE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或标记为固体。 |
| com.huawei.android.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章 |
| com.huawei.android.launcher.permission.WRITE\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章 |
| android.permission.READ\_APP\_BADGE | 正常 | 显示应用程序通知 | 允许应用程序显示应用程序图标徽章 |
| com.oppo.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| com.oppo.launcher.permission.WRITE\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| me.everything.badger.permission.BADGE\_COUNT\_READ | 未知 | Unknown permission | Unknown permission from android reference |
| me.everything.badger.permission.BADGE\_COUNT\_WRITE | 未知 | Unknown permission | Unknown permission from android reference |
| io.zzsf.app.enterprisechat.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| com.huawei.appmarket.service.commondata.permission.GET\_COMMON\_DATA | 未知 | Unknown permission | Unknown permission from android reference |

## **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。**