



ANDROID 静态分析报告



启林 • v1.223

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: 2025-05-19 14:51:48

i应用概览

文件名称:	app.apk
文件大小:	75.22MB
应用名称:	启林
软件包名:	com.geoway.lcs
主活动:	com.geoway.cloudquery_leader.SplashActivity
版本号:	1.223
最小SDK:	23
目标SDK:	28
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	32/100 (高风险)
跟踪器检测:	3/432
杀软检测:	AI评估: 很危险, 请谨慎安装
MD5:	db248b9ed3f2006ac56eca4e17ce3b43
SHA1:	593fa7f57c941a893330141c502ee037b52ed052
SHA256:	38e0f771cf7e0458d151dba531c3b2c2674d75bdf11f8cee2fba671479706459

📊 分析结果严重性分布

🚨 高危	⚠️ 中危	i 信息	✓ 安全	🔍 关注
16	25	3	1	30

📦 四大组件导出状态统计

Activity组件: 64个, 其中export的有: 6个
Service组件: 12个, 其中export的有: 2个
Receiver组件: 4个, 其中export的有: 1个
Provider组件: 7个, 其中export的有: 0个

应用签名证书信息

APK已签名

v1 签名: True

v2 签名: True

v3 签名: False

v4 签名: False

主题: OU=geoway, CN=cloud_survey

签名算法: rsassa_pkcs1v15

有效期自: 2018-02-07 08:08:20+00:00

有效期至: 2043-02-01 08:08:20+00:00

发行人: OU=geoway, CN=cloud_survey

序列号: 0x76396825

哈希算法: sha256

证书MD5: 0a7b929daa3781bd8e9df31e7e6b601f

证书SHA1: 73cd2975a662d976c3666b83d6e8643e466638bf

证书SHA256: 842458b1c2a0919271d823f5ca60814eb71b733491bf16219340a57dd4346215

证书SHA512:

9012b62c9b13f29d1e45bbe5663444f0dbdd4902b4b0e6eb4c4e20116fd6acf1cd732541fb5fdded5fee3ba9b6fa9d52973cc29b9cbb04b0c3fee97956ca73575

公钥算法: rsa

密钥长度: 2048

指纹: 96348a9d649517345c3bf8d1ed4b8eb9734ea4065760af8528936075a594feab

共检测到 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.GET_PACKAGE_SIZE	普通	测量应用程序空间大小	允许一个程序获取任何package占用空间容量。
android.permission.DELETE_CACHE_FILES	签名(系统)	删除缓存文件	允许应用删除缓存文件。
android.permission.BLUETOOTH_CONNECT	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够连接到配对的蓝牙设备。
android.permission.BLUETOOTH_SCAN	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够发现和配对附近的蓝牙设备。
android.permission.BLUETOOTH_ADVERTISE	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够向附近的蓝牙设备进行广告。
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.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.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.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.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_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.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.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_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.CHANGE_CONFIGURATION	危险	改变UI设置	允许应用程序 允许应用程序更改当前配置。例如语言区域或整体的字体大小。
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_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.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.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.ACCESS_LOCATION_EXTRA_COMMANDS	普通	访问定位额外命令	访问额外位置提供程序命令，恶意应用程序可能会使用它来干扰GPS或其他位置源的操作。
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.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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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.GET_TOP_ACTIVITY_INFO	未知	未知权限	来自 android 引用的未知权限。
android.permission.ACCESS_NOTIFICATION_POLICY	普通	标记访问通知策略的权限	对希望访问通知政策的应用程序的标记许可。
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.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。
com.geoway.lcs.permission.MIRUSH_RECEIVE	未知	未知权限	来自 android 引用的未知权限。
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.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.SYSTEM_OVERLAY_WINDOW	未知	未知权限	来自 android 引用的未知权限。
getui.permission.GetuiService.com.geoway.lcs	未知	未知权限	来自 android 引用的未知权限。
com.geoway.cloudquery_leader.permission.MIP_USH_RECEIVE	未知	未知权限	来自 android 引用的未知权限。
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.BROADCAST_STICKY	普通	发送置顶广播	允许应用程序发送顽固广播，这些广播在结束后仍会保留。恶意应用程序可能会借此使手机耗用太多内存，从而降低其速度或稳定性。
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。
com.geoway.lcs.permission.RECEIVE_MSG	未知	未知权限	来自 android 引用的未知权限。
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.ACCESS_GPS	签名(系统)	使用GPS权限	这个权限已经被废弃，不再被系统支持。这个权限曾经用于访问GPS位置，但是现在已经被android.permission.ACCESS_FINE_LOCATION替代。
com.android.launcher.permission.READ_SETTINGS	危险	读取桌面快捷方式	这种权限的作用是允许应用读取桌面快捷方式的设置。
android.permission.SCHEDULE_EXACT_ALARM	普通	精确的闹钟权限	允许应用程序使用准确的警报 API。
com.vivo.notification.permission.BADGE_ICON	普通	桌面图标角标	vivo平台桌面图标角标，接入vivo平台后需要用户手动开启，开启完成后收到新消息时，在已安装的应用桌面图标右上角显示“数字角标”。
com.geoway.lcs.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
com.sec.android.provider.badge.permission.READ	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	普通	在应用程序上显示通知计数	在apex的应用程序启动图标上显示通知计数或徽章。

com.majeur.launcher.permission.UPDATE_BADGE	普通	在应用程序上显示通知计数	在solid的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	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.huawei.android.launcher.permission.READ_SETTINGS	普通	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.huawei.android.launcher.permission.WRITE_SETTINGS	普通	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。
android.permission.READ_APP_BADGE	普通	显示应用程序通知	允许应用程序显示应用程序图标徽章。
com.oppo.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	未知	未知权限	来自 android 引用的未知权限。
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	未知权限	来自 android 引用的未知权限。
com.asus.msa.SupplementaryDID.ACCESS	普通	获取厂商oaid相关权限	获取设备识别信息oaid, 在华硕设备上需要用到权限。
com.asus.permission.READ_SDID_PROVIDER	未知	未知权限	来自 android 引用的未知权限。
freemme.permission.msa	未知	未知权限	来自 android 引用的未知权限。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID, 并且可能会投放广告。
android.permission.REORDER_TASKS	危险	正在运行的应用程序重新排序	允许应用程序将任务移至前端和后台。恶意应用程序可借此强行进入前端, 而不受您的控制。

🔒 网络通信安全风险分析

高危: 4 | 警告: 1 | 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。
2	*	警告	基本配置配置为信任系统证书。
3	*	高危	基本配置配置为绕过证书固定。
4	*	高危	基本配置配置为信任用户安装的证书。
5	*	高危	基本配置配置为绕过证书固定。

证书安全合规分析

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	应用已使用代码签名证书进行签名。

Manifest 配置安全分析

高危: 7 | 警告: 12 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、Media Player 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	应用已配置网络安全策略 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。
3	应用可被调试 [android:debuggable=true]	高危	应用开启了可调试标志，攻击者可轻易附加调试器进行逆向分析，导出堆栈信息或访问调试相关类，极大提升被攻击风险。
4	Activity 设置了 TaskAffinity 属性 (m.geoway.adf.base.wxloginutil.WXEntryActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
5	Activity (m.geoway.adf.base.wxloginutil.WXEntryActivity) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空 (taskAffinity="")，或将应用的 target SDK 版本 (28) 升级至 29 及以上，从平台层面修复该漏洞。
6	Activity (m.geoway.adf.base.wxloginutil.WXEntryActivity) 未受保护 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
7	Activity (com.geoway.cloudquery_leader.MainActivity) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空 (taskAffinity="")，或将应用的 target SDK 版本 (28) 升级至 29 及以上，从平台层面修复该漏洞。
8	Activity (com.geoway.cloudquery_leader.MainActivity) 未受保护 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。

