



ANDROID 静态分析报告



◆ QQ • v9.0.19

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: 2025-04-07 21:06:44

i应用概览

文件名称:	QQ v9.0.19.apk
文件大小:	3.18MB
应用名称:	QQ
软件包名:	dkplugin.wlg.pkr
主活动:	com.bly.dkplat.PluginFirstRunActivity
版本号:	9.0.19
最小SDK:	19
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:	36/100 (高风险)
杀软检测:	3 个杀毒软件报毒
MD5:	1aca6f81f527b3576976d53c1f00e44a
SHA1:	e462c52c9f0ff20d503570380236a142206e1007
SHA256:	994a3fe6c88a875b81f1f9d86f547b9e8c72a3185b4f5e02e924da285f7cf1b

分析结果严重性

高危	中危	信息	安全	关注
76	196	1	1	2

四大组件信息

Activity组件: 77个, 其中export的有: 72个
Service组件: 25个, 其中export的有: 23个
Receiver组件: 4个, 其中export的有: 4个
Provider组件: 2个, 其中export的有: 23个

证书信息

二进制文件已签名
v1 签名: True

v2 签名: True
 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:
 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccb6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569

公钥算法: rsa
 密钥长度: 2048
 指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75
 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.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_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。
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.INTERACT_ACROSS_USERS	未知	未知权限	来自 android 引用的未知权限。
android.permission.INTERACT_ACROSS_USERS_FULL	签名	允许应用程序在所有用户之间进行交互	允许应用程序在所有用户之间进行交互。这包括在其他用户的应用程序中创建活动、发送广播和执行其他操作。
android.permission.REAL_GET_TASKS	未知	未知权限	来自 android 引用的未知权限。
com.huawei.android.launcher.permission.WRITE_SETTINGS	普通	在应用程序上显示通知计数	在华为首手机的应用程序启动图标上显示通知计数或徽章。
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_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.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.AUTHENTICATE_ACCOUNTS	危险	作为帐户身份验证程序	允许应用程序使用 AccountManager 的帐户身份验证程序功能，包括创建帐户以及获取和设置其密码。
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.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电太多内存，从而降低其速度或稳定性。
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_MULTICAST_STATE	危险	允许接收WLAN多播	允许应用程序接收并非直接向您的设备发送的数据包。这在查找附近提供的服务时很有用。这种操作所耗电量大于非多播模式。
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.DISABLE_KEYGUARD	危险	禁用键盘锁	允许应用程序停用键锁和任何关联的密码安全设置。例如，在手机上接听电话时停用键锁，在通话结束后重新启用键锁。
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	普通	后台下载文件	这个权限是允许应用通过下载管理器下载文件，且不对用户进行任何提示。
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.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	探索已知帐户	允许应用程序访问帐户服务中的帐户列表。
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.KILL_BACKGROUND_PROCESSES	普通	结束进程	允许应用程序结束其他应用程序的后台进程。
android.permission.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加、删除帐户及删除其密码之类的操作。
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.NFC	危险	控制nfc功能	允许应用程序与支持nfc的物体交互。
android.permission.PERSISTENT_ACTIVITY	危险	让应用程序始终运行	允许应用程序部分持续运行，这样系统便不能将其用于其他应用程序。
android.permission.READ_CALENDAR	危险	读取日历活动	允许应用程序读取您手机上存储的所有日历活动。恶意应用程序可借此将您的日历活动发送给其他人。
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_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.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.READ_SYNC_SETTINGS	普通	读取同步设置	允许应用程序读取同步设置，例如是否为 联系人 启用同步。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.RESTART_PACKAGES	普通	重启进程	允许程序自己重启或重启其他程序
android.permission.ACTIVITY_RECOGNITION	危险	允许应用程序识别身体活动	允许应用程序识别身体活动。
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.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_CALENDAR	危险	添加或修改日历活动以及向邀请对象发送电子邮件	允许应用程序添加或更改日历中的活动。 这可能会向邀请对象发送电子邮件。 恶意应用程序可能会借此清除或修改您的日历活动，或者向邀请对象发送电子邮件。
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_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.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.WRITE_SYNC_SETTINGS	危险	修改同步设置	允许应用程序修改同步设置。
android.permission.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。 应用程序应改为请求USE_BIOMETRIC
com.google.android.gms.permission.ACTIVITY_RECOGNITION	危险	允许应用程序识别身体活动	允许应用程序识别身体活动。
com.google.android.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	普通	OPPO推送服务	OPPO推送服务正常工作所必需的，它允许应用接收来自OPPO推送系统的消息。
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_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.WRITE_OWNER_DATA	未知	未知权限	来自 android 引用的未知权限。
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。
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。
com.android.launcher.permission.WRITE_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.android.launcher3.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。

