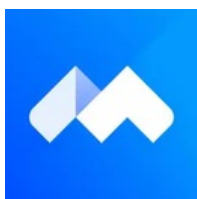




ANDROID 静态分析报告



云会议 · v1.1.8

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

分析日期: 2025-04-02 09:09:38

i应用概览

文件名称	云会议 v1.1.8.apk
文件大小	22.11MB
应用名称	云会议
软件包名	uni.UNI366769E
主活动	io.dcloud.PandoraEntry
版本号	1.1.8
最小SDK	23
目标SDK	28
加固信息	未加壳
开发框架	DCloud, Weex
应用程序安全分数	50/100 (中风险)
杀软检测	3 个杀毒软件报毒
MD5:	0ec5253d6ab2d240d87f4d837cb43087
SHA1:	0b3123e4a6da16deb814c1ed9c149141b8d5cf4c
SHA256:	db67a22b226d86252084c95ffdaa25e77c45e5d5d42a7ed93a9ff585255bf5b2

⚠️ 恶意软件家族信息

恶意家族	CustServRemoteThier_2.0
描述信息	CustServRemoteThier (中文名: 六耳吞金, 灵感源自《西游记》中六耳猕猴伪装孙悟空的典故) 是一款由南明离火平台命名的恶意软件。其2.0版本放弃了基于RustDesk的远程控制技术, 转而采用DCloud平台进行开发, 最早可追溯至2023年。该恶意软件主要通过伪造知名应用程序和冒充客服的方式进行传播, 诱导用户下载并安装。一旦成功侵入受害者设备, 攻击者即可获得远程访问权限, 窃取包括银行资金在内的敏感信息。目前已发现的恶意APP名称包括但不限于: 银联会议、银保会议、银监会议、腾讯会议、专用会议、抖音会议、中银会议、认证会议、在线会议、银万通、云会议、U会议等。
C2服务器	服务器信息通常存储在apk的 assets/apps/{dcloud的APPID}/www/ 目录下的js代码中
凭证数据	升级会员: 解锁高级权限
关联情报	升级会员: 解锁高级权限

🔍 分析结果严重性

🚨 高危	⚠️ 中危	i 信息	✓ 安全	🔍 关注
1	21	1	1	1

四大组件信息

Activity组件: 37个, 其中export的有: 0个
Service组件: 8个, 其中export的有: 0个
Receiver组件: 1个, 其中export的有: 0个
Provider组件: 2个, 其中export的有: 0个

证书信息

二进制文件已签名

v1 签名: True

v2 签名: True

v3 签名: True

v4 签名: False

主题: C=cn, ST=YunNan, L=KunMing, O=ACP, OU=ACP, CN=ACP

签名算法: rsassa_pkcs1v15

有效期自: 2023-09-12 07:59:50+00:00

有效期至: 2078-06-15 07:59:50+00:00

发行人: C=cn, ST=YunNan, L=KunMing, O=ACP, OU=ACP, CN=ACP

序列号: 0x4d6225b467d15829

哈希算法: sha256

证书MD5: 2299259a7278e642e8aec3a887eebe65

证书SHA1: e1ba990a79df6606d4962ed155a92b8406555294

证书SHA256: bf92eedc0331ae23f2f70a988ec76c440ea0b5d84f71284752b4a906fe138f1f

证书SHA512:

91e1f178e895029652240ce4cfc82798f08650b0bc17c77172b5bebc3e82e6cfba51491b4f158cdf575547635435e4e16495fda88918073249f2c936bd36456