9	Broadcast Receiver (com.g eoway.cloudquery_leader. app.USBReceiver) 未受保 护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享, 因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出, 存在安全风险。
10	Activity 设置了 TaskAffinity 属性 (com.igexin.sdk.GActivity)	警告	设置 taskAffinity 后, 其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露, 建议保持默认 affinity (包名)。
11	Activity (com.igexin.sdk.G Activity) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部, 使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空 (taskAffinity=""), 或将应用的 target SDK 版本 (28) 升级至 29 及以上, 从平台层面修复该漏洞。
12	Activity (com.igexin.sdk.G Activity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出, 未受任何权限保护, 任意应用均可访问。
13	Service (com.igexin.sdk.GS ervice) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出, 未受任何权限保护, 任意应用均可访问。
14	Service (com.netease.niml ib.job.NIMJobService) 受权 限保护, 但应检查权限保护 级别。 Permission: android.permi ssion.BIND_JOB_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous, 恶意应用可申请并与组件交互; 若为 signature, 仅同证书签名应用可访问。
15	Activity (androidx.test.cor e.app.InstrumentationActi vityInvoker\$BootstrapActi vity) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部, 使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空 (taskAffinity=""), 或将应用的 target SDK 版本 (28) 升级至 29 及以上, 从平台层面修复该漏洞。
16	Activity (androidx.test.cor e.app.InstrumentationActi vityInvoker\$BootstrapActi vity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出, 未受任何权限保护, 任意应用均可访问。
17	Activity (androidx.test.cor e.app.InstrumentationActi vityInvoker\$EmptyActivity) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部, 使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空 (taskAffinity=""), 或将应用的 target SDK 版本 (28) 升级至 29 及以上, 从平台层面修复该漏洞。
18	Activity (androidx.test.cor e.app.InstrumentationActi vityInvoker\$EmptyActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出, 未受任何权限保护, 任意应用均可访问。

19	Activity (androidx.test.core.app.InstrumentationActivityInvoker\$EmptyFloatingActivity) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空 (taskAffinity="")，或将应用的 target SDK 版本 (28) 升级至 29 及以上，从平台层面修复该漏洞。
20	Activity (androidx.test.core.app.InstrumentationActivityInvoker\$EmptyFloatingActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。

代码安全漏洞检测

高危: 5 | 警告: 10 | 信息: 3 | 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	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-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: MSTG-STORAGE-14	升级会员; 解锁高级权限
4	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询在不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不当 OWASP Top 10: M7: Client Code Quality	升级会员; 解锁高级权限
5	启用了调试配置。生产版本不能是可调试的	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员; 解锁高级权限
6	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员; 解锁高级权限

7	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
8	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
9	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
10	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
11	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	警告	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限
12	应用程序在加密算法中使用ECB模式。ECB模式是已知的弱模式，因为它对相同的明文块(Plaintext)产生相同的密文	高危	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	升级会员：解锁高级权限
13	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: MSTG-CRYPTO-6	升级会员：解锁高级权限

14	应用程序创建临时文件。敏感信息永远不应该被写入临时文件	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
15	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当 ('跨站脚本') OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
16	应用程序可以写入应用程序目录。敏感信息应加密	信息	CWE: CWE-276: 默认权限不正确 OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
17	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
18	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
19	SSL的不安全实现。信任所有证书或接受自签名证书是一个严重的安全漏洞。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	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/libandroid.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。这使得面向返回的代码(ROP)攻击更难可靠地执行。</p>	<p>False high</p> <p>这个二进制文件没有在栈上添加栈哨兵值。栈哨兵用于检测和防止攻击者覆盖返回地址的一种技术。使用选项-fstack-protector-all来启用栈哨兵。这对于Dart/Flutter库不适用，除非使用了Dart FFI。</p>	<p>Full RELRO info</p> <p>此共享对象已完全启用RELRO。RELRO确保GOT不会在易受攻击的二进制文件中被覆盖。在整个RELRO中，整个GOT(.got和.got.plt两者)被标记为只读。</p>	None info	None info	<p>False warning</p> <p>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。</p>	True info

2	arm64-v8a/libantitrace.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)</p> <p>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>	None info	None info	<p>True info</p> <p>二进制文件有以下加固函数: ['_vsprintf_chk']</p>	True info
3	arm64-v8a/libBeiDouProbe.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)</p> <p>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>	None info	None info	<p>True info</p> <p>二进制文件有以下加固函数: ['_vsprintf_chk', '_memcpy_chk', '_strlen_chk']</p>	True info

4	arm64-v8a/libcmcc_sdk.so	<p>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。</p>	<p>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。</p>	<p>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</p>	<p>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。</p>	None info	None info	<p>True info 二进制文件有以下加固函数: ['_vsprintf_chk', '_strlen_chk', '_memcpy_chk', '_vsprintf_chk', '_strcpy_chk']</p>	True info
5	arm64-v8a/libgda.so	<p>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。</p>	<p>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。</p>	<p>False info 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项 -fstack-protector-all 来启用栈哨兵。这对于 Dart/Flutter 不适用，除非使用了 Dart FFI</p>	<p>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。</p>	None info	None info	<p>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</p>	True info

6	arm64-v8a/libgeos_c.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>False high</p> <p>这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项 -fstack-protector-all 来启用栈哨兵。这对于 Dart/Flutter 库不适用，除非使用了 Dart FFI</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>	None info	None info	<p>False warning</p> <p>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。</p>	True info
7	arm64-v8a/libgeowayXWebView.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>	None info	None info	<p>True info</p> <p>二进制文件有以下加固函数: ['_strlen_chk', '_memmove_chk', '_vsnprintf_chk']</p>	True info

8	arm64-v8a/libgeoway_mobile_sdk.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>	None info	None info	<p>False warning</p> <p>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</p>	True info
9	arm64-v8a/libgrowease.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>	None info	None info	<p>False warning</p> <p>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</p>	True info

10	arm64-v8a/libnrtc_mp4v2.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)</p> <p>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>	None info	None info	<p>False warning</p> <p>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</p>	True info
11	arm64-v8a/libpcre2.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)</p> <p>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>False info</p> <p>这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项 -fstack-protector-all 来启用栈哨兵。这对于 Dart/Flutter 不适用，除非使用了 Dart FFI</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>	None info	None info	<p>False warning</p> <p>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</p>	True info

12	arm64-v8a/libqxinertial.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)</p> <p>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>	None info	None info	<p>False warning</p> <p>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</p>	True info
13	arm64-v8a/libqxrtk_half.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)</p> <p>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>	None info	None info	<p>False warning</p> <p>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</p>	True info

14	arm64-v8a/libqwxz_sdk_core.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)</p> <p>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>	None info	None info	<p>True info</p> <p>二进制文件有以下加固函数: ['_FD_ISSET_chk', '_FD_SET_chk']</p>	True info
15	arm64-v8a/libstdc++_shared.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)</p> <p>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>	None info	None info	<p>True info</p> <p>二进制文件有以下加固函数: ['_FD_ISSET_chk', '_FD_SET_chk']</p>	True info

16	arm64-v8a/libsixents-core-sdk.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>	None	None	<p>True info</p> <p>二进制文件有以下加固函数: ['_vsprintf_chk', '_FD_ISSET_chk', '_strlen_chk', '_memcpy_chk', '_FD_SET_chk', '_strchr_chk']</p>	True info
17	arm64-v8a/libyhmcheckcode.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>	None	None	<p>True info</p> <p>二进制文件有以下加固函数: ['_vsprintf_chk', '_strlen_chk', '_memcpy_chk', '_vsprintf_chk', '_memset_chk', '_strcat_chk', '_strcpy_chk']</p>	True info

18	arm64-v8a/libzprotect.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)</p> <p>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>None info</p> <p>二进制文件没有设置运行时间搜索路径或 RPATH</p>	<p>None info</p> <p>二进制文件没有设置 RUNPATH</p>	<p>False warning</p> <p>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</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
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
00002	打开相机并拍照	相机	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
00195	设置录制文件的输出路径	录制音视频文件	升级会员：解锁高级权限
00199	停止录音并释放录音资源	录制音视频	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
00007	Use absolute path of directory for the output media file path	文件	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

