



MoGua

云客服 1.0.0.APK 分析报告



APP名称:

云客服

包名:	a1qql.eqwnw.fc26v
域名线索:	15条
URL线索:	8条
邮箱线索:	7条
分析日期:	2025年8月8日
分析平台:	摸瓜APK反编译平台

文件名: Yunkf9171 (1).apk
文件大小: 43.32MB
MD5值: 923c8a604389a5258074d6f1049e9be4
SHA1值: 986f72d6b9c71dad50773a6b312f55935abc30c
SHA256值: 6fb50693a7ae10f2cae28a545da3be24c75fdefd04c957f7c519218b6540bdc9

i APP 信息

App名称: 云客服
包名: a1qql.eqwnw.fc6v
主活动Activity: io.livekit.example.MainActivity
安卓版本名称: 1.0.0
安卓版本: 3

🔍 域名线索

域名	服务器信息
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
dartbug.com	IP: 216.239.32.21 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.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
www.w3.org	IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
crbug.com	IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
webrtc.googlesource.com	IP: 74.125.197.82 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
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

www.ietf.org	IP: 104.16.44.99 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
yunkefu.org	IP: 172.66.43.104 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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
fonts.gstatic.com	IP: 203.208.39.194 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
aomediacodec.github.io	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
www.webrtc.org	IP: 142.251.33.110 所属国家: Canada 地区: Ontario 城市: Toronto 纬度: 43.653660

	经度: -79.382927
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

 URL线索

URL信息	Url所在文件
http://yunkefu.org/	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so
https://developer.mozilla.org/en-US/docs/Web/HTTP/Status	lib/armeabi-v7a/libapp.so
https://docs.flutter.dev/development/data-and-backend/networking	lib/armeabi-v7a/libapp.so
https://aomediacodec.github.io/av1-rtp-spec/	lib/armeabi-v7a/libapp.so
https://github.com/material-foundation/flutter-packages/blob/main/packages/google_fonts/example/test	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.	lib/armeabi-v7a/libapp.so
https://fonts.gstatic.com/s/a/	lib/armeabi-v7a/libapp.so
https://crbug.com/1053756	lib/armeabi-v7a/libjingle_peerconnection_so.so
https://webrtc.googlesource.com/src/+/refs/heads/main/docs/native-code/rtp-hdrex/playout-delay/	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/generic-frame-descriptor-00	lib/armeabi-v7a/libjingle_peerconnection_so.so
https://aomediacodec.github.io/av1-rtp-spec/	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/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
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
https://crbug.com/1053756	lib/x86/libjingle_peerconnection_so.so

https://webrtc.googlesource.com/src/+refs/heads/main/docs/native-code/rtp-hdrex/playout-delay/ ,	lib/x86/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrex/abs-send-time	lib/x86/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrex/generic-frame-descriptor-00	lib/x86/libjingle_peerconnection_so.so
https://aomediacodec.github.io/av1-rtp-spec/	lib/x86/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrex/abs-capture-time	lib/x86/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrex/video-content-type	lib/x86/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrex/video-timing	lib/x86/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrex/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-hdrex/transport-wide-cc-02	lib/x86/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrex/playout-delay	lib/x86/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrex/color-space	lib/x86/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrex/video-frame-tracking-id	lib/x86/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrex/inband-cn	lib/x86/libjingle_peerconnection_so.so
https://crbug.com/1053756	lib/x86_64/libjingle_peerconnection_so.so
https://webrtc.googlesource.com/src/+refs/heads/main/docs/native-code/rtp-hdrex/playout-delay/ ,	lib/x86_64/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrex/abs-send-time	lib/x86_64/libjingle_peerconnection_so.so