com.android.launcher3.permission.WRITE_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.android.launcher2.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。
com.lenovo.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
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.bbk.launcher2.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
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.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。
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.GET_INSTALLED_APPS	未知	未知权限	来自 android 引用的未知权限。
com.android.permission.GET_INSTALLED_APPS	未知	未知权限	来自 android 引用的未知权限。
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。
android.permission.LOCAL_MAC_ADDRESS	未知	未知权限	来自 android 引用的未知权限。
android.permission.START_ANY_ACTIVITY	未知	未知权限	来自 android 引用的未知权限。
android.permission.WRITE_APN_SETTINGS	危险	写入访问点名称设置	允许应用程序写入访问点名称设置。
android.permission.REORDER_TASKS	危险	对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。
com.android.launcher.permission.INSTALL_SHORTCUT	签名	创建快捷方式	这个权限是允许应用程序创建桌面快捷方式。
com.android.launcher.permission.UNINSTALL_SHORTCUT	签名	删除快捷方式	这个权限是允许应用程序删除桌面快捷方式。
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.huawei.authentication.HW_ACCESS_AUTH_SERVICE	未知	未知权限	来自 android 引用的未知权限。
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.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.USE_FULL_SCREEN_INTENT	普通	全屏通知	Android 10以后的全屏 Intent 的通知。
miui.permission.READ_STEPS	未知	未知权限	来自 android 引用的未知权限。

com.soter.permission.ACCESS_SOTER_KEYSTORE	未知	未知权限	来自 android 引用的未知权限。
android.permission.USE_FACERECOGNITION	未知	未知权限	来自 android 引用的未知权限。
android.permission.READ_PACKAGE_BADGE	未知	未知权限	来自 android 引用的未知权限。
telecom.mdesk.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
android.permission.HIGH_SAMPLING_RATE_SENSORS	普通	传感器的数据刷新率限制	允许应用以大于 200 Hz 的采样率访问传感器数据, 此数据包括由设备的加速度, 陀螺仪和磁力传感器记录的值。
org.adw.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.qihoo360.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.lge.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.sec.android.app.twlauncher.settings.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.fede.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.ebproductions.android.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.meizu.launcher2.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.meizu.android.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.huawei.launcher3.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.huawei.launcher2.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
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.WRITE_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.open.gallery.smart.Read	未知	未知权限	来自 android 引用的未知权限。
com.open.gallery.smart.Write	未知	未知权限	来自 android 引用的未知权限。
com.open.gallery.smart.Provider	未知	未知权限	来自 android 引用的未知权限。
com.huaqin.launcher.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.htc.launcher.settings	未知	未知权限	来自 android 引用的未知权限。
android.permission.SYSTEM_OVERLAY_WINDOW	未知	未知权限	来自 android 引用的未知权限。
com.tencent.permission.VIRUS_SCAN	未知	未知权限	来自 android 引用的未知权限。
com.lenovo.launcher.permission.BADGE_READ	未知	未知权限	来自 android 引用的未知权限。
com.lenovo.launcher.permission.BADGE_WRITE	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.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.asus.msa.SupplementaryDID.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。

🔒 网络通信安全

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: 73 | 警告: 187 | 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.bly.dkplat.PluginFirstRunActivity) 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”并设置空 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。
5	Activity (com.bly.chaos.plugin.sub.StubBridgeActivity) 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”并设置空 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。

6	Activity (com.bly.chaos.plugin.stub.StubBridgeActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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。
7	Activity设置了TaskAffinity属性 (com.bly.chaosapp.activity.SplashActivity)	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	Broadcast Receiver (com.bly.chaos.host.receiver.KillSelfReceiver) 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。
9	Activity (com.bly.dkplat.PluginCleanActivity) 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”并设置空 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。
10	Activity (com.bly.dkplat.PluginCleanActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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	Activity (com.bly.dkplat.MigrateEntryActivity) 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”并设置空 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。
12	Activity (com.bly.dkplat.MigrateEntryActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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	Activity (com.bly.dkplat.MigrateNewActivity) 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”并设置空 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。
14	Activity (com.bly.dkplat.MigrateNewActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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	Activity (com.bly.dkplat.MigrateNewNextActivity) 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”并设置空 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。
16	Activity (com.bly.dkplat.MigrateNewNextActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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。
17	Activity (com.bly.dkplat.MigrateOldActivity) 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”并设置空 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。

