



MoGua

云聊通 1.3.9.APK 分析报告



APP名称:

云聊通

包名:	com.exrpculx.ryeeqx
域名线索:	12条
URL线索:	13条
邮箱线索:	0条
分析日期:	2025年6月20日
分析平台:	摸瓜APK反编译平台

文件名: C617.apk
文件大小: 21.93MB
MD5值: 65bd7ef72043efa0182715bd59904044
SHA1值: f52aeaf448fbd815b222e0088f7fdb2f8506ea43
SHA256值: a3b0d061a0852f26ecb42b7dc7e430c2f708985d5ca166b60973749f52b06994

i APP 信息

App名称: 云聊通
包名: com.exrpculx.ryeeqx
主活动Activity: com.exrpculx.ryeeqx.MainActivity
安卓版本名称: 1.3.9
安卓版本: 2057

🔍 域名线索

域名	服务器信息
schemas.android.com	没有服务器地理信息.
dashif.org	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
aomedia.org	IP: 108.160.166.49 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

ns.adobe.com	没有服务器地理信息.
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
xmlpull.org	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
schemas.microsoft.com	IP: 13.107.253.39 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main 纬度: 50.110882 经度: 8.681996
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
xml.org	IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest 纬度: 29.499678 经度: -98.399246
	IP: 142.251.215.238 所属国家: United States of America 地区: California

developer.android.com	城市: Mountain View 纬度: 37.405991 经度: -122.078514
default.url	没有服务器地理信息.
developer.apple.com	IP: 17.253.87.196 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692

 URL线索

URL信息	Url所在文件
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/g.java
https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted	o3/z.java
https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread	s1/a1.java
https://docs.flutter.dev/deployment/android	p5/d.java
http://xml.org/sax/features/external-general-entities	r1/k.java
http://xml.org/sax/features/external-parameter-entities	r1/k.java
http://xml.org/sax/properties/lexical-handler	r1/k.java
http://xmlpull.org/v1/doc/features.html	r1/k.java

http://schemas.android.com/apk/res/android	x/n.java
http://schemas.android.com/apk/res/android	x4/b.java
http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	w1/o0.java
https://x</LA_URL>	w1/n0.java
https://default.url	w1/n0.java
http://dashif.org/guidelines/last-segment-number	y2/d.java
http://dashif.org/guidelines/trickmode	y2/d.java
http://dashif.org/thumbnail_tile	y2/d.java
http://dashif.org/guidelines/thumbnail_tile	y2/d.java
http://ns.adobe.com/xap/1.0/\u0000	r0/a.java
http://ns.adobe.com/xap/1.0/	c2/a.java
https://aomedia.org/emsg/ID3	m2/a.java
https://developer.apple.com/streaming/emsg-id3	m2/a.java

 邮箱线索

 手机线索

手机号	
-----	--

	所在文件
17179869184	r1/k.java
17179869184	r1/h.java
17512775099	u3/a.java

✿ 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=5PExw, ST=pprdj, L=0wu1C, O=dq1750236505465, OU=co1750236505465, CN=javs
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-18 08:48:26+00:00
有效期至: 2075-06-06 08:48:26+00:00
发行人: C=5PExw, ST=pprdj, L=0wu1C, O=dq1750236505465, OU=co1750236505465, CN=javs
序列号: 0x23872684
哈希算法: sha512
md5值: e3cba9e4e962dac2ed446687b052d438
sha1值: 4a41b4d6f9c608ca4b499190353a1a2acb1be0b7
sha256值: b97bf7ad00b14a8b792b93380e4e016af6e60dd12fa1432e68e71c32b96a0aa6
sha512值: b18d42311a43b456fa97054e9d2b8387e6257d1e2757b70f730f511bf3489fdb3039471ca364562f4bf35b434d4f58747a2a67a307bb077472f4ead00ec41fc5
公钥算法: rsa
密钥长度: 4096
指纹: 3b8d811365bb45665aad360e2f1c4df806a208c8f59217fbf6b2143bbb905a68

🔑 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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

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.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
com.exrpculx.ryeeqx.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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.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

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.exrpculx.ryeeqx.MainActivity	Schemes: 云聊通://,