公钥算法: rsa

密钥长度: 2048

指纹: e5c6006d71dc3aedb20095d89b772b75270b8b88c5c8669b16759314b0b148cf

找到 1 个唯一证书

应用权限

权限名称	安全等级	权限内容	权限描述
android.permission.INTERNET	危险	完全互联网访问	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	普通	获取网络状态	允许应用程序查看所有网络的状态。
android.permission.ACCESS_WIFI_STATE	普通	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	签名(系统)	请求安装APP	允许应用程序安装全新的或更新的 Android 包。恶意应用程序可能会借此添加其具有任意权限的新应用程序。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。

android.permission.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频, 且允许应用程序收集相机在任何时候拍到的图像。
android.permission.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
android.permission.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
android.permission.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
android.permission.READ_CONTACTS	危险	读取联系人信息	允许应用程序读取您手机上存储的所有联系人(地址)数据。恶意应用程序可借此将您的数据发送给其他人。
android.permission.READ_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况, 这些信息还可能包含用户个人信息或保密信息, 造成隐私数据泄露。
android.permission.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号, 是否正在通话, 以及对方的号码等。
android.permission.VIBRATE	普通	控制振动器	允许应用程序控制振动器, 用于消息通知振动功能。
android.permission.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠, 在手机屏幕关闭后后台进程仍然运行。
android.permission.WRITE_CONTACTS	危险	写入联系人信息	允许应用程序修改您手机上存储的联系人(地址)数据。恶意应用程序可借此清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置方面的数据。恶意应用程序可借此破坏您的系统配置。
android.permission.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置, 如音量。多用于消息语音功能。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户粗略的经纬度信息, 定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息, 定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
com.asus.msa.SupplementalDisplay.ACCESS	普通	获取厂商oaid相关权限	获取设备标识信息oaid, 在华硕设备上需要用到的权限。
android.permission.READ_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
android.permission.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。恶意程序可以接管手机的整个屏幕。

android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground, 用于podcast播放 (推送悬浮播放, 锁屏播放)
android.permission.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。

🔒 网络通信安全

序号	范围	严重级别	描述
----	----	------	----

📄 证书安全分析

高危: 0 | 警告: 1 | 信息: 1

标题	严重程度	描述信息
已签名应用	信息	应用程序使用代码签名证书进行签名

🔍 MANIFEST分析

高危: 1 | 警告: 16 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量, 例如明文HTTP, FTP协议, DownloadManager和MediaPlayer。针对API级别21或更低的应用程序, 默认值为“true”。针对API级别28或更高的应用程序, 默认值为“false”。避免使用明文流量的主要原因是缺乏机密性, 真实性和防篡改保护; 网络攻击者可以窃听传输的数据, 并且可以在不被检测到的情况下修改它。
2	Activity (io.dcloud.PandoraEntry) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时, 其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部, 从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置 taskAffinity (taskAffinity=“”) 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
3	Activity设置了TaskAffinity属性 (io.dcloud.feature.sdk.multi.DCUniMPEntty0)	警告	如果设置了 taskAffinity, 其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息, 请始终使用默认设置, 将 affinity 保持为包名
4	Activity设置了TaskAffinity属性 (io.dcloud.feature.sdk.multi.DCUniMPEntty1)	警告	如果设置了 taskAffinity, 其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息, 请始终使用默认设置, 将 affinity 保持为包名
5	Activity设置了TaskAffinity属性 (io.dcloud.feature.sdk.multi.DCUniMPEntty2)	警告	如果设置了 taskAffinity, 其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息, 请始终使用默认设置, 将 affinity 保持为包名
6	Activity设置了TaskAffinity属性 (io.dcloud.feature.sdk.multi.DCUniMPEntty3)	警告	如果设置了 taskAffinity, 其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息, 请始终使用默认设置, 将 affinity 保持为包名

