MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

华祝软件
HUAZHU SOFTWARE

华祝客户管理 1.0.1.APK

APP名称:	华祝客户管理
包名:	uni.UNIFC20DAF
域名线索:	4条
URL线索:	7条
邮箱线索:	0条
分析日期:	2022年2月2日 20:18

文件信息

文件名: hzkhgl570707.apk
文件大小: 11.29MB
MD5值: 4fee07044c785de77e3811b459289d34
SHA1值: b1ec17831548155b28a9a9407445d70dabdb7126
SHA256值: 5ff0270052c6635915f4f71b702582f43a0d958699e65df9c7880dc9c0351252

APP 信息

App名称: 华祝客户管理
包名: uni.UNIFC20DAF
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	是否危险域名	服务器信息
ask.dcloud.net.cn	good	**IP:** 124.95.157.146 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432777 查看地图: Google Map

域名	是否危险域名	服务器信息
crbug.com	good	**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 **查看地图:** Google Map
lame.sf.net	good	**IP:** 204.68.111.100 **所属国家:** United States of America **地区:** California **城市:** San Diego **纬度:** 32.799797 **经度:** -117.137047 **查看地图:** Google Map
ns.adobe.com	good	没有服务器地理信息.

URL线索

URL信息	Url所在文件
https://ask.dcloud.net.cn/article/36199	Android String Resource
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libstatic-webp.so
https://crbug.com/v8/8520	lib/armeabi-v7a/libweexjss.so
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libnative-imagetranscoder.so

URL信息	Url所在文件
http://lame.sf.net	lib/armeabi-v7a/liblamemp3.so

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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

向手机申请的权限	是否危险	类型	详细情况
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.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_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.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.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_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
getui.permission.GetuiService.uni.UNIFC20DAF	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

向手机申请的权限	是否危险	类型	详细情况
com.asus.msa.SupplementaryDID.ACCESS	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
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
uni.UNIFC20DAF.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
uni.UNIFC20DAF.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
uni.UNIFC20DAF.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=App Gallery, OU=App Gallery, O=Huawei Software Technologies Co., Ltd, C=China
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-12-16 06:38:29+00:00
Valid To: 2051-12-16 06:38:29+00:00
Issuer: CN=App Gallery, OU=App Gallery, O=Huawei Software Technologies Co., Ltd, C=China
Serial Number: 0x1
Hash Algorithm: sha256
md5: 8d4e142a98c4102fd886d9ea6d0196df
sha1: 061686e803d4d4d8d1764b808d10faccf60de4ea
sha256: a45bfd39596bafd052a9a089881e60d72126d0fca9bfd7a863cc9f3fa99d5dbe
sha512: be0a5351d27c5a22e379f511f453cebac7ff9152ee48ce8bd59fff97e984991381438fc35e91324bcb9da86bfad5f3e2b1fd738f6334a0bd1f5fd856a5c0bd29
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 0b91e5e891802c3275e94677154a14f706321b854981f5d0fd52777468fa4a8b

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"

可能的敏感信息
"dcloud_permissions_reauthorization" : "重新授权"

加壳分析

文件列表	分析结果
classes2.dex	<table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>反虚拟机</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check</td></tr><tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr></table>

文件列表	分析结果
classes.dex	<table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>反虚拟机</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check possible Build.SERIAL check SIM operator check network operator name check device ID check subscriber ID check possible VM check</td></tr><tr><td>编译器</td><td>r8</td></tr></table>