



ANDROID 静态分析报告



• v1.1

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: 2025-04-08 20:20:49

i应用概览

文件名称:	oo.apk
文件大小:	13.3MB
应用名称:	
软件包名:	com.service.forcall2
主活动:	com.service.forcall2.activity.MainMyActivity31
版本号:	1.1
最小SDK:	19
目标SDK:	19
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	49/100 (中风险)
杀软检测:	20 个杀毒软件报毒
MD5:	ed7463ff2c9a1b8ede1151928ea7c869
SHA1:	f3458751a660b88276b334bc82ca7457f0b7472a
SHA256:	c2b2e55cfc9d924e976554fa5a58e659088215da38256898966d7f3507ea23ec

📊 分析结果严重性分布

🚨 高危	⚠️ 中危	i 信息	✓ 安全	🔍 关注
3	7	1	2	0

📊 四大组件导出状态统计

Activity组件: 5个, 其中export的有: 1个
Service组件: 11个, 其中export的有: 10个
Receiver组件: 1个, 其中export的有: 1个
Provider组件: 1个, 其中export的有: 0个

🌟 应用签名证书信息

二进制文件已签名

v1 签名: True
 v2 签名: False
 v3 签名: False
 v4 签名: False
 主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
 签名算法: rsassa_pkcs1v15
 有效期自: 2008-02-29 01:33:46+00:00
 有效期至: 2035-07-17 01:33:46+00:00
 发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
 序列号: 0x936eacbe07f201df
 哈希算法: sha1
 证书MD5: e89b158e4bcf988ebd09eb83f5378e87
 证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
 证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
 证书SHA512:
 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccb6b34ec4233f5f640703581053abfea303977272d17959704d89b7711292a4569

找到 1 个唯一证书

权限声明与风险分级

权限名称	安全等级	权限内容	权限描述
android.permission.ANSWER_PHONE_CALLS	危险	允许应用程序接听来电	一个用于以编程方式应答来电的运行时代码。
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.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
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.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.PROCESS_OUTGOING_CALLS	危险	拦截外拨电话	允许应用程序处理外拨电话或更改要拨打的号码。恶意应用程序可能会借此监视、另行转接甚至阻止外拨电话。
android.permission.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
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.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_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.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.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.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录
android.permission.READ_PRIVILEGED_PHONE_STATE	签名(系统)	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.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.WRITE_CALL_LOG	危险	写入通话记录	允许应用程序写入（但不读取）用户的通话记录数据。
android.permission.READ_CONTACTS	危险	读取联系人信息	允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_SMS	危险	读取短信	允许应用程序读取您的手机或SIM卡中存储的短信。恶意应用程序可借此读取您的机密信息。
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.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.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失，但不被允许拨打紧急电话。
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.FORCE_STOP_PACKAGES	签名	强行停止其他应用程序	允许应用程序强行停止其他应用程序。
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。
android.permission.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
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.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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
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.BATTERY_STATS	普通	修改电池统计	允许对手机电池统计信息进行修改
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.EXPAND_STATUS_BAR	普通	展开/收拢状态栏	允许应用程序展开或折叠状态条。
android.permission.BIND_ACCESSIBILITY_SERVICE	签名	AccessibilityServices 需要进行系统绑定	必须由 AccessibilityService要求，以确保只有系统可以绑定到它。
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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。

android.permission.MODIFY_PHONE_STATE	签名(系统)	修改手机状态	允许应用程序控制设备的电话功能。拥有此权限的应用程序可自行切换网络、打开和关闭无线通信等，而不会通知您。
---------------------------------------	--------	--------	--

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.service.forcall2.activity.BaseCallActivity	Schemes: tel://,

网络通信安全风险分析

高危: 1 | 警告: 0 | 信息: 0 | 安全: 0

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量

证书安全合规分析

高危: 1 | 警告: 0 | 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
应用程序容易受到 Janus 漏洞的影响	高危	应用程序使用 v1 签名方案进行签名，如果仅使用 v1 签名方案进行签名，则在 Android 5.0-8.0 上容易受到 Janus 漏洞的影响。仅使用 v1 和 v2/v3 方案签名的 Android 5.0-7.0 上运行的应用程序也容易受到攻击。

Manifest 配置安全分析

高危: 1 | 警告: 15 | 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27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	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
3	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。
4	Activity (com.service.forcall2.activity.BaseCallActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使它成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
5	Activity (com.service.forcall2.activity.BaseCallActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。

6	Service (com.service.forcall2.service.PhoneCallService) 受权限保护,但是应该检查权限的保护级别。 Permission: android.permission.BIND_INCALL_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序,因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此,应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险,一个恶意应用程序可以请求并获得这个权限,并与该组件交互。如果它被设置为签名,只有使用相同证书签名的应用程序才能获得这个权限。
7	Service (com.service.forcall2.service.UPLoadService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享,因此可被设备上的任何其他应用程序访问。
8	Service (com.service.forcall2.service.RecordService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享,因此可被设备上的任何其他应用程序访问。
9	Broadcast Receiver (com.service.forcall2.receiver.BootStartCast) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享,因此可被设备上的任何其他应用程序访问。
10	Service (com.service.forcall2.service.ProService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享,因此可被设备上的任何其他应用程序访问。
11	Service (com.service.forcall2.service.LiveService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享,因此可被设备上的任何其他应用程序访问。
12	Service (com.service.forcall2.service.MainStartService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享,因此可被设备上的任何其他应用程序访问。
13	Service (com.service.forcall2.service.CameraService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享,因此可被设备上的任何其他应用程序访问。
14	Service (com.service.forcall2.service.StartLocationService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享,因此可被设备上的任何其他应用程序访问。
15	Service (com.service.forcall2.service.BaseMusicService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享,因此可被设备上的任何其他应用程序访问。
16	Service (com.service.forcall2.service.CallService) 受权限保护,但是应该检查权限的保护级别。 Permission: android.permission.BIND_ACCESSIBILITY_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序,因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此,应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险,一个恶意应用程序可以请求并获得这个权限,并与该组件交互。如果它被设置为签名,只有使用相同证书签名的应用程序才能获得这个权限。