18	Activity (com.bly.dkplat.MigrateOldActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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。
19	Activity (com.bly.dkplat.MigrateOldNextActivity) 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”并设置空 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。
20	Activity (com.bly.dkplat.MigrateOldNextActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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。
21	Activity (com.bly.dkplat.PluginBackupActivity) 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”并设置空 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。
22	Activity (com.bly.dkplat.PluginBackupActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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。
23	Service (com.bly.chaos.host.service.DaemonService) 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。
24	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.PendingActivityStub)	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
25	Activity (com.bly.chaos.plugin.stub.PendingActivityStub) 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”并设置空 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。
26	Activity (com.bly.chaos.plugin.stub.PendingActivityStub) 未被保护。 [android:exported=true]	警告	发现 Activity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。
27	Service (com.bly.chaos.plugin.stub.PendingServiceStub) 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。
28	Broadcast Receiver (com.bly.chaos.plugin.stub.PendingReceiverStub) 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。

29	Service (com.bly.chaos.plugin.stub.JobStub) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_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。
30	Activity (com.bly.chaos.plugin.stub.ChooserActivityStub) 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"并设置空 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。
31	Activity (com.bly.chaos.plugin.stub.ChooserActivityStub) 未被保护。 [android:exported=true]	警告	发现 Activity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。
32	Activity (com.bly.chaos.plugin.stub.ResolverActivity) 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"并设置空 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。
33	Activity (com.bly.chaos.plugin.stub.ResolverActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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。
34	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.StubNotificationPendingActivity)	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
35	Activity (com.bly.chaos.plugin.stub.StubNotificationPendingActivity) 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"并设置空 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。
36	Activity (com.bly.chaos.plugin.stub.StubNotificationPendingActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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。
37	Content Provider (com.bly.chaos.plugin.stub.ServiceProvider) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
38	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$P0)	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
39	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P0) 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"并设置空 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。

40	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P0) 未被保护。 [android:exported=true]	警告	发现 Activity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。
41	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$P1)	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
42	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P1) 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”并设置空 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。
43	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P1) 未被保护。 [android:exported=true]	警告	发现 Activity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。
44	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$P2)	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
45	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P2) 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”并设置空 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。
46	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P2) 未被保护。 [android:exported=true]	警告	发现 Activity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。
47	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$P3)	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
48	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P3) 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”并设置空 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。
49	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P3) 未被保护。 [android:exported=true]	警告	发现 Activity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。
50	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$P4)	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
51	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P4) 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”并设置空 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。

52	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P4) 未被保护。 [android:exported=true]	警告	发现 Activity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。
53	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$P5)	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
54	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P5) 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”并设置空 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。
55	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P5) 未被保护。 [android:exported=true]	警告	发现 Activity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。
56	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$P6)	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
57	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P6) 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”并设置空 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。
58	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P6) 未被保护。 [android:exported=true]	警告	发现 Activity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。
59	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$P7)	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
60	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P7) 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”并设置空 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。
61	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P7) 未被保护。 [android:exported=true]	警告	发现 Activity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。
62	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$P8)	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
63	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P8) 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”并设置空 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。

64	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P8) 未被保护。 [android:exported=true]	警告	发现 Activity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。
65	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$P9)	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
66	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P9) 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”并设置空 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。
67	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P9) 未被保护。 [android:exported=true]	警告	发现 Activity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。
68	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$P10)	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
69	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P10) 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”并设置空 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。
70	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P10) 未被保护。 [android:exported=true]	警告	发现 Activity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。
71	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$P11)	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
72	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P11) 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”并设置空 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。
73	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P11) 未被保护。 [android:exported=true]	警告	发现 Activity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。
74	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$P12)	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
75	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P12) 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”并设置空 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。

76	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P12) 未被保护。 [android:exported=true]	警告	发现 Activity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。
77	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$P13)	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
78	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P13) 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”并设置空 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。
79	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P13) 未被保护。 [android:exported=true]	警告	发现 Activity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。
80	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$P14)	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
81	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P14) 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”并设置空 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。
82	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P14) 未被保护。 [android:exported=true]	警告	发现 Activity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。
83	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$P15)	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
84	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P15) 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”并设置空 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。
85	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P15) 未被保护。 [android:exported=true]	警告	发现 Activity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。
86	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$P16)	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
87	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P16) 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”并设置空 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。

