MoGua

云计算 1.1.677.APK 分析报告

APP名称: 云计算

包名:	yunjisuan0612h5.matainwork.com
域名线索:	14条
URL线索:	25条
邮箱线索:	0条
分析日期:	2025年6月17日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 阿里云计算.apk
文件大小: 7.7MB

MD5值: 975eecdc0bf154344427bf715a328759
SHA1值: 4887b04a4a19991d0cecc4086d08d21ca6d5d80f
SHA256值: 30bbf8ba2d3b6449e9f84d71a3d85655f88f11242b38f48eac8fa41419fff358

APP 信息

App名称: 云计算
包名: yunjisuan0612h5.matainwork.com
主活动Activity: yunjisuan0612h5.matainwork.com.SplashActivity
安卓版本名称: 1.1.677
安卓版本: 1

域名线索

域名	服务器信息
xml.apache.org	**IP:** 151.101.2.132 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203
119.29.29.98	**IP:** 119.29.29.98 **所属国家:** Singapore **地区:** Singapore **城市:** Singapore **纬度:** 1.289987 **经度:** 103.850281
dfai-gx.oss-cn-shenzhen.aliyuncs.com	**IP:** 211.95.146.153 **所属国家:** China **地区:** Sichuan **城市:** Chengdu **纬度:** 30.666670 **经度:** 104.066269

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
yunweb.qgrjgmu.com	IP: 138.113.139.42 **所属国家**: Canada **地区**: Ontario **城市**: North York **纬度**: 43.771862 **经度**: -79.331528
astat.bugly.cros.wr.pvp.net	IP: 170.106.118.26 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418
in2-app.oss-cn-hongkong.aliyuncs.com	IP: 47.79.66.55 **所属国家**: United States of America **地区**: California **城市**: San Mateo **纬度**: 37.547424 **经度**: -122.330589
69.176.85.108	IP: 69.176.85.108 **所属国家**: United States of America **地区**: California **城市**: Aptos **纬度**: 36.992641 **经度**: -121.876740
astat.bugly.qcloud.com	IP: 119.28.121.133 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987

	经度: 103.850281
schemas.android.com	没有服务器地理信息.
h.trace.qq.com	**IP**: 113.56.189.162 **所属国家**: China **地区**: Hubei **城市**: Huangshi **纬度**: 30.204170 **经度**: 115.077606
hk.506download.top	没有服务器地理信息.
android.bugly.qq.com	**IP**: 124.95.225.146 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
119.29.29.99	**IP**: 119.29.29.99 **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://%s/d?%s&alg=des	a/a/a/a/d/p/b/b.java
http://%s/d?%s&alg=aes	a/a/a/a/d/p/a/b.java
https://h.trace.qq.com/kv?attaid=0f500064192&token=4725229671&carrier=	a/a/a/a/e/a.java

http://xml.apache.org/xslt	com/blankj/utilcode/util/LogUtils.java
https://119.29.29.99/conf?token=	com/tencent/msdk/dns/DnsService.java
http://119.29.29.98/conf?id=	com/tencent/msdk/dns/DnsService.java
https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://h.trace.qq.com/kv	com/tencent/bugly/proguard/ad.java
https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/proguard/ac.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/proguard/ac.java
http://69.176.85.108:8088	com/tiocloud/chat/retrofit/Retrofits$retrofit$2.java
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/exceptions/UndeliverableException.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://dfai-gx.oss-cn-shenzhen.aliyuncs.com/idomi.json	yunjisuan0612h5/matainwork/com/SplashActivity.java
https://yunweb.qgrjgmu.com	yunjisuan0612h5/matainwork/com/SplashActivity.java
https://yunweb.qgrjgmu.com	yunjisuan0612h5/matainwork/com/MainActivity.java
https://hk.506download.top/Mata	yunjisuan0612h5/matainwork/com/MainActivity.java
https://in2-app.oss-cn-hongkong.aliyuncs.com/idomi.json	yunjisuan0612h5/matainwork/com/util/FloatCustomServiceButton.java