00041	将录制的音频/视频保存到文件	录制音视频	升级会员：解锁高级权限
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00014	将文件读入流并将其放入JSON对象中	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
00005	获取文件的绝对路径并将其放入JSON对象	文件	升级会员：解锁高级权限
00004	获取文件名并将其放入JSON对象	文件 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
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
00015	将缓冲流（数据）放入JSON对象	文件	升级会员：解锁高级权限
00024	Base64解码后写入文件	反射 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
00028	从assets目录中读取文件	文件	升级会员：解锁高级权限
00192	获取短信收件箱中的消息	短信	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
00092	发送广播	命令	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
00147	获取当前位置的时间	信息收集 位置	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
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
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
00009	将游标中的数据放入JSON对象	文件	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
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

00016	获取设备的位置信息并将其放入 JSON 对象	位置 信息收集	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
00033	查询IMEI号	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
00083	查询IMEI号	信息收集 电话服务	升级会员：解锁高级权限
00209	从最新渲染图像中获取像素	信息收集	升级会员：解锁高级权限
00104	检查给定路径是否是目录	文件	升级会员：解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00123	连接到远程服务器后将响应保存为 JSON	网络 命令	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	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
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00153	通过 HTTP 发送二进制数据	http	升级会员：解锁高级权限
00031	检查当前正在运行的应用程序列表	反射 信息收集	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
00102	将手机扬声器设置为打开	命令	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
00075	获取设备的位置	信息收集 位置	升级会员：解锁高级权限
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
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
00131	获取当前GSM的位置并将其放入JSON中	信息收集 位置	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
00042	查询WiFi BSSID及扫描结果	信息收集 WiFi	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
00116	获取当前WiFi MAC地址并放入JSON中	WiFi 信息收集	升级会员：解锁高级权限
00139	获取当前WiFi id	信息收集 WiFi	升级会员：解锁高级权限
00135	获取当前WiFi id并放入JSON中	WiFi 信息收集	升级会员：解锁高级权限
00076	获取当前WiFi信息并放入JSON中	信息收集 WiFi	升级会员：解锁高级权限
00099	获取当前GSM的位置并将其放入JSON中	信息收集 位置	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
00056	修改语音音量	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	13/30	android.permission.READ_PHONE_STATE android.permission.WRITE_CONTACTS android.permission.SYSTEM_ALERT_WINDOW android.permission.WRITE_SETTINGS android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.CAMERA android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.RECORD_AUDIO android.permission.GET_TASKS android.permission.MODIFY_AUDIO_SETTINGS android.permission.REQUEST_INSTALL_PACKAGES

其它常用权限	15/46	android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.INTERNET android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.FLASHLIGHT android.permission.ACCESS_NOTIFICATION_POLICY android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.BROADCAST_STICKY com.google.android.gms.permission.AD_ID android.permission.REORDER_TASKS
--------	-------	---

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
t0.tianditu.gov.cn	安全	是	IP地址: 203.107.54.59 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图
nisportal.10010.com	安全	是	IP地址: 203.107.54.59 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图
gdal.orgtext	安全	否	No Geolocation information available.
cloud.landinspector.org	安全	否	No Geolocation information available.
api.jl1mall.com	安全	是	IP地址: 203.107.54.59 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图

aid.mobileservice.cn	安全	是	IP地址: 115.231.163.68 国家: 中国 地区: 浙江 城市: 嘉兴 纬度: 30.752199 经度: 120.750000 查看: 高德地图
api.geonames.org	安全	否	IP地址: 5.9.41.208 国家: 德国 地区: 萨克森 城市: 法尔肯施泰因 纬度: 50.477852 经度: 12.371562 查看: Google 地图
t6.tianditu.cn	安全	否	No Geolocation information available.
opengis.net	安全	否	IP地址: 66.244.86.70 国家: 美国 地区: 印第安纳州 城市: 布鲁明顿 纬度: 39.220310 经度: -86.468237 查看: Google 地图
where.yahooapis.com	安全	否	No Geolocation information available.
t6.tianditu.com	安全	是	IP地址: 203.107.54.59 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图
guotu.s4.udesk.cn	安全	是	IP地址: 203.107.54.59 国家: 中国 地区: 广东 城市: 广州 纬度: 23.127361 经度: 113.264572 查看: 高德地图
www.tianditu.com	安全	是	IP地址: 117.78.24.38 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图
acs.amazonaws.com	安全	否	No Geolocation information available.

www.safe.com	安全	否	<p>IP地址: 45.77.186.192 国家: 美国 地区: 加利福尼亚 城市: 圣克拉拉 纬度: 37.354111 经度: -121.955490 查看: Google 地图</p>
mt2.google.cn	安全	否	No Geolocation information available.
ditu1.zjzwfw.gov.cn	安全	是	<p>IP地址: 122.228.10.40 国家: 中国 地区: 浙江 城市: 温州 纬度: 27.999420 经度: 120.666817 查看: 高德地图</p>
landcloud.org.cn	安全	是	<p>IP地址: 116.205.71.7 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397402 查看: 高德地图</p>
pds.nasa.gov	安全	否	<p>IP地址: 3.167.212.81 国家: 美国 地区: 加利福尼亚 城市: 洛杉矶 纬度: 34.052570 经度: -118.243904 查看: Google 地图</p>
ogr.maptools.org	安全	否	<p>IP地址: 94.23.4.142 国家: 法国 地区: 上法兰西岛 城市: 鲁拜克斯 纬度: 50.693710 经度: 3.174439 查看: Google 地图</p>
docs.opengeoportal.org	安全	否	<p>IP地址: 85.215.173.101 国家: 德国 地区: 黑森 城市: 美因河畔法兰克福 纬度: 50.110882 经度: 8.681996 查看: Google 地图</p>
beidouprobe.wonca.cn	安全	是	<p>IP地址: 120.26.69.21 国家: 中国 地区: 浙江 城市: 杭州 纬度: 30.293650 经度: 120.161583 查看: 高德地图</p>

www.google.cn	安全	否	<p>IP地址: 52.219.120.120 国家: 美国 地区: 加利福尼亚 城市: 洛杉矶 纬度: 34.052570 经度: -118.243904 查看: Google 地图</p>
api.aiplants.cn	安全	是	<p>IP地址: 103.83.45.234 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图</p>
cloudmade.com	安全	否	No Geolocation information available.
www.amazon.com	安全	否	<p>IP地址: 3.169.253.105 国家: 美国 地区: 加利福尼亚 城市: 洛杉矶 纬度: 34.052570 经度: -118.243904 查看: Google 地图</p>
zxid-m.mobileservice.cn	安全	是	<p>IP地址: 115.231.163.68 国家: 中国 地区: 浙江 城市: 嘉兴 纬度: 30.752199 经度: 120.750000 查看: 高德地图</p>
m.tb.cn	安全	是	<p>IP地址: 203.119.175.235 国家: 中国 地区: 浙江 城市: 杭州 纬度: 30.293650 经度: 120.161583 查看: 高德地图</p>
t3.tianditu.gov.cn	安全	是	<p>IP地址: 49.4.56.30 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图</p>
mobsv3.tianditu.com	安全	否	No Geolocation information available.
webst04.taotona.com	安全	是	<p>IP地址: 221.231.92.232 国家: 中国 地区: 江苏 城市: 盐城 纬度: 33.385559 经度: 120.125282 查看: 高德地图</p>

metadata.google.internal	安全	否	No Geolocation information available.
dev.virtualearth.net	安全	否	IP地址: 13.107.246.71 国家: 美国 地区: 华盛顿 城市: 雷德蒙 纬度: 47.682899 经度: -122.120903 查看: Google 地图
www.garmin.com	安全	否	IP地址: 104.17.148.16 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.75700 经度: -122.395903 查看: Google 地图
s3-us-west-1.amazonaws.com	安全	否	IP地址: 52.219.120.120 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.774929 经度: -122.419418 查看: Google 地图
osgeo.org	安全	否	IP地址: 140.211.15.13 国家: 美国 地区: 俄勒冈 城市: 尤金 纬度: 44.036083 经度: -123.052429 查看: Google 地图
schemas.opengis.net	安全	否	IP地址: 217.154.65.51 国家: 德国 地区: 巴登符腾堡 城市: 卡尔斯鲁厄 纬度: 49.004719 经度: 8.385830 查看: Google 地图
www.opengis.net	安全	否	IP地址: 66.244.86.70 国家: 美国 地区: 印第安纳州 城市: 布鲁明顿 纬度: 39.220310 经度: -86.458237 查看: Google 地图
nominatim.openstreetmap.org	安全	否	IP地址: 140.211.167.100 国家: 美国 地区: 俄勒冈 城市: 尤金 纬度: 44.036083 经度: -123.052429 查看: Google 地图