88	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P16) 未被保护。 [android:exported=true]	警告	发现 Activity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。
89	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$P17)	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
90	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P17) 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”并设置空 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。
91	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P17) 未被保护。 [android:exported=true]	警告	发现 Activity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。
92	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$P18)	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
93	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P18) 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”并设置空 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。
94	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P18) 未被保护。 [android:exported=true]	警告	发现 Activity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。
95	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$P19)	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
96	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P19) 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”并设置空 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。
97	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P19) 未被保护。 [android:exported=true]	警告	发现 Activity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。
98	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$P20)	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
99	Activity (com.bly.chaos.plugin.stub.ActivityStub\$P20) 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”并设置空 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。

100	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL0) 未被保护。 [android:exported=true]	警告	发现 Activity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。
101	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$PL1)	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
102	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL1) 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”并设置空 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。
103	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL1) 未被保护。 [android:exported=true]	警告	发现 Activity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。
104	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$PL2)	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
105	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL2) 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”并设置空 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。
106	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL2) 未被保护。 [android:exported=true]	警告	发现 Activity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。
107	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$PL3)	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
108	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL3) 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”并设置空 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。
109	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL3) 未被保护。 [android:exported=true]	警告	发现 Activity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。
110	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$PL4)	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
111	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL4) 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”并设置空 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。

112	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL4) 未被保护。 [android:exported=true]	警告	发现 Activity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。
113	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$PL5)	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
114	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL5) 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”并设置空 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。
115	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL5) 未被保护。 [android:exported=true]	警告	发现 Activity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。
116	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$PL6)	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
117	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL6) 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”并设置空 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。
118	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL6) 未被保护。 [android:exported=true]	警告	发现 Activity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。
119	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$PL7)	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
120	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL7) 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”并设置空 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。
121	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL7) 未被保护。 [android:exported=true]	警告	发现 Activity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。
122	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$PL8)	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
123	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL8) 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”并设置空 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。

124	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL8) 未被保护。 [android:exported=true]	警告	发现 Activity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。
125	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$PL9)	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
126	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL9) 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”并设置空 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。
127	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL9) 未被保护。 [android:exported=true]	警告	发现 Activity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。
128	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$PL10)	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
129	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL10) 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”并设置空 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。
130	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL10) 未被保护。 [android:exported=true]	警告	发现 Activity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。
131	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$PL11)	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
132	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL11) 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”并设置空 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。
133	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL11) 未被保护。 [android:exported=true]	警告	发现 Activity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。
134	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$PL12)	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
135	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL12) 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”并设置空 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。

136	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL12) 未被保护。 [android:exported=true]	警告	发现 Activity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。
137	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$PL13)	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
138	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL13) 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”并设置空 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。
139	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL13) 未被保护。 [android:exported=true]	警告	发现 Activity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。
140	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$PL14)	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
141	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL14) 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”并设置空 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。
142	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL14) 未被保护。 [android:exported=true]	警告	发现 Activity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。
143	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$PL15)	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
144	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL15) 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”并设置空 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。
145	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL15) 未被保护。 [android:exported=true]	警告	发现 Activity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。
146	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$PL16)	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
147	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL16) 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”并设置空 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。

148	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL16) 未被保护。 [android:exported=true]	警告	发现 Activity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。
149	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$PL17)	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
150	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL17) 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”并设置空 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。
151	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL17) 未被保护。 [android:exported=true]	警告	发现 Activity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。
152	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$PL18)	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
153	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL18) 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”并设置空 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。
154	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL18) 未被保护。 [android:exported=true]	警告	发现 Activity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。
155	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.ActivityStub\$PL19)	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
156	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL19) 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”并设置空 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。
157	Activity (com.bly.chaos.plugin.stub.ActivityStub\$PL19) 未被保护。 [android:exported=true]	警告	发现 Activity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。
158	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.DialogStub\$P0)	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
159	Activity (com.bly.chaos.plugin.stub.DialogStub\$P0) 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”并设置空 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。

160	Activity (com.bly.chaos.plugin.stub.DialogStub\$P0) 未被保护。 [android:exported=true]	警告	发现 Activity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。
161	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.DialogStub\$P1)	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
162	Activity (com.bly.chaos.plugin.stub.DialogStub\$P1) 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”并设置空 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。
163	Activity (com.bly.chaos.plugin.stub.DialogStub\$P1) 未被保护。 [android:exported=true]	警告	发现 Activity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。
164	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.DialogStub\$P2)	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
165	Activity (com.bly.chaos.plugin.stub.DialogStub\$P2) 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”并设置空 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。
166	Activity (com.bly.chaos.plugin.stub.DialogStub\$P2) 未被保护。 [android:exported=true]	警告	发现 Activity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。
167	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.DialogStub\$P3)	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
168	Activity (com.bly.chaos.plugin.stub.DialogStub\$P3) 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”并设置空 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。
169	Activity (com.bly.chaos.plugin.stub.DialogStub\$P3) 未被保护。 [android:exported=true]	警告	发现 Activity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。
170	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.DialogStub\$P4)	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
171	Activity (com.bly.chaos.plugin.stub.DialogStub\$P4) 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”并设置空 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。