7	Activity设置了TaskAffinity属性 (io.dcloud.feature.sdk.multi.DCUniMPEntry4)	警告	如果设置了 taskAffinity, 其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息, 请始终使用默认设置, 将 affinity 保持为包名
8	Activity设置了TaskAffinity属性 (io.dcloud.feature.sdk.multi.DCUniMPNoRecentsEntry0)	警告	如果设置了 taskAffinity, 其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息, 请始终使用默认设置, 将 affinity 保持为包名
9	Activity设置了TaskAffinity属性 (io.dcloud.feature.sdk.multi.DCUniMPNoRecentsEntry1)	警告	如果设置了 taskAffinity, 其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息, 请始终使用默认设置, 将 affinity 保持为包名
10	Activity设置了TaskAffinity属性 (io.dcloud.feature.sdk.multi.DCUniMPNoRecentsEntry2)	警告	如果设置了 taskAffinity, 其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息, 请始终使用默认设置, 将 affinity 保持为包名
11	Activity设置了TaskAffinity属性 (io.dcloud.feature.sdk.multi.DCUniMPNoRecentsEntry3)	警告	如果设置了 taskAffinity, 其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息, 请始终使用默认设置, 将 affinity 保持为包名
12	Activity设置了TaskAffinity属性 (io.dcloud.feature.sdk.multi.DCUniMPNoRecentsEntry4)	警告	如果设置了 taskAffinity, 其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息, 请始终使用默认设置, 将 affinity 保持为包名
13	Activity设置了TaskAffinity属性 (io.dcloud.feature.sdk.multi.DCUniMPActivity0)	警告	如果设置了 taskAffinity, 其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息, 请始终使用默认设置, 将 affinity 保持为包名
14	Activity设置了TaskAffinity属性 (io.dcloud.feature.sdk.multi.DCUniMPActivity1)	警告	如果设置了 taskAffinity, 其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息, 请始终使用默认设置, 将 affinity 保持为包名
15	Activity设置了TaskAffinity属性 (io.dcloud.feature.sdk.multi.DCUniMPActivity2)	警告	如果设置了 taskAffinity, 其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息, 请始终使用默认设置, 将 affinity 保持为包名
16	Activity设置了TaskAffinity属性 (io.dcloud.feature.sdk.multi.DCUniMPActivity3)	警告	如果设置了 taskAffinity, 其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息, 请始终使用默认设置, 将 affinity 保持为包名
17	Activity设置了TaskAffinity属性 (io.dcloud.feature.sdk.multi.DCUniMPActivity4)	警告	如果设置了 taskAffinity, 其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息, 请始终使用默认设置, 将 affinity 保持为包名

</> 安全漏洞检测

高危: 0 | 警告: 4 | 信息: 1 | 安全: 0 | 屏蔽: 0

序号	问题	等级	参考标准	文件位置
1	应用程序记录日志信息,不得记录敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MST G-STORAGE-3	升级会员: 解锁高级权限
2	应用程序可以读取/写入外部存储器,任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MST G-STORAGE-2	升级会员: 解锁高级权限
3	文件可能包含硬编码的敏感信息,如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MST G-STORAGE-14	升级会员: 解锁高级权限
4	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MST G-CRYPTO-6	升级会员: 解锁高级权限
5	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MST G-STORAGE-2	升级会员: 解锁高级权限

动态库分析

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	RELRO	RPATH (指定SO搜索路径)	RUNPATH (指定SO搜索路径)	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED (裁剪符号表)
1	armeabi-v7a/liblamemp3.so	True info 二进制文件设置了NX位。这标志着内存页面不可执行,使得攻击者注入的shellcode不可执行。	动态共享对象(DSO) info 共享库是使用-fPIC标志构建的,该标志启用与地址无关的代码。这使得面向返回的编程(NOP)攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值,以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出。	Full RELRO info 此共享对象已完全启用RELRO。RELRO确保GOT不会在易受攻击的ELF二进制文件中被覆盖。在完整RELRO中,整个GOT(.got和.got.plt)两者)被标记为只读。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对glibc的常见不安全函数(如strcpy, gets等)的缓冲区溢出检查。使用编译选项-D_FORTIFY_SOURCE=2来加固函数。这个检查对于Dart/Flutter库不适用。	True info 符号被剥离