gdal.org	安全	否	<p>IP地址: 104.16.253.120 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.775700 经度: -122.395203 查看: Google 地图</p>
obs-zxjz-test.obs.cn-north-1.myhuaweicloud.com	安全	是	<p>IP地址: 114.115.192.98 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图</p>
inspire.ec.europa.eu	安全	否	<p>IP地址: 3.168.132.80 国家: 美国 地区: 加利福尼亚 城市: 洛杉矶 纬度: 34.052570 经度: -118.243900 查看: Google 地图</p>
www.geopackage.org	安全	否	<p>IP地址: 185.189.108.153 国家: 美国 地区: 宾夕法尼亚 城市: 加利福尼亚 纬度: 40.065647 经度: -79.891724 查看: Google 地图</p>
www.winimage.com	安全	否	<p>IP地址: 205.251.81.217 国家: 美国 地区: 弗吉尼亚州 城市: 雷斯顿 纬度: 38.956692 经度: -77.342102 查看: Google 地图</p>
console.tianditu.gov.cn	安全	是	<p>IP地址: 116.205.64.44 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图</p>
api.tianditu.gov.cn	安全	是	<p>IP地址: 116.205.64.184 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图</p>

xcx.geoway.com.cn	安全	是	<p>IP地址: 124.70.125.100 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图</p>
t1.tianditu.gov.cn	安全	是	<p>IP地址: 49.4.56.37 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图</p>
dh.ditu.zj.cn	安全	否	<p>IP地址: 208.98.40.204 国家: 美国 地区: 内华达州 城市: 拉斯维加斯 纬度: 36.082401 经度: -115.10109 查看: Google 地图</p>
www.tianditu.cn	安全	是	<p>IP地址: 117.78.24.40 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图</p>
gtdcy-task.obs.cn-north-1.myhuaweicloud.com	安全	是	<p>IP地址: 114.115.192.98 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图</p>
www.landcloud.org.cn	安全	是	<p>IP地址: 116.205.65.5 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图</p>
s.s	安全	否	No Geolocation information available.
mt3.google.cn	安全	否	No Geolocation information available.
download.tianditu.com	安全	否	No Geolocation information available.

herbs.aiplants.cn	安全	是	<p>IP地址: 8.131.71.170 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图</p>
maps1.ynmap.cn	安全	是	<p>IP地址: 94.23.4.142 国家: 中国 地区: 云南 城市: 昆明 纬度: 25.038891 经度: 102.718320 查看: 高德地图</p>
cloud.geoway.com.cn	安全	是	<p>IP地址: 94.23.4.142 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图</p>
t6.tianditu.gov.cn	安全	是	<p>IP地址: 49.4.56.44 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图</p>
api.mapbox.com	安全	否	<p>IP地址: 216.137.39.69 国家: 美国 地区: 加利福尼亚 城市: 洛杉矶 纬度: 34.052570 经度: -118.243904 查看: Google 地图</p>
www.georss.org	安全	否	<p>IP地址: 172.67.152.147 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.775700 经度: -122.395203 查看: Google 地图</p>
www.gaia-gis.it	安全	否	<p>IP地址: 195.231.20.209 国家: 意大利 地区: 托斯卡纳 城市: 阿雷佐 纬度: 43.461441 经度: 11.876960 查看: Google 地图</p>
mobile.tianditu.com	安全	否	No Geolocation information available.

xml.nls.fi	安全	否	<p>IP地址: 195.156.69.167 国家: 芬兰 地区: 新地省 城市: 赫尔辛基 纬度: 60.169521 经度: 24.935450 查看: Google 地图</p>
maps.ynmap.cn	安全	是	<p>IP地址: 182.247.253.70 国家: 中国 地区: 云南 城市: 昆明 纬度: 25.038891 经度: 102.718370 查看: 高德地图</p>
open.mapquestapi.com	安全	否	No Geolocation information available.
mt1.google.cn	安全	否	No Geolocation information available.
mt0.google.cn	安全	否	No Geolocation information available.
t2.tianditu.gov.cn	安全	是	<p>IP地址: 49.4.56.47 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图</p>
www.topografix.com	安全	否	<p>IP地址: 104.209.197.87 国家: 美国 地区: 弗吉尼亚州 城市: 博伊顿 纬度: 36.667641 经度: -78.387497 查看: Google 地图</p>
www.lpi.usra.edu	安全	否	<p>IP地址: 172.67.22.158 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.775700 经度: -122.395203 查看: Google 地图</p>
jg.landcloud.org.cn	安全	是	<p>IP地址: 117.78.24.34 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图</p>

 URL 链接安全分析

URL信息	源码文件
-------	------

<ul style="list-style-type: none"> • https://github.com/zloirock/core-js • https://www.udesk.cn/terms_service.html • https://github.com/adobe-type-tools/cmap-resources • https://mozilla.github.io • http://mozilla.org/MPL/2.0 • https://www.tencent.com/zh-cn/privacy-policy.html • https://netease.im • https://www.getui.com/privacy • https://www.udesk.cn • https://www.tencent.com • https://github.com/zloirock/core-js/blob/v3.21.1/LICENSE • https://www.getui.com • https://bugzilla.mozilla.org/show_bug.cgi?id=706209 • http://mozilla.github.io • https://netease.im/clauses 	<p>自研引擎-A</p>
<ul style="list-style-type: none"> • http://dh.ditu.zj.cn:18005/inverse/getinversegeocoding.json?&detail=1&zoom=11&latlon=%s&customer=2 • http://api.tianditu.gov.cn/geocoder?poststr=%s&type=geocode&tk=%s 	<p>com/geoway/tdtlibrary/util/tdt/TGeoDecode.java</p>
<ul style="list-style-type: none"> • https://s3-us-west-1.amazonaws.com 	<p>com/amazonaws/services/s3/AmazonS3Client.java</p>
<ul style="list-style-type: none"> • http://www.tianditu.com/mobile_url/v223 • http://mobile.tianditu.com/mobileversionandmessage/mobilev.action? • http://mobile.tianditu.com/phoneservice/route.do? • http://t6.tianditu.cn/dataserver? • http://www.tianditu.com/query.shtml • http://download.tianditu.com/download/mobile/layers201.xml • http://www.tianditu.cn/mobile_url/weathercode • http://mobile.tianditu.com/mobileversionandmessage/sendv.action • http://mobile.tianditu.com/mobileservice/bases.action • http://mobsv3.tianditu.com • http://download.tianditu.com/download/mobile/category.xml • http://download.tianditu.com/download/mobile/download_v23.xml 	<p>com/geoway/tdtlibrary/util/tdt/LoadServicesURL.java</p>
<ul style="list-style-type: none"> • https://zxid-m.mobileservice.cn/sdk/channel/report 	<p>com/zx/a/I8b7/o2.java</p>
<ul style="list-style-type: none"> • http://cloud.landinspector.org 	<p>m/geoway/cloud/base/workmate/bean/ShareType.java</p>
<ul style="list-style-type: none"> • http://%s.%s/%s 	<p>com/geoway/cloudquery_leader/configtask/ui/ConfigTaskBaseListMgr.java</p>
<ul style="list-style-type: none"> • https://beidou.phone.woncan.cn/api/index/getephemeris 	<p>com/woncan/device/c.java</p>
<ul style="list-style-type: none"> • http://dev-task.obs.cn-north-1.myhuaweicloud.com/media/a4a00eab-ba23-4af0-ac11-9e6aad465ab/hvl5/20231127.gwz 	<p>m/geoway/cloud/base/configtask/util/GwzTool.java</p>
<ul style="list-style-type: none"> • http://www.opengis.net/gml 	<p>com/vividsolutions/jts/io/gml2/GMLConstants.java</p>
<ul style="list-style-type: none"> • http://api.tianditu.gov.cn/v2/search?tk=%s&poststr={ • http://api.tianditu.gov.cn/v2/search?tk=%s&type=query&poststr={ 	<p>m/geoway/adf/base/TdtDef.java</p>
<ul style="list-style-type: none"> • javascript:device.calldownloadresult 	<p>com/geoway/cloudquery_leader/work/WorkH5UiActivity.java</p>

