MoGua

ITSM服务管理平台 1.0.1.APK 分析报告

APP名称: ITSM服务管理平台

包名:	uni.UNI77CF8A6
域名线索:	16条
URL线索:	27条
邮箱线索:	0条
分析日期:	2024年10月16日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: itsm-1.0.1.apk

文件大小: 14.8MB
MD5值: 76c31908ead4f34f0fda6a5fc9e52d7b
SHA1值: f30a303608dbdd493b4b920cc40dbd0914649df0
SHA256值: 4db8e0f91923c62eb3e13c4111836ba9a83ebe4635461525aef876a82bb44286

APP 信息

App名称: ITSM服务管理平台
包名: uni.UNI77CF8A6
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.0.1
安卓版本: 101

域名线索

域名	服务器信息
stream.dcloud.net.cn	**IP**: 49.234.42.40 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com	没有服务器地理信息.
ask.dcloud.net.cn	**IP**: 116.196.150.176 **所属国家**: China **地区**: Zhejiang **城市**: Jinhua **纬度**: 30.013470 **经度**: 120.288658
	IP: 116.130.224.140 **所属国家**: China

apis.map.qq.com	**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.
m3w.cn	**IP**: 221.204.15.62 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
service.dcloud.net.cn	**IP**: 115.159.204.155 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
lame.sf.net	**IP**: 104.18.34.154 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
183.221.218.243	**IP**: 183.221.218.243 **所属国家**: China **地区**: Sichuan **城市**: Ya'an **纬度**: 29.983334 **经度**: 103.016670
schemas.android.com	没有服务器地理信息.
	IP: 104.18.22.19 **所属国家**: United States of America

www.w3.org	**地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
81.68.228.77	**IP**: 81.68.228.77 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
stream.mobihtml5.com	没有服务器地理信息.
www.lebenszeuge.cn	没有服务器地理信息.
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
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

URL线索

URL**信息**	Url**所在文件**
http://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java

https://stream.mobihtml5.com/	io/dcloud/common/constant/StringConst.java
https://stream.dcloud.net.cn/	io/dcloud/common/constant/StringConst.java
http://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/splash-screen/report	io/dcloud/feature/gg/dcloud/ADHandler.java
http://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/g/a/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/g/a/a.java
https://service.dcloud.net.cn/sta/so?p=a&pn=%s&ver=%s&appid=%s	io/dcloud/g/b/c.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/rewarded-video/report?p=a&t=	io/dcloud/g/b/h/a.java
http://ask.dcloud.net.cn/article/283	io/dcloud/i/b.java
http://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://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

http://183.221.218.243:8214	摸瓜V2引擎
http://81.68.228.77	摸瓜V2引擎
https://www.lebenszeuge.cn:447/app/getoperator.php	摸瓜V2引擎
https://apis.map.qq.com/ws/	摸瓜V2引擎
https://quilljs.com/	摸瓜V2引擎
https://quilljs.com	摸瓜V2引擎
https://apis.map.qq.com/ws/';	摸瓜V2引擎
http://lame.sf.net	lib/armeabi-v7a/liblamemp3.so
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libnative-imagetranscoder.so
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libstatic-webp.so
https://crbug.com/v8/8520	lib/armeabi-v7a/libweexjss.so

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: True

v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=CN, ST=, L=, O=Android, OU=Android,
CN=DELEdzpCxGkSJfJGuvCJiKqqb%2BK%2Blod56zxWtqOxIi2F%2BqdJUXhnrVIdHDOSqMjCZ5MHAwX%2B9xb0M8OCwOj5wA%3D%3D
签名算法: rsassa_pkcs1v15
有效期自: 2021-10-04 13:13:07+00:00
有效期至: 2121-09-10 13:13:07+00:00
发行人: C=CN, ST=, L=, O=Android, OU=Android,
CN=DELEdzpCxGkSJfJGuvCJiKqqb%2BK%2Blod56zxWtqOxIi2F%2BqdJUXhnrVIdHDOSqMjCZ5MHAwX%2B9xb0M8OCwOj5wA%3D%3D
序列号: 0x74ab2b13
哈希算法: sha256
md5值: 9a5b70af90c7b70ef6ebd574d59c8cc1
sha1值: d97c221605bc3cb4e6e6801cfcb25b5747dbb148
sha256值: 5099997840cddc68cd50b8d577b2185c0d0289961fa6ffab7acd18a897342de5
sha512值: 56774dce0f6cd862ea80a5e7070d5dcc9be64c1b82ee5e9c83e37027a1ed400366db08be419776ee369d98739533ee67d93222e58c6ffb0ff10d2cfe2ed7b72c
公钥算法: rsa
密钥长度: 2048
指纹: 25ee32b3b3ad2c256401da197056b54211a2eadd2c20922cf0c19e5d37c9006d

🔑 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_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"

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.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.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.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_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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.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.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.WRITE_CONTACTS	危险	写入联系人数据	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据
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。
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown	Unknown permission from android reference

		permission	
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.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
