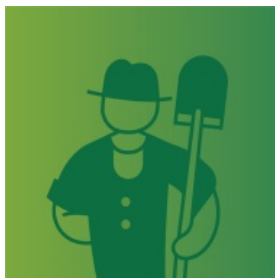




MoGua

SCEA 12.7.30.64114.APK 分析报告



APP名称:

SCEA

包名:	uni.UNI222222
域名线索:	18条
URL线索:	7条
邮箱线索:	2条
分析日期:	2025年6月13日
分析平台:	摸瓜APK反编译平台

文件名: SCEA.apk
文件大小: 17.52MB
MD5值: 4da5470709caf0d775531c24a47a5e82
SHA1值: 0ff9e5cc7a770962e419331d50f47bde8230e5b9
SHA256值: 5fa10ecb8129be2ab1b419142a076b0a80d2dcc3a96259bd4b75966f88509153

i APP 信息

App名称: SCEA
包名: uni.UNI222222
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 12.7.30.64114
安卓版本: 114

🔍 域名线索

域名	服务器信息
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
api.djskdj.shop	IP: 154.38.70.118 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
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
api-origin.shinchanger.shop	IP: 104.21.56.89 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
service.dcloud.net.cn	IP: 110.40.169.99 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
bit.ly	IP: 67.199.248.11 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.750134 经度: -73.997009
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
www.google.com	IP: 31.13.88.169 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
	IP: 172.67.176.210

api-origin.live371.icu	所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
api.fertetoi.shop	IP: 154.38.70.118 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
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
api.dfogakrgm.shop	IP: 154.38.70.117 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
api.shinchanger.shop	IP: 154.38.70.118 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
www.shinchanger.comsitenameu516cu53f8u5b98u7f51	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
ask.dcloud.net.cn	IP: 116.136.188.184 所属国家: China 地区: Nei Mongol 城市: Hohhot 纬度: 40.810650 经度: 111.650665
at.alicdn.com	IP: 101.72.250.130 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
vkceyugu.cdn.bspapp.com	IP: 116.140.34.229 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877

 URL线索

URL信息	Url所在文件
https://ask.dcloud.net.cn/article/36199	摸瓜V1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
http://feross.org >	摸瓜V2引擎
https://api.shinchanger.shop	摸瓜V2引擎
https://api.fertetoi.shop	摸瓜V2引擎
https://api.dfogakrgm.shop	摸瓜V2引擎
https://api.djskdj.shop	摸瓜V2引擎
https://api-origin.shinchanger.shop	摸瓜V2引擎
https://api-origin.live371.icu	摸瓜V2引擎
https://www.shinchanger.com&sitename=\u516c\u53f8\u5b98\u7f51	摸瓜V2引擎
https://bit.ly/2Zqjzkp	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://vkceyugu.cdn.bspapp.com/VKCEYUGU-6bef1fe3-e3e3-4909-9f0c-6ed9bd11c93b/aae2360a-6628-4c93-b873-ce1600b9a852.apk	摸瓜V2引擎
https://feross.org/opensource >	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

 邮箱线索

邮箱地址	所在文件
ic-yjt@3x.png ic-yhk@3x.png ic-wjdd@3x.png group2234@3x.png tp1@3x.png tp-f@3x.png tp-sc@3x.png	摸瓜V2引擎
ic-ywzh@3x.png group2234@3x.png ic-sjh@3x.png ic-yx@3x.png ic-fx@3x.png ic-yl@3x.png ic-gsgw@2x.png ic-fengx2@2x.png ic-cs@3x.png tp-jb@3x.png ic-yjt@3x.png ic-sz@3x.png ic-yx@3x-1.png ic-rw@3x.png ic-gr@3x.png ic-dp@3x.png ic-yhk@3x.png ic-xx@3x.png ic-gth@3x.png ic-jq@3x.png	摸瓜V2引擎

手机线索

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=leiluo, ST=leiluo, L=leiluo, O=leiluo, OU=leiluo, CN=lei
签名算法: rsassa_pkcs1v15
有效期自: 2024-10-10 08:51:35+00:00
有效期至: 2124-09-16 08:51:35+00:00
发行人: C=leiluo, ST=leiluo, L=leiluo, O=leiluo, OU=leiluo, CN=lei
序列号: 0x20080aea
哈希算法: sha256
md5值: 07c4113de786cf40290e83e55585ad1a
sha1值: 700d53096ef162dd91c65b7ecaf13167f3baa168
sha256值: 4819ff641fe57153d3ff00e185735f1a21941c8e20615daa7918f931b7c645a9
sha512值: 681a08dcd8c447a82e5f54fcde286dafbffa4f030b4835c0bd3dec5c306a0f241096359f2b6ee89939e2957699b6434e6b6ebba3fc5fb719ebe27af82e7ea2f5
公钥算法: rsa
密钥长度: 2048
指纹: 1e3ea6bd909e21ec4eb957bd5f06440e3aaf89be4724b64ad974f40f112d5f1a

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.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_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.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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
		Unknown	

android.permission.READ_MEDIA_VIDEO	未知	permission	Unknown permission from android reference
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
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.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
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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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。

应用内通信