<ul style="list-style-type: none"> https://m.tb.cn/h.usbfw0p https://m.tb.cn/h.uhnw8an 	com/geoway/cloudquery_leader/location/precise/PreciseDeviceInstructionMgr.java
<ul style="list-style-type: none"> 10.0.0.168 103.0.0.205 9.1.0.225 	com/geoway/cloudquery_leader/app/constant/Common.java
<ul style="list-style-type: none"> https://www.landcloud.org.cn/appcenter/code/ https://www.landcloud.org.cn 	m/geoway/cloud/base/net/interf/ConfigCenterNewInterface.java
<ul style="list-style-type: none"> https://cloud.geoway.com.cn:5443/t/appconfig/findbyregionandproid?region=000001&proid=bl https://cloud.geoway.com.cn:5443/t/app/publish/apkpath?proid= https://cloud.geoway.com.cn:5443 https://cloud.geoway.com.cn:5443/t/app/publish/findupdate?proid= https://cloud.geoway.com.cn:5443/t/appconfig/findbyregionandproid?region= 	m/geoway/cloud/base/net/interf/ConfigCenterInterface.java
<ul style="list-style-type: none"> 192.98.102.21 	m/geoway/cloud/base/net/SurveyLogic.java
<ul style="list-style-type: none"> http://117.78.16.173 http://117.78.16.173/antmap/ai/recone0?transsemantics=1&usefocus=1 	m/geoway/cloud/base/net/OkhttpUtils.java
<ul style="list-style-type: none"> http://acs.amazonaws.com/groups/s3/logdelivery http://acs.amazonaws.com/groups/global/allusers http://acs.amazonaws.com/groups/global/authenticatedusers 	com/amazonaws/services/s3/model/GroupPrinter.java
<ul style="list-style-type: none"> https://zxid-m.mobileservice.cn/sdk/module/getcoremodule 	com/zx/a/I8b7/x.java
<ul style="list-style-type: none"> http://49.4.122.19:8095/landcloudwork/tempurl/geturl.action 	m/geoway/adf/base/net/download/DownloadManager.java
<ul style="list-style-type: none"> www.amazon.com 	com/amazonaws/auth/policy/Principal\$WebIdentityProviders.java
<ul style="list-style-type: none"> http://acs.amazonaws.com/groups/s3/logdelivery http://acs.amazonaws.com/groups/global/allusers http://acs.amazonaws.com/groups/global/authenticatedusers 	com/obs/services/internal/Constants.java
<ul style="list-style-type: none"> https://herbs.aiplants.cn/rest/supply/grasstype https://api.aiplants.cn/third/recognize https://herbs.aiplants.cn/rest/supply/coverage 	com/geoway/cloudquery_leader/net/aiplant/AiPlants.java
<ul style="list-style-type: none"> https://guotts43desk.cn/im_client?web_plugin_id= 	m/geoway/adf/ui/activity/WebIMActivity.java
<ul style="list-style-type: none"> http://169.254.169.254 	com/obs/services/internal/security/EcsSecurityUtils.java
<ul style="list-style-type: none"> https://zxid-m.mobileservice.cn/sdk/uaid/get 	com/zx/a/I8b7/c1.java
<ul style="list-style-type: none"> 127.0.0.1 	com/geoway/cloudquery_leader/util/VirtualApkCheckUtil.java

- http://t6.tianditu.com/dataserver?t=cva_c&x={x}&y={y}&l={z}&tk=%s
- http://t6.tianditu.com/dataserver?t=img_w&x={x}&y={y}&l={z}&tk=%s
- <http://218.84.107.14:8090/ime-cloud/rest/ygyx2022/wmts?tilematrix={z}&layer=yx2020&style=default&tilerow={y}&tilecol={x}&tilematrixset=default028mm&format=image%2fjpeg&service=wmts&version=1.0.0&request=gettile>
- http://t6.tianditu.com/dataserver?t=img_c&x={x}&y={y}&l={z}&tk=de159c76d86ca0a75f2831f61b800d12
- <https://webst04.is.autonavi.com/appmaptile?style=6&x={x}&y={y}&z={z}>
- https://ditu1.zjzwfw.gov.cn/mapserver/data/zjwmap/getdata?x={x}&y={y}&l={zoom}&styleid=tdt_biaozhunyangshi_2017&tilesize=512
- http://t6.tianditu.gov.cn/dataserver?t=vec_w&x={x}&y={y}&l={z}&tk=%s
- http://t6.tianditu.com/dataserver?t=cia_w&x={x}&y={y}&l={z}&tk=%s
- http://t6.tianditu.com/dataserver?t=cva_w&x={x}&y={y}&l={z}&tk=%s
- <https://www.google.cn/maps/vt?lyrs=y&gl=cn&x={x}&y={y}&z={z}>
- https://console.tianditu.gov.cn/mapserver/vmap/tdt2018_mercator/getmap?x={x}&y={y}&l={z}&styleid=imglabel0731&0.19109099846291144&ratio=1&tilesize=512&clientversion=jssdk_bate@%20leaflet%203.0.8
- https://maps.ynmap.cn/services/img/map/3857/2017/wmts?service=wmts&request=gettile&version=1.0.0&layer=tdtynimg100cm2000_2017&style=default&tilematrixset=default&tilematrix={z}&tilerow={y}&tilecol={x}&format=image%252fpng
- http://t6.tianditu.com/dataserver?t=img_c&x={x}&y={y}&l={z}&tk=%s
- http://172.16.67.34:8066/ime-cloud/rest/world_v20/terrain/data?level={zoom}&col={x}&row={y}
- https://gss0.bdstatic.com/5bwhcj7labfu8t_jkk_z1zrvfdw6buu/it/u=x={x};y={y};z={z};v=009;type=sate&fm=46&udt=20200225
- <http://124.128.48.214:6080/arcgis/services/fwzy/sdxzj/mapserver/wmserver?service=wms&version=1.1.1&request=getmap&bbox=%s&srs=epsg:4326&width=%d&height=%d&layers=1,2&styles=&format=image/png&transparent=true>
- <http://10.40.40.246:8091/mapserver/vmap/dltb20211221/getmap?styleid=dltb20211221&x={x}&y={y}&l={z}&tilesize=512&ccc=1>
- http://t6.tianditu.com/dataserver?t=cia_c&x={x}&y={y}&l={z}&tk=%s
- http://222.240.168.21:8093/ime-cloud/rest/pyq_hn30mdem/terrain/data?gk=1539143597801637489899068&level={zoom}&col={x}&row={y}
- http://www.landcloud.org.cn:81/atlas-ime/rest/globe_world_terrain/terrain/data?level={zoom}&col={x}&row={y}
- <https://maps1.ynmap.cn/tileservice/service/maps1ynimgcn/4490/wmts/tile/default/{z}/{y}/{x}?key=cdbeb44a424c48f2b1215f06a4810350>
- <http://218.84.107.14:8061/mapserver/label/wmts/10/ht5003/ht5003?tilematrix={z}&layer=ht5003&style=default&tilerow={y}&tilecol={x}&tilematrixset=default028mm&format=image%2fjpeg&service=wmts&version=1.0.0&request=gettile>
- <https://t1.tianditu.gov.cn/mapserver/swdx?x={x}&y={y}&l={z}&tk=d5d53c86aea82b5978d9992eb50ba4df>
- http://t6.tianditu.com/dataserver?t=vec_c&x={x}&y={y}&l={z}&tk=%s
- https://console.tianditu.gov.cn/mapserver/vmap/tdt2018_mercator/getmap?x={x}&y={y}&l={z}&styleid=mercator_v3_6&0.772546628707314&ratio=2&tilesize=512&clientversion=jssdk_bate@%20leaflet%203.0.8