2	armeabi-v7a/libstatic-webp.so	True info 二进制文件设置了NX位。这标志着内存页面不可执行,使得攻击者注入的shellcode不可执行。	动态共享对象(DSO) info 共享库是使用-fPIC标志构建的,该标志启用与地址无关的代码。这使得面向返回的编程(ROP)攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值,以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用RELRO。RELRO确保GOT不会在易受攻击的ELF二进制文件中被覆盖。在完整RELRO中,整个GOT(.got和.got.plt两者)被标记为只读。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对glibc的常见不安全函数(如strcpy, gets等)的缓冲区溢出检查。使用编译选项-D_FORTIFY_SOURCE=2来加固函数。这个检查对于Dart/Flutter库不适用	True info 符号被剥离
3	armeabi-v7a/libtxsoundtouch.so	True info 二进制文件设置了NX位。这标志着内存页面不可执行,使得攻击者注入的shellcode不可执行。	动态共享对象(DSO) info 共享库是使用-fPIC标志构建的,该标志启用与地址无关的代码。这使得面向返回的编程(ROP)攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值,以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用RELRO。RELRO确保GOT不会在易受攻击的ELF二进制文件中被覆盖。在完整RELRO中,整个GOT(.got和.got.plt两者)被标记为只读。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对glibc的常见不安全函数(如strcpy, gets等)的缓冲区溢出检查。使用编译选项-D_FORTIFY_SOURCE=2来加固函数。这个检查对于Dart/Flutter库不适用	True info 符号被剥离

行为分析

编号	行为	标签	文件
00022	从给定的文件绝对路径打开文件	文件	升级会员: 解锁高级权限
00013	读取文件并将其放入流中	文件	升级会员: 解锁高级权限
00012	读取数据并放入缓冲流	文件	升级会员: 解锁高级权限

00183	获取当前相机参数并更改设置	相机	升级会员: 解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员: 解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员: 解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员: 解锁高级权限
00063	隐式意图 (查看网页、拨打电话等)	控制	升级会员: 解锁高级权限
00051	通过setData隐式意图 (查看网页、拨打电话等)	控制	升级会员: 解锁高级权限
00072	将 HTTP 输入流写入文件	命令 网络 文件	升级会员: 解锁高级权限
00094	连接到 URL 并从中读取数据	命令 网络	升级会员: 解锁高级权限
00108	从给定的 URL 读取输入流	网络 命令	升级会员: 解锁高级权限
00121	创建目录	文件 命令	升级会员: 解锁高级权限
00125	检查给定的文件路径是否存在	文件	升级会员: 解锁高级权限

:::敏感权限分析

类型	匹配	权限
恶意软件常用权限	14/30	android.permission.REQUEST_INSTALL_PACKAGES android.permission.CAMERA android.permission.GET_ACCOUNTS android.permission.READ_CONTACTS android.permission.READ_PHONE_STATE android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.WRITE_CONTACTS android.permission.WRITE_SETTINGS android.permission.RECORD_AUDIO android.permission.MODIFY_AUDIO_SETTINGS android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.SYSTEM_ALERT_WINDOW
其它常用权限	11/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.FLASHLIGHT android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.FOREGROUND_SERVICE android.permission.BLUETOOTH

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

🔍 域名检测

域名	状态	中国境内	位置信息
lame.sf.net	安全	否	IP地址: 104.18.20.237 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.775700 经度: -122.395103 查看: Google 地图
cloud.tencent.com	安全	是	IP地址: 183.131.59.139 国家: 中国 地区: 浙江 城市: 宁波 纬度: 29.878410 经度: 121.549767 查看: 高德地图