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: False
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=CN, ST=Beijing, L=Beijing, O=OxuNYgqb, OU=tUksUhXR, CN=DCgZKNUz
签名算法: dsa
有效期自: 2025-06-13 02:36:00+00:00
有效期至: 2028-08-04 02:36:00+00:00
发行人: C=CN, ST=Beijing, L=Beijing, O=OxuNYgqb, OU=tUksUhXR, CN=DCgZKNUz
序列号: 0x565fe421
哈希算法: sha256
md5值: 506f8676a4599d3bbf55fd446e1ad90a
sha1值: 20be3c30a10be3e21e5170aa26337e4030b02a9b
sha256值: d8b8e0e399beba23d6555b7e5f2a4cc3fdeff29af1706d378d7927215157b9cf

sha512值: 989657b4ae37971ddc28706b6e7a72bc94d522d43c7e0f0d954873a67d1113acac486ba466c1253aff8e5a64e8a5d22e5acea5b8ce5c3a93ed182d963c4879e8
公钥算法: dsa
密钥长度: 2048
指纹: ee2f53cabdc4ca757604bec57822d2dbbd10c8981b175c8143fecd1f03619823

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
	危	读取电话状	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

android.permission.READ_PHONE_STATE	险	态和身份	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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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
android.permission.SEND_RESPOND_VIA_MESSAGE	系统需要		允许应用程序（电话）向其他应用程序发送请求以在来电期间处理通过消息响应的操作
android.permission.BROADCAST_SMS	合法	send SMS-received broadcast	允许应用程序广播已收到 SMS 消息的通知。恶意应用程序可能会使用它来伪造传入的 SMS 消息
android.permission.BROADCAST_WAP_PUSH	合法	send WAP-PUSH-received broadcast	允许应用程序广播已收到 WAP-PUSH 消息的通知。恶意应用程序可能会使用它来伪造 MMS 消息接收或用恶意变体悄悄地替换任何网页的内容
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.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.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.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.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
android.permission.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
android.permission.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价
android.permission.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示
android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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.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
	正	防止手机睡	

android.permission.WAKE_LOCK	常	眠	允许应用程序防止手机进入睡眠状态
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.WRITE_SYNC_SETTINGS	正常	写入同步设置	允许应用程序修改同步设置,例如是否为联系人启用同步
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
android.permission.AUTHENTICATE_ACCOUNTS	危险	充当帐户验证器	允许应用程序使用帐户管理器的帐户验证器功能,包括创建帐户以及获取和设置其密码
android.permission.READ_SYNC_SETTINGS	正常	读取同步设置	允许应用程序读取同步设置,例如是否为联系人启用同步
android.permission.USE_BIOMETRIC	正常		允许应用使用设备支持的生物识别模式。
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
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
com.samsung.android.knox.permission.KNOX_REMOTE_CONTROL	未知	Unknown permission	Unknown permission from android reference
com.samsung.android.knox.permission.KNOX_CUSTOM_SYSTEM	未知	Unknown permission	Unknown permission from android reference
	未	Unknown	

com.samsung.android.knox.permission.KNOX_APP_MGMT	知	permission	Unknown permission from android reference
android.permission.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
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.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.EXPAND_STATUS_BAR	正常	展开/折叠状态栏	允许应用程序展开或折叠状态栏
com.android.launcher.permission.UNINSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_CLIPBOARD_IN_BACKGROUND	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.MANAGE_DEVICE_ADMINS	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.ACCESS_NOTIFICATION_POLICY	正常		希望访问通知策略的应用程序的标记权限。
android.permission.CHANGE_CONFIGURATION	系统需	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小

	要		
android.permission.MANAGE_ACTIVITY_STACKS	未知	Unknown permission	Unknown permission from android reference
android.permission.SET_LOCK_TASK_PACKAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.RESET_PASSWORD	未知	Unknown permission	Unknown permission from android reference
android.permission.REBOOT	系统需要	强制手机重启	允许应用强制手机重启
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.MANAGE_MEDIA_PROJECTION	未知	Unknown permission	Unknown permission from android reference
android.permission.CAPTURE_VIDEO_OUTPUT	正常		允许应用程序捕获视频输出
android.permission.CAPTURE_SECURE_VIDEO_OUTPUT	正常		允许应用程序捕获安全视频输出
yunjisuan0612h5.matainwork.com.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信