com/geoway/mobile/TestActivity.java

<ul style="list-style-type: none"> • http://t6.tianditu.com/dataserver?t=cva_c&x={x}&y={y}&l={z}&tk=%s • http://t6.tianditu.com/dataserver?t=img_w&x={x}&y={y}&l={z}&tk=%s • http://218.84.107.14:8090/ime-cloud/rest/ygyx2022/wmts?tilematrix={z}&layer=yx2020&style=default&tilerow={y}&tilecol={x}&tilematrixset=default028mm&format=image%2fjpeg&service=wmts&version=1.0.0&request=gettile • https://webst04.is.autonavi.com/appmaptile?style=6&x={x}&y={y}&z={z} • https://ditu1.zjzfwf.gov.cn/mapserver/data/zjvmap/getdata?x={x}&y={y}&l={zoom}&styleid=tt_biaozhunyangshi_2017&tilesize=512 • http://t6.tianditu.gov.cn/dataserver?t=vec_w&x={x}&y={y}&l={z}&tk=%s • https://api.jl1mall.com/getmap/{z}/{x}/{y}?mk=878ee154cd70417e54f6d07bb18cc3fe&tk=fcd5bd3c17c17a0e00ffc57e45418984c&pro=073bd8195d024c5681338b3d9c4f53ed&sch=wmts • http://t6.tianditu.com/dataserver?t=cia_w&x={x}&y={y}&l={z}&tk=%s • http://t6.tianditu.com/dataserver?t=cva_w&x={x}&y={y}&l={z}&tk=%s • https://www.google.cn/maps/vt?lyrs=y&gl=cn&x={x}&y={y}&z={z} • https://console.tianditu.gov.cn/mapserver/vmap/tdt2018_mercator/getmap?x={x}&y={y}&l={z}&styleid=imglabel0731&0.19109099846291144&ratio=1&tilesize=512&clientversion=jssdk_bate@%20leaflet%203.0.8 • https://maps.ynmap.cn/services/img/map/3857/2017/wmts?service=wmts&request=gettile&version=1.0.0&layer=tdtynimg100cm2000_2017&style=default&tilematrixset=default&tilematrix={z}&tilerow={y}&tilecol={x}&format=image%252fpng • http://t6.tianditu.com/dataserver?t=img_c&x={x}&y={y}&l={z}&tk=%s • http://172.16.67.34:8066/ime-cloud/rest/worlds_20/terrain/data?level={zoom}&col={x}&row={y} • https://gss0.bdstatic.com/5bwhcj7labfu8t_jkk_zjzfwfdu6buu/it/u=x={x};y={y};z={z};v=009;type=sate&fm=46&udt=20200225 • http://124.128.48.214:6080/arcgis/services/nvzy/sdxj/mapserver/wms/server?service=wms&version=1.1.1&request=getmap&bbox=%s&srs=epsg:4326&width=%d&height=%d&layers=1,2&styles=&format=image/png&transparent=true • http://10.40.40.246:8091/mapserver/vmap/dltb20211221/getmap?styleid=dltb20211221&x={x}&y={y}&l={z}&tilesize=512&ccc=1 • http://t6.tianditu.com/dataserver?t=cia_c&x={x}&y={y}&l={z}&tk=%s • http://222.240.168.21:8093/ime-cloud/rest/pyqz/3030/dem/terrain/data?gk=1539143597861837489899068&level={zoom}&col={x}&row={y} • http://www.landcloud.org.cn:81/atlas-ime/rest/globe_world_terrain/terrain/data?level={zoom}&col={x}&row={y} • http://218.84.107.14:8061/mapserver/label/wmts/1.0/ht5003/ht5003?tilematrix={z}&layer=ht5003&style=default&tilerow={y}&tilecol={x}&tilematrixset=default028mm&format=image%2fjpeg&service=wmts&version=1.0.0&request=gettile • https://t1.tianditu.gov.cn/mapservice/swdx?x={x}&y={y}&l={z}&tk=d5d53c86aea82b5978d9992eb50ba4df • http://t6.tianditu.com/dataserver?t=vec_c&x={x}&y={y}&l={z}&tk=%s • https://console.tianditu.gov.cn/mapserver/vmap/tdt2018_mercator/getmap?x={x}&y={y}&l={z}&styleid=mercator_2018_6&0.772548628707314&ratio=2&tilesize=512&clientversion=jssdk_bate@%20leaflet%203.0.8 	<p>com/geoway/mobile/MainActivity.java</p>

<ul style="list-style-type: none"> • javascript:device.callbackresult • javascript:console.error 	m/geoway/xwebview/base/BaseXWebView.java
<ul style="list-style-type: none"> • http://%.%/s 	com/geoway/cloudquery_leader/gallery/quicksnap/QuickSnapMgr.java
<ul style="list-style-type: none"> • https://obs-zxjz-test.obs.cn-north-1.myhuaweicloud.com/taskthrd/9999/a25c8a9f-995c-4ecb-8832-1af60c1b7127.jpg?awsaccesskeyid=efbo6zttbdc339xulkin&expires=1577330434&signature=ot%2b lxabm87nxxz8exl6k6kftmo%3d • https://obs-zxjz-test.obs.cn-north-1.myhuaweicloud.com:443/task/23082b/1114/20191225/20191225-142320-3a44bcd2.db 	geoway/tdtlibrary/MainActivity.java
<ul style="list-style-type: none"> • 192.98.102.21 	com/geoway/cloudquery_leader/LoginActivity.java
<ul style="list-style-type: none"> • http://172.16.67.50:2880/output/earth-1.50/index.htm 	com/geoway/cloudquery_leader/MainActivity.java
<ul style="list-style-type: none"> • https://api.weixin.qq.com/sns/oauth2/access_token?appid= 	m/geoway/cloud/ui/activity/PersonInfoActivityCloud.java
<ul style="list-style-type: none"> • http://api.ditu.zj.cn:8880/bus/getbusrigidity.json?orig=%s&dest=%s&encode=utf-8&city=%s&all=1&walkshow=1&customer=2 • http://api.tianditu.gov.cn/transn?type=%s&poststr=%s&tk=%s 	geoway/tdtlibrary/search/support/SearchRequest.java
<ul style="list-style-type: none"> • http://dh.ditu.zj.cn:8880/search?area= • http://%.%/s/%s/%s/rest/%s/place/search?format=json&page_num=0&page_size=%d&q=%s&sq_type=bounds&bounds=%f,%f,%f,%f • http://api.tianditu.gov.cn/search?type=query&poststr={ 	geoway/tdtlibrary/search/support/PoiSearch.java
<ul style="list-style-type: none"> • http://%.%/s/%s 	m/geoway/cloud/base/gallery/bean/Media.java

<ul style="list-style-type: none"> • http://%s/%s/%s • http://%s.%s/%s 	m/geoway/cloud/base/OSSAndOBS.java
<ul style="list-style-type: none"> • http://%s.%s/%s 	m/geoway/cloud/base/ObsSdk.java
<ul style="list-style-type: none"> • http://49.4.122.19:8095/landcloudwork/tempurl/geturl.action 	m/geoway/adf/base/download/DownloadObsTask.java
<ul style="list-style-type: none"> • http://dh.ditu.zj.cn:8880/route/getdrivebylatlon.json?&orig=%s&dest=%s&width=500&height=430&style=%d&customer=2&encode=utf-8 • http://api.tianditu.gov.cn/drive?poststr=%s&type=search&tk=%s 	geoway/tdtlibrary/bus/TDrivingRoute.java
<ul style="list-style-type: none"> • https://jg.landcloud.org.cn/apk/android-gengdihecha-wrj2.html • https://jg.landcloud.org.cn/apk/android-gengdihecha-wrj.html 	m/geoway/cloud/m/UAUtil.java

