MoGua

融创数科 5.09.APK 分析报告

APP名称:	融创数科
包名:	cn.rongchuan.com

域名线索:	26条
URL线索:	27条
邮箱线索:	0条
分析日期:	2024年10月18日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: app.apk
文件大小: 15.52MB
MD5值: b28fbbc8efabaf7f307622a1e9917015
SHA1值: f94840f502bea270bde4b8641d47fae16417caa9
SHA256值: b121d83a9d1aecbdfda9fe114a484467cd58e6f384134bc22ba8ad3ee122a0db

APP 信息

App名称: 融创数科
包名: cn.rongchuan.com
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 5.09
安卓版本: 509

域名线索

域名	服务器信息
appclint.hrqt.top	**IP:** 47.121.200.245 **所属国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161583
open.weixin.qq.com	**IP:** 220.196.154.28 **所属国家:** China **地区:** Jiangsu **城市:** Wuxi **纬度:** 31.569349 **经度:** 120.288788
jiaoyisuo666.oss-cn-beijing.aliyuncs.com	**IP:** 61.135.144.152 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397102
gitee.com	**IP:** 180.76.198.77 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397102

api.bspapp.com	**IP**: 39.96.249.142 **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
static-6d65bd90-8508-4d6c-abbc-a4ef5c8e49e7.bspapp.com	**IP**: 39.96.249.142 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
uniapp.dcloud.net.cn	**IP**: 116.196.150.71 **所属国家**: China **地区**: Zhejiang **城市**: Jinhua **纬度**: 30.013470 **经度**: 120.288658
hrqt.top	**IP**: 47.121.200.245 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
vkceyugu.cdn.bspapp.com	**IP**: 124.95.151.235 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
	IP: 116.136.188.184 **所属国家**: China

ask.dcloud.net.cn	**地区**: Nei Mongol **城市**: Hohhot **纬度**: 40.810650 **经度**: 111.650665
apis.map.qq.com	**IP**: 116.130.224.140 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
ns.adobe.com	没有服务器地理信息.
service.dcloud.net.cn	**IP**: 110.40.181.119 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
api.next.bspapp.com	**IP**: 203.107.60.33 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
huifupa.hrqt.top	**IP**: 47.121.200.245 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
www.google.com	**IP**: 199.59.148.96 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
schemas.android.com	没有服务器地理信息.

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
at.alicdn.com	**IP**: 120.220.58.232 **所属国家**: China **地区**: Shandong **城市**: Zibo **纬度**: 36.790775 **经度**: 118.063354
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
quilljs.com	**IP**: 172.66.43.93 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
cdn.pixabay.com	**IP**: 104.18.40.96 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
er.dcloud.net.cn	**IP**: 43.142.57.168 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
	IP: 60.221.17.65 **所属国家**: China

m3w.cn	**地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
er.dcloud.io	没有服务器地理信息.

URL线索

URL信息	Url所在文件
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://er.dcloud.io/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://er.dcloud.net.cn/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/e/b/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/e/b/a.java
https://er.dcloud.io/rv	io/dcloud/e/c/h/c.java
https://er.dcloud.net.cn/rv	io/dcloud/e/c/h/c.java
https://ask.dcloud.net.cn/article/283	io/dcloud/g/b.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java

http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
https://ask.dcloud.net.cn/article/36199	摸瓜V1引擎
https://hrqt.top/xieyi/\	摸瓜V2引擎
https://vkceyugu.cdn.bspapp.com/VKCEYUGU-dc-site/c2b17470-50be-11eb-b680-7980c8a877b8.png	摸瓜V2引擎
https://vkceyugu.cdn.bspapp.com/VKCEYUGU-dc-site/d684ae40-50be-11eb-8ff1-d5dcf8779628.png	摸瓜V2引擎
https://vkceyugu.cdn.bspapp.com/VKCEYUGU-dc-site/e7a79520-50be-11eb-b997-9918a5dda011.png	摸瓜V2引擎
https://vkceyugu.cdn.bspapp.com/VKCEYUGU-dc-site/0dacdbe0-50bf-11eb-8ff1-d5dcf8779628.png	摸瓜V2引擎
https://open.weixin.qq.com/connect/oauth2/authorize?appid=wx946d56ecf8cdda4d&redirect_uri=http%3A%2F%2Fshop.juhejiazhuang.com%2F&response_type=code&scope=snsapi_base&state=	摸瓜V2引擎
https://jiaoyisuo666.oss-cn-beijing.aliyuncs.com/	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://feross.org/opensource>	摸瓜V2引擎
https://api.next.bspapp.com	摸瓜V2引擎
https://api.bspapp.com	摸瓜V2引擎
https://uniapp.dcloud.net.cn/uniCloud/secure-network.html	摸瓜V2引擎
https://uniapp.dcloud.net.cn/uniCloud/faq?id=promise	摸瓜V2引擎
https://appclint.hrqt.top	摸瓜V2引擎
http://feross.org>	摸瓜V2引擎
https://gitee.com/dcloud/uni-app/raw/dev/dist/	摸瓜V2引擎