17	高优先级的Intent (1000) - {1} 个命中 [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。
----	---	----	--

</> 代码安全漏洞检测

高危: 0 | 警告: 2 | 信息: 1 | 安全: 1 | 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: MSTG-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: MSTG-STORAGE-2	升级会员: 解锁高级权限
3	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当 ('SQL注入') OWASP Top 10: M7: Client Code Quality	升级会员: 解锁高级权限
4	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员: 解锁高级权限

Native 库安全加固检测

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	arm64-v8a/libhelper.so	<p>True info</p> <p>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。</p>	<p>动态共享对象 (DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	<p>No info</p> <p>二进制文件没有设置运行时搜索路径或 RPATH</p>	<p>N info</p> <p>二进制文件没有设置 RUNPATH</p>	<p>True info</p> <p>二进制文件有以下加固函数: ['__strlen_chk', '__vsprintf_chk', '__strcat_chk', '_umask_chk']</p>	<p>True info</p> <p>符号被剥离</p>
2	arm64-v8a/libNodeMediaClient.so	<p>True info</p> <p>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。</p>	<p>动态共享对象 (DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	<p>No info</p> <p>二进制文件没有设置运行时搜索路径或 RPATH</p>	<p>N info</p> <p>二进制文件没有设置 RUNPATH</p>	<p>True info</p> <p>二进制文件有以下加固函数: ['__strlen_chk', '__vsprintf_chk', '__vsnprintf_chk']</p>	<p>True info</p> <p>符号被剥离</p>

应用行为分析

编号	行为	标签	文件
00189	获取短信内容	短信	升级会员：解锁高级权限
00188	获取短信地址	短信	升级会员：解锁高级权限
00011	从 URI 查询数据 (SMS、CALLLOGS)	短信 通话记录 信息收集	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限

00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	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
00202	打电话	控制	升级会员：解锁高级权限
00203	将电话号码放入意图中	控制	升级会员：解锁高级权限
00025	监视要执行的一般操作	反射	升级会员：解锁高级权限
00002	打开相机并拍照	相机	升级会员：解锁高级权限
00001	初始化位图对象并将数据（例如JPEG）压缩为位图对象	相机	升级会员：解锁高级权限
00062	查询WiFi信息和WiFi Mac地址	WiFi 信息收集	升级会员：解锁高级权限
00035	查询已安装的包列表	反射	升级会员：解锁高级权限
00038	查询电话号码	信息收集	升级会员：解锁高级权限
00130	获取当前WiFi信息	WiFi 信息收集	升级会员：解锁高级权限
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
00134	获取当前WiFi IP地址	WiFi 信息收集	升级会员：解锁高级权限
00067	查询IMSI号码	信息收集	升级会员：解锁高级权限
00082	获取当前WiFi MAC地址	信息收集 WiFi	升级会员：解锁高级权限
00102	将手机扬声器设置为打开	命令	升级会员：解锁高级权限
00161	对可访问性节点信息执行可访问性服务操作	无障碍服务	升级会员：解锁高级权限
00159	使用辅助服务执行通过文本获取节点信息的操作	无障碍服务	升级会员：解锁高级权限
00033	查询IMEI号	信息收集	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
00198	初始化录音机并开始录音	录制音视频	升级会员：解锁高级权限

00194	设置音源（MIC）和录制文件格式	录制音视频	升级会员：解锁高级权限
00197	设置音频编码器并初始化录音机	录制音视频	升级会员：解锁高级权限
00196	设置录制文件格式和输出路径	录制音视频文件	升级会员：解锁高级权限
00137	获取设备的最后已知位置	位置信息收集	升级会员：解锁高级权限
00115	获取设备的最后已知位置	信息收集位置	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
00056	修改语音音量	控制	升级会员：解锁高级权限
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00064	监控来电状态	控制	升级会员：解锁高级权限

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	16/30	android.permission.RECORD_AUDIO android.permission.GET_TASKS android.permission.PROCESS_OUTGOING_CALLS android.permission.RECEIVE_BOOT_COMPLETED android.permission.SYSTEM_ALERT_WINDOW android.permission.WAKE_LOCK android.permission.READ_CALL_LOG android.permission.READ_PHONE_STATE android.permission.WRITE_CALL_LOG android.permission.READ_CONTACTS android.permission.READ_SMS android.permission.CALL_PHONE android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.CAMERA android.permission.MODIFY_AUDIO_SETTINGS
其它常用权限	14/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.FORCE_STOP_PACKAGES android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.READ_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE android.permission.BATTERY_STATS android.permission.FLASHLIGHT

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。

🔍 恶意域名威胁检测

域名	状态	中国境内	位置信息
www.videolan.org	安全	否	IP地址: 213.36.253.2 国家: 法国 地区: 法兰西岛 城市: 巴黎 纬度: 48.859077 经度: 2.293486 查看: Google 地图

🌐 URL 链接安全分析

URL信息	源码文件
• 154.212.129.2	com/service/forCall2/service/LiveService.java
• https://www.baidu.com	com/service/forCall2/activity/MainMyActivity31.java
• http://107.148.149.122:3456/	lib/arm64-v8a/libhelper.so
• http://www.videolan.org/x264.html	lib/arm64-v8a/libNodeMediaClient.so

☰ 第三方 SDK 组件分析

SDK名称	开发者	描述信息
Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
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。

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