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

<ul style="list-style-type: none"> • http://118.253.184.111:8090/service?layer=zny_4326_layer&style=&tilematrixset=w&service=wmts&request=gettile&version=1.0.0&format=webp&tilematrix={z}&tilecol={x}&tilerow={y} • https://t3.tianditu.gov.cn/dataserver?t=cva_c&x={x}&y={y}&l={z}&tk=%s • https://t2.tianditu.gov.cn/dataserver?t=vec_w&x={x}&y={y}&l={z}&tk=%s • http://mt3.google.cn/vt/lyrs=y@126&hl=zh-cn&gl=cn&src=app&s=g&x={x}&y={y}&z={z} • http://mt2.google.cn/vt/lyrs=m@207000000&hl=zh-cn&gl=cn&src=app&x={x}&y={y}&z={z}&s=gale • http://mt2.google.cn/vt/lyrs=y@126&hl=zh-cn&gl=cn&src=app&s=g&x={x}&y={y}&z={z} • http://mt0.google.cn/vt/lyrs=m@207000000&hl=zh-cn&gl=cn&src=app&x={x}&y={y}&z={z}&s=gale • http://mt0.google.cn/vt/lyrs=y@126&hl=zh-cn&gl=cn&src=app&s=g&x={x}&y={y}&z={z} • https://api.jl1mall.com/getmap/{z}/{x}/y?mk=878ee154cd70417e54f6d07bb18cc3fe&tk=6cd3bdc17c17a0e00ffc57e45418984c&pro=ea95d11209614d4bea6bca6dc21f34616&sch=wmts • http://mt1.google.cn/vt/lyrs=y@126&hl=zh-cn&gl=cn&src=app&s=g&x={x}&y={y}&z={z} • https://t3.tianditu.gov.cn/dataserver?t=cva_w&x={x}&y={y}&l={z}&tk=%s • http://mt3.google.cn/vt/lyrs=m@207000000&hl=zh-cn&gl=cn&src=app&x={x}&y={y}&z={z}&s=gale • https://t1.tianditu.gov.cn/dataserver?t=cia_w&x={x}&y={y}&l={z}&tk=%s • https://t2.tianditu.gov.cn/dataserver?t=vec_c&x={x}&y={y}&l={z}&tk=%s • http://49.4.85.64:9017/mapserver/label/osm/getdatas?x={x}&y={y}&l={zoom}&styleid=test&0.029263976091863375&tilesize=512&clientversion=jssdk_bate@%20leaflet%203.0.10 • https://t0.tianditu.gov.cn/dataserver?t=img_w&x={x}&y={y}&l={z}&tk=%s • https://t0.tianditu.gov.cn/dataserver?t=img_c&x={x}&y={y}&l={z}&tk=%s • https://t1.tianditu.gov.cn/dataserver?t=cia_c&x={x}&y={y}&l={z}&tk=%s • https://xcx.geoway.com.cn:18000/ime-cloud/rest/dem30m_xj65/terrain/data?level={z}&col={x}&row={y} • http://mt1.google.cn/vt/lyrs=m@207000000&hl=zh-cn&gl=cn&src=app&x={x}&y={y}&z={z}&s=gale 	<p>m/geoway/cloud/base/def/MapCommon.java</p>
<ul style="list-style-type: none"> • https://pcidprobe.woncan.cn/api/difference/heart • https://pcidprobe.woncan.cn/api/difference/getnew 	<p>com/woncan/device/e.java</p>
<ul style="list-style-type: none"> • https://aid.mobileservice.cn/ 	<p>com/zx/a/I8b7/g2.java</p>

<ul style="list-style-type: none"> • https://nisportal.10010.com:9001 	com/zx/a/i8b7/g1.java
<ul style="list-style-type: none"> • https://beidouprobe.woncan.cn/api/version/get 	com/woncan/device/DeviceManager.java
<ul style="list-style-type: none"> • https://zxid-m.mobileservice.cn/sdk/config/init 	com/zx/a/i8b7/g.java
<ul style="list-style-type: none"> • https://landcloud.org.cn 	自研引擎-S
<ul style="list-style-type: none"> • 120.253.239.161 • 10.73.1.205 • 120.253.226.97 • 117.135.142.201 • 120.253.239.171 	lib/arm64-v8a/libcmtdc_sdk.so
<ul style="list-style-type: none"> • http://osgeo.org/gdal/ • http://www.geopackage.org/spec120/#extension_metadata • http://www.opengis.net/def/crs/ • http://undefined_namespace • http://xml.nls.fi/xml/namespace/maastotietojarjestelma/siirtotiedostonmalli/2011-02 • http://open.mapquestapi.com/nominatim/v1/reverse.php?format=xml&lat={lat}&lon={lon} • http://www.geopackage.org/spec120/#extension_geometry_types • http://inspire.ec.europa.eu/enumeration/elevationpropertytypevalue/height • http://www.geopackage.org/spec121/#extension_schema • https://pds.nasa.gov/pds4/cart/v1/pds4_cart_1700.xsd • https://accounts.google.com/o/oauth2 • http://www.garmin.com/xmlschemas/gpxextensions/v3 • http://www.opengis.net/def/crs/%s/0/%s • http://www.topografix.com/gpx/1/1 • http://www.opengis.net/def/ogc-eo/opt/spectralmode/pandromat • http://www.opengis.net/def/crs • http://www.opengis.net/wmts/1.0 • http://www.topografix.com/gpx/1/1/gpx.xsd • http://www.opengis.net/gmlsf/2.0 • http://schemas.opengis.net/gmlsfprofile/2.0/gmlsflevels.xsd • http://pds.nasa.gov/pds4/pds/v1 • http://osgeo.org/gdal • http://gdal.org', 'text/xml', '%q • http://schemas.opengis.net/kml/2.0/ogckml22.xsd • http://pds.nasa.gov/pds4/cart/v1 • http://api.geonames.org/search?q=%s&style=long • http://ogr.maptools.org/ • http://gdal.org • http://nominatim.openstreetmap.org/search?q=%s&format=xml&polygon_text=1 • http://www.geopackage.org/spec120/#extension_tiles_webp • http://nominatim.openstreetmap.org/reverse?format=xml&lat={lat}&lon={lon} • http://where.yahooapis.com/geocode?q={lat},{lon}&gflags=r • http://www.opengis.net/def/crs/epsg/0/5714 • http://api.geonames.org/findnearby?lat={lat}&lng={lon}&style=long • http://cloudmade.com/ • http://www.opengis.net/gml • http://metadata.google.internal/computemetadata/v1/instance/service-accounts/default/token • http://www.opengis.net/gmlsf • http://www.geonames.org/georss • http://www.geopackage.org/spec120/#extension_zoom_other_intervals • https://www.gaia-gis.it/fossil/libspatialite/wiki?name=shadowed+rowid+issues • http://schemas.opengis.net/gml/3.1.1/profiles/gmlsfprofile/1.0.0/gmlsflevels.xsd • http://www.opengis.net/kml/2.2 • http://www.opengis.net/def/ogc-eo/opt/spectralmode/color • http://docs.opengeospatial.org/is/17-066r1/17-066r1.html 	lib/arm64-v8a/libgdal.so

<ul style="list-style-type: none"> • http://where.yahooapis.com/geocode?q=%s • http://ogr.maptools.org/%d • http://dev.virtualearth.net/rest/v1/locations?q=%s&o=xml • http://www.geopackage.org/spec120/#extension_crs_wkt • http://schemas.opengis.net/gml/3.1.1/base/gml.xsd • https://github.com/ • http://www.geopackage.org/spec120/#extension_rtree • http://opengis.net/def/crs • https://accounts.google.com/o/oauth2/token • http://gdal.org • http://www.opengis.net/def/crs/epsg/0/%d • http://www.opengis.net/gml/3.2 • http://open.mapquestapi.com/nominatim/v1/search.php?q=%s&format=xml • http://schemas.opengis.net/gml/3.2.1/gml.xsd • http://gdal.org/geopackage_aspatial.html • http://www.lpi.usra.edu/meetings/lpsc2014/pdf/1088.pdf • http://ogr.maptools.org/ • http://schemas.opengis.net/gml/2.1.2/feature.xsd • http://schemas.opengis.net/gml/3.1.1/profiles/gmlsfprofile/1.0.0/gmlsf.xsd • http://www.opengis.net/gml/srs/epsg.xml# • http://www.opengis.net/wfs • http://www.safe.com/gml/fme • http://dev.virtualearth.net/rest/v1/locations/{lat},{lon}?includeentitytypes=countryregion&o=xml 	
<ul style="list-style-type: none"> • data::polygondrawdata: • 3.8.7.1 • data::polygon3ddrawdata: • https://api.mapbox.com 	ms/arm64-v8a/libgeoway_mobile_sdk.so
<ul style="list-style-type: none"> • http://www.winimage.com/zlibdll • 106.14.20.110 	lib/arm64-v8a/libqxinertial.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
EasyProtector	lamstrat2016	一行代码检测 WP/调试/多开/模拟器/root。
Fresco	Facebook	Fresco 是一个用于管理图像及其使用的内存的 Android 库。
Bugly	Tencent	腾讯 Bugly，为移动开发者提供专业的异常上报和运营统计，帮助开发者快速发现并解决异常，同时掌握产品运营动态，及时跟进用户反馈。
C++ 共享库	Android	在 Android 应用中运行原生代码。
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.
网易云信	Netease	网易云信致力于互联网络技术的开发与研究，使开发者通过简单集成客户端 SDK 和云端开放 API，快速实现强大的移动互联网 IM 和音视频功能。
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。