🌐 URL链接分析

URL信息	源码文件
<ul style="list-style-type: none"> https://service.dcloud.net.cn/uniapp/feedback.html http://ios.iefdr4.xyz:5001 http://an1.dnhsy1.xyz:5001/ https://mp-2fe77857-2014-4c91-9329-c62db715e66b.cdn.sspapp.com/xinurl.txt? 	自研引擎-A
<ul style="list-style-type: none"> https://cloud.tencent.com/document/product/269/11673 	op234qwojf/op234qwojf/op234qwojf/a1/op234qwojf/h/a1/a/p.java
<ul style="list-style-type: none"> https://cloud.tencent.com/document/product/269/11673 	op234qwojf/op234qwojf/op234qwojf/x0/op234qwojf/h/v0/a/q.java
<ul style="list-style-type: none"> https://cloud.tencent.com/document/product/269/11673 	op234qwojf/op234qwojf/op234qwojf/y0/op234qwojf/d/d1/a/f.java
<ul style="list-style-type: none"> http://lame.sf.net 	lib/armeabi-v7a/liblamemp3.so

☰ 第三方SDK

SDK名称	开发者	描述信息
MSA SDK	移动安全联盟	移动智能终端补充设备标识体系统一调用 SDK 由中国信息通信研究院泰尔终端实验室、移动安全联盟整合提供, 知识产权归中国信息通信研究院所有。
Fresco	Facebook	Fresco 是一个用于管理图像及其使用的内存的 Android 库。
C++ 共享库	Android	在 Android 应用中运行原生代码。
DCloud	数字天堂	libdeflate is a library for fast, whole-buffer DEFLATE-based compression and decompression.

GIFLIB	GIFLIB	The GIFLIB project maintains the giflib service library, which has been pulling images out of GIFs since 1989. It is deployed everywhere you can think of and some places you probably can't - graphics applications and web browsers on multiple operating systems, game consoles, smartphones, and likely your ATM too.
IJKPlayer	Bilibili	IJKPlayer 是一款基于 FFmpeg 的轻量级 Android/iOS 视频播放器, 具有 API 易于集成、编译配置可裁剪、支持硬件加速解码、DanmakuFlameMaster 架构清晰、简单易用等优势。
腾讯云通信 SDK	Tencent	腾讯云通信基于 QQ 底层 IM 能力开发, 仅需植入 SDK 即可轻松集成聊天、会话、群组、资料管理能力, 帮助您实现文字、图片、短语音、短视频等富媒体消息收发, 全面满足通信需要。
腾讯云短视频 SDK	Tencent	腾讯云点播推出了短视频一站式解决方案, 覆盖了视频生成、上传、处理、分发和播放在内的各个环节, 帮助用户以最快速度实现短视频应用的上线。
android-gif-drawable	koral--	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。
腾讯云实时音视频 SDK	Tencent	实时音视频 (Tencent RTC) 基于腾讯多年来在网络与音视频技术上的深度积累, 以多人音视频通话和低延时互动直播两大场景化方案, 通过腾讯云服务向开发者开放, 致力于帮助开发者快速搭建低成本、低延时、高品质的音视频互动解决方案。
Weex	Alibaba	Weex 致力于使开发者能基于通用跨平台的 Web 开发语言和开发经验, 来构建 Android、iOS 和 Web 应用。简单来说, 在集成了 WeexSDK 之后, 你可以使用 JavaScript 语言和前端开发经验来开发移动应用。
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类, 它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。

🔑 密钥凭证

可能的密钥
DCLLOUD的 "APPID" : "_UNI_366769E"
DCLLOUD的 "DCLLOUD_STREAMAPP_CHANNEL" : "uni.UNI366769E _UNI_366769E 123816220108 "
DCLLOUD的 "AD_ID" : "123816220108"
DCLLOUD的 "ApplicationId" : "uni.UNI366769E"
"dcloud_permissions_reauthorization" : "reauthorize"
e1262d907666861cefb131c67aa59d9ac0cf369bd9126c1f337116e9571b8073

免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成, 内容仅供参考, 不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究, 不得违反中华人民共和国相关法律法规。如有任何疑问, 请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架。它能够执行静态分析和动态分析, 深入扫描软件中中潜在的漏洞和安全隐患。

© 2025 南明离火 - 移动安全分析平台自动生成