http://www.webrtc.org/experiments/rtp-hdrex/generic-frame-descriptor-00	lib/x86_64/libjingle_peerconnection_so.so
https://aomediacodec.github.io/av1-rtp-spec/	lib/x86_64/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrex/abs-capture-time	lib/x86_64/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrex/video-content-type	lib/x86_64/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrex/video-timing	lib/x86_64/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrex/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-hdrex/transport-wide-cc-02	lib/x86_64/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrex/playout-delay	lib/x86_64/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrex/color-space	lib/x86_64/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrex/video-frame-tracking-id	lib/x86_64/libjingle_peerconnection_so.so
http://www.webrtc.org/experiments/rtp-hdrex/inband-cn	lib/x86_64/libjingle_peerconnection_so.so
http://www.unicode.org/copyright.html	lib/x86_64/libflutter.so
https://docs.flutter.dev/release/breaking-changes/android-surface-plugins	lib/x86_64/libflutter.so
https://github.com/flutter/flutter/issues	lib/x86_64/libflutter.so
https://dartbug.com/52121	lib/x86_64/libflutter.so
https://crbug.com/1053756	lib/arm64-v8a/libjingle_peerconnection_so.so
https://webrtc.googlesource.com/src/+refs/heads/main/docs/native-code/rtp-hdrex/playout-delay/ ,	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/generic-frame-descriptor-00	lib/arm64-v8a/libjingle_peerconnection_so.so
https://aomediacodec.github.io/av1-rtp-spec/	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/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
http://www.unicode.org/copyright.html	lib/arm64-v8a/libflutter.so
https://docs.flutter.dev/release/breaking-changes/android-surface-plugins	lib/arm64-v8a/libflutter.so
https://github.com/flutter/flutter/issues	lib/arm64-v8a/libflutter.so
https://dartbug.com/52121	lib/arm64-v8a/libflutter.so

 邮箱线索

邮箱地址	所在文件
authenticationscheme@13463476.fromstring _list@0150898.of _httpparser@13463476.responsepa _list@0150898.generate _typeerror@0150898._create _list@0150898._ofgrowabl _list@0150898._ofefficie _growablelist@0150898._ofarray _double@0150898.fromintege _growablelist@0150898._literal3 _future@4048458.immediate _growablelist@0150898._literal _growablelist@0150898._ofother _link@14069316.fromrawpat _growablelist@0150898.withcapaci _timer@1026248._internal _growablelist@0150898._literal6 _growablelist@0150898._literal5 _receiveportimpl@1026248.fromrawrec _imagefilter@15065589.composed _list@0150898._ofarray storationinformation@251124995.fromserial _timer@1026248.periodic _growablelist@0150898._literal2 _compressednode@34137193.single _list@0150898.empty _list@0150898._ofother _bytebuffer@7027147._new _directory@14069316.fromrawpat _invocationmirror@0150898._withtype ngstreamsubscription@4048458.zoned _assertionerror@0150898._create _nativesocket@14069316.normal _colorfilter@15065589.lineartosr _imagefilter@15065589.fromcolorf	lib/armeabi-v7a/libapp.so

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=admincrfzi9, ST=admincrfzi9, L=admincrfzi9, O=admincrfzi9, OU=admincrfzi9, CN=admincrfzi9
签名算法: rsassa_pkcs1v15
有效期自: 2024-12-15 05:42:49+00:00
有效期至: 2124-11-21 05:42:49+00:00
发行人: C=admincrfzi9, ST=admincrfzi9, L=admincrfzi9, O=admincrfzi9, OU=admincrfzi9, CN=admincrfzi9
序列号: 0x41e8b3ed
哈希算法: sha256
md5值: 8651c3355e839344785eb4e2ebd0c5a8
sha1值: 7c0ade81a1c65dd30ca2e48452a9dd0447344ce4
sha256值: 7a7b5205d45b2edfd6051156cc524c50d02732f956c6995cace955b5eefd64f8
sha512值: 5eb836ab552692a3cc468cffcb3c4a7e6d93f75f82ed3b61b831a6fd1c4384213b79820211a20020dd6fe9380088d7340e86b40ef386718c18a75fb69d68fcbb
公钥算法: rsa
密钥长度: 1024
指纹: 1702703b3fb7c1399e74e51df144508b8ad8667914088c7507741a04dacb2412

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.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_CONNECT	未知	Unknown permission	Unknown permission from android reference
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.FOREGROUND_SERVICE_MEDIA_PROJECTION	未知	Unknown permission	Unknown permission from android reference

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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.ANSWER_PHONE_CALLS	危险		允许应用接听来电。
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.FOREGROUND_SERVICE_MICROPHONE	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	未知	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
a1qql.eqwnw.fc6v.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信