Jetpack Camera	Google	CameraX 是 Jetpack 的新增库。利用该库，可以更轻松地应用添加相机功能。该库提供了很多兼容性修复程序和解决方法，有助于在众多设备上打造一致的开发体验。
百度 LBS	Baidu	百度地图 Android SDK 是一套基于 Android 4.0 及以上版本设备的应用程序接口。您可以使用该套 SDK 开发适用于 Android 系统移动设备的地图应用，通过调用地图 SDK 接口，您可以轻松访问百度地图服务和数据，构建功能丰富、交互性强的地图类应用程序。
OpenCV	OpenCV	OpenCV 是一个跨平台的计算机视觉库，可用于开发实时的图像处理、计算机视觉以及模式识别程序。
SQLite	SQLite	SQLite 是遵守 ACID 的关系数据库管理系统，它包含在一个相对小的 C 程序库中。与许多其它数据库管理系统不同，SQLite 不是一个客户端/服务器结构的数据库引擎，而是被集成在用户程序中。SQLite 遵守 ACID，实现了大多数 SQL 标准。它使用动态的、弱类型的 SQL 语法。
Jetpack Test	Google	在 Android 中进行测试。
EasyPermissions	Google	EasyPermissions 是一个包装器库，用于简化针对 Android M 或更高版本的基本系统权限逻辑。
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。
Jetpack App Startup	Google	App Startup 库提供了一种直接、高效的方法来在应用程序启动时初始化组件。库开发人员 and 应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。
网易云通信 SDK	Netease	IM SDK 是网易云通信其他能力（实时语音视频、互动白板等）的基础，本节讲述 IM SDK 的集成步骤也将其他能力 SDK 的集成步骤融合起来，开发者可以根据实际业务需要选择接入的类库。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media3 取代。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).

✉ 邮箱地址敏感信息提取

EMAIL	源码文件
piyush.agram@jpl.nasa.gov	lib/arm64-v8a/libgdal.so

🕒 第三方追踪器检测

名称	类别	网址
AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97
Bugly		https://reports.exodus-privacy.eu.org/trackers/190

🔑 敏感凭证泄露检测

可能的密钥
个推-推送服务的=> "PUSH_APPID" : "dVXz3REjsK9M1hwjcseshi"
高德地图的=> "com.amap.api.v2.apikey" : "d3b57b915034c6f90ec40a77e6f81b82"
个推-推送服务的=> "GETUI_APPID" : "dVXz3REjsK9M1hwjcseshi"
百度地图的=> "com.baidu.lbsapi.API_KEY" : "ghHGU5S1yaTZZwQyDeCjxeMc8S8KIagl"
"user_auth_address" : "https://landcloud.org.cn"
nusTjjSFCXDl6qOBXfdOQ2bKfreTynIzGUXk2UxB9P9LYFq124Pk93bwjuysSS31sifqYX
0ce8c792-8dd0-4911-aa5a-fc44085f0aca
nMDgyOTA4MDg1OFowjTELMaKGA1UEBhMCQ04xFlAUBGNVBAoMDVWESUQgU0RLIFByij13K
ndkO2OrPD2LLosGvskAzXKNW2FfihAenUvQboKxgN6Ce638Iypg3QuopWJSsbWoV3Lix41
nb2QwggEiMA0GCSqGSIsb3DQEBAQUAA4IBDwAwggEKAoIBAQC0Y+iQLMxyq2qaLKaDLijxK
28e9fa9e9d9f5e344d5a9e4bcf6509a7f39789f515ab8f92ddbcdb414d940e93
uDjBjuikjKI5iN0ECdTD80mAoYk4xFap
XTUMwQ0ZDNGo4cFZKMKmZHFQVdZditGYzduazV4QzZBaFVBbkjzRUEXmInhqynFxSEY3bkpTUFVYMoM2NzdRPQoKXYXBwVG9rZW49YzQxYTM5ZjktN2I5MC00MThhLTkyZjUtN2I0ODljZDYxZmFhCnBhY2thZ2VOYW11PWVhbnVzSjYXJ0by5oZWxsb211eShbmRyb2lkcm9ubGluZUxpY2Vuc2U9MQpwcm9kdWN0cz1zZGstYW5kcm9pZC00LioKd2F0ZXJtYXJrPWNhcnRyZGki
a4a00eab-ba23-4af0-ac11-9e6aad465ab
6cd3bdc17c17a0e00ffc57e45418984c
32c4ae2c1f1981195f9904466a39c9948fe30bbbf2e60be1715a4589334c74c7
e7827fd1fc8c8f713af553b26cc4d981
057091df-5c02-492f-bf4a-3d5a2095b51c
337b96b6-65c6-4293-8954-0114f6433fd2
e8e8b6ec-f114-473c-b011-8ccb562e08e8
nTjEWMBOGA1UECjwvURJRCBTRERglJHjZDAgFw0yMTA5MjIwODA4NThaGA8yMTIxKliqX
bc3736a2f1f6879c59bdcee36b692153a0a9877cc62a474002df32e52139f0a0
073bd8195d024c5681338b3d904f53ed
1AB21D8355CFA17F8E61197831E81A8F22BEC8C728FEFB747ED035EB5082AA2B
n3FgpZL+464f932u0te6doKzk6EYGubC3c3YbPaHTpvZ1BF185Gmlb8UHO63UnrfHli1JU
-361d2832796043df2db3dd115622f302f4b4690cfa9f3d9e79397f4cb044ae9
cdbeb44a424c48f2b1215f06a4810350

7165c5ec-d7f7-4bcb-b25c-7c78204326c3
4dceed7b-e30d-4ac1-82f6-0375c93a5be9
nea0eWqeKM0I2RFbTsSBZDdfk4g6i2OA9e9Rp3cBq8GNED81sGbVKaq3NQ=jqliO
33472b7e-410e-426d-b09e-6ffa72257e35
nKQTHaBxNTrrjDrrnLHYoUogIFP9P+LS5Ua9i0onfnRqmJhyyMp+n/yf+ejdU0Ac3biu91U
a25c8a9f-995c-4ecb-8832-1af60c1b7127
7d6637705c7cfbbdfffc28389b4fa60e6
97f846ee-2e67-4568-b114-18b49acec8a3
befb26a0-0128-4b23-9770-35d85d6e4a0d
MIIcYDCCAbACCQCDpoADskZ6uTANBgkqhkiG9w0BAQsFADAIMQswCQYDVQQGEwJDUixIK
09d60fd4-33de-4db5-8919-ee5a4351fdde
e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855
878ee154cd70417e54f6d07bb18cc3fe
ea95d11209614dbea6bca6dc21f34616
1539143597861837489899068
AWSAccessKeyId=EFBO6ZTTBDC339XURKIN
d5d53c86aea82b5978d9992eb50ba4df
de159c76d86ca0a75f2831f61b800d12
nfXK9AgMBAAEwDQYJKoZIhvcNAQELBQAQggEBADauzLvXVQIyZNo4qUOchnod1SaaIxxqKy
4ac87a9c-108b-4db0-b4ea-081001acc0a15
a9f938af-759d-480f-94ff-0182b3ac073c

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