https://static-6d65bd90-8508-4d6c-abbc-a4ef5c8e49e7.bspapp.com/lime-painter/	摸瓜V2引擎
https://cdn.pixabay.com/photo/2016/11/29/13/24/balloons-1869816__340.jpg	摸瓜V2引擎
https://huifupa.hrqt.top	摸瓜V2引擎
https://appclint.hrqt.top/share/	摸瓜V2引擎
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf)	摸瓜V2引擎
https://service.dcloud.net.cn/uniapp/feedback.html	摸瓜V2引擎
https://apis.map.qq.com/jsapi?qt=translate&type=1&points=	摸瓜V2引擎
https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=	摸瓜V2引擎
https://www.google.com/maps/?daddr=	摸瓜V2引擎
https://www.google.com/maps/	摸瓜V2引擎
https://quilljs.com/	摸瓜V2引擎
https://quilljs.com	摸瓜V2引擎
https://huifupa.hrqt.top	摸瓜V2引擎
https://appclint.hrqt.top	摸瓜V2引擎
https://appclint.hrqt.top/share/	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://huifupa.hrqt.top	摸瓜V2引擎
https://appclint.hrqt.top	摸瓜V2引擎
https://appclint.hrqt.top/share/	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎

邮箱线索

手机线索

手机号	所在文件
15527131853	摸瓜V2引擎
13146116731	摸瓜V2引擎
15488322036	摸瓜V2引擎
19492315001	摸瓜V2引擎
14791934041	摸瓜V2引擎
19441357581	摸瓜V2引擎
16469422263	摸瓜V2引擎
17635154594	摸瓜V2引擎
13004868295	摸瓜V2引擎
13146116731	摸瓜V2引擎
15488322036	摸瓜V2引擎
19492315001	摸瓜V2引擎
14791934041	摸瓜V2引擎
19441357581	摸瓜V2引擎

16469422263	摸瓜V2引擎
17635154594	摸瓜V2引擎
13004868295	摸瓜V2引擎
13146116731	摸瓜V2引擎
15488322036	摸瓜V2引擎
19492315001	摸瓜V2引擎
14791934041	摸瓜V2引擎
19441357581	摸瓜V2引擎
16469422263	摸瓜V2引擎
17635154594	摸瓜V2引擎
13004868295	摸瓜V2引擎

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=CN, O=yourcomname, OU=IT, CN=yourcomname
签名算法: rsassa_pkcs1v15
有效期自: 2024-07-24 08:01:53+00:00
有效期至: 2124-06-30 08:01:53+00:00
发行人: C=CN, O=yourcomname, OU=IT, CN=yourcomname
序列号: 0x4fc02460
哈希算法: sha256
md5值: 3401fa8fc1b3fb2999d6427b149ed89c
sha1值: 1aa22123f9190448fbdf24d3a9541de070f15e45
sha256值: 911599e9311d72eba7f64924b0e25d692e1d192718a2e3ce0fa8c558325050c4

sha512值: f4b387958fad884d7d7b2c98a670ff232f59ae3ea8c850f0021968e51fa97c46bd3504b877000860de3fef0e1c62dc3c8951c5ee5a22305883d4911f1c9a69dc
公钥算法: rsa
密钥长度: 2048
指纹: 5581a75059865fdb2116f975d3559f2631381611b2b60b6cb28b13e227b49f10

🔑 硬编码敏感信息

可能的敏感信息
"dcloud_common_user_refuse_api" : "the user denies access to the API"
"dcloud_io_without_authorization" : "not authorized"
"dcloud_oauth_authentication_failed" : "failed to obtain authorization to log in to the authentication service"
"dcloud_oauth_empower_failed" : "the Authentication Service operation to obtain authorized logon failed"
"dcloud_oauth_logout_tips" : "not logged in or logged out"
"dcloud_oauth_oauth_not_empower" : "oAuth authorization has not been obtained"
"dcloud_oauth_token_failed" : "failed to get token"
"dcloud_permissions_reauthorization" : "reauthorize"
"dcloud_tips_certificate" : "certificate"
"dcloud_common_user_refuse_api" : "用户拒绝该API访问"
"dcloud_io_without_authorization" : "没有获得授权"
"dcloud_oauth_authentication_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_empower_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_logout_tips" : "未登录或登录已注销"

"dcloud_oauth_oauth_not_empower" : "尚未获取oauth授权"
"dcloud_oauth_token_failed" : "获取token失败"
"dcloud_permissions_reauthorization" : "重新授权"
"dcloud_tips_certificate" : "证书"

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.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_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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
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.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
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.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.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_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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
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_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
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。
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference

应用内通信