172	Activity (com.bly.chaos.plugin.stub.DialogStub\$P4) 未被保护。 [android:exported=true]	警告	发现 Activity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。
173	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.DialogStub\$P5)	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
174	Activity (com.bly.chaos.plugin.stub.DialogStub\$P5) 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”并设置空 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。
175	Activity (com.bly.chaos.plugin.stub.DialogStub\$P5) 未被保护。 [android:exported=true]	警告	发现 Activity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。
176	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.DialogStub\$P6)	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
177	Activity (com.bly.chaos.plugin.stub.DialogStub\$P6) 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”并设置空 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。
178	Activity (com.bly.chaos.plugin.stub.DialogStub\$P6) 未被保护。 [android:exported=true]	警告	发现 Activity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。
179	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.DialogStub\$P7)	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
180	Activity (com.bly.chaos.plugin.stub.DialogStub\$P7) 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”并设置空 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。
181	Activity (com.bly.chaos.plugin.stub.DialogStub\$P7) 未被保护。 [android:exported=true]	警告	发现 Activity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。
182	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.DialogStub\$P8)	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
183	Activity (com.bly.chaos.plugin.stub.DialogStub\$P8) 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”并设置空 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。

184	Activity (com.bly.chaos.plugin.stub.DialogStub\$P8) 未被保护。 [android:exported=true]	警告	发现 Activity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。
185	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.DialogStub\$P9)	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
186	Activity (com.bly.chaos.plugin.stub.DialogStub\$P9) 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”并设置空 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。
187	Activity (com.bly.chaos.plugin.stub.DialogStub\$P9) 未被保护。 [android:exported=true]	警告	发现 Activity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。
188	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.DialogStub\$P10)	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
189	Activity (com.bly.chaos.plugin.stub.DialogStub\$P10) 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”并设置空 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。
190	Activity (com.bly.chaos.plugin.stub.DialogStub\$P10) 未被保护。 [android:exported=true]	警告	发现 Activity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。
191	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.DialogStub\$P11)	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
192	Activity (com.bly.chaos.plugin.stub.DialogStub\$P11) 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”并设置空 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。
193	Activity (com.bly.chaos.plugin.stub.DialogStub\$P11) 未被保护。 [android:exported=true]	警告	发现 Activity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。
194	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.DialogStub\$P12)	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
195	Activity (com.bly.chaos.plugin.stub.DialogStub\$P12) 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”并设置空 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。

196	Activity (com.bly.chaos.plugin.stub.DialogStub\$P12) 未被保护。 [android:exported=true]	警告	发现 Activity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。
197	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.DialogStub\$P13)	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
198	Activity (com.bly.chaos.plugin.stub.DialogStub\$P13) 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”并设置空 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。
199	Activity (com.bly.chaos.plugin.stub.DialogStub\$P13) 未被保护。 [android:exported=true]	警告	发现 Activity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。
200	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.DialogStub\$P14)	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
201	Activity (com.bly.chaos.plugin.stub.DialogStub\$P14) 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”并设置空 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。
202	Activity (com.bly.chaos.plugin.stub.DialogStub\$P14) 未被保护。 [android:exported=true]	警告	发现 Activity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。
203	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.DialogStub\$P15)	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
204	Activity (com.bly.chaos.plugin.stub.DialogStub\$P15) 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”并设置空 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。
205	Activity (com.bly.chaos.plugin.stub.DialogStub\$P15) 未被保护。 [android:exported=true]	警告	发现 Activity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。
206	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.DialogStub\$P16)	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
207	Activity (com.bly.chaos.plugin.stub.DialogStub\$P16) 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”并设置空 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。

208	Activity (com.bly.chaos.plugin.stub.DialogStub\$P16) 未被保护。 [android:exported=true]	警告	发现 Activity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。
209	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.DialogStub\$P17)	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
210	Activity (com.bly.chaos.plugin.stub.DialogStub\$P17) 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”并设置空 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。
211	Activity (com.bly.chaos.plugin.stub.DialogStub\$P17) 未被保护。 [android:exported=true]	警告	发现 Activity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。
212	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.DialogStub\$P18)	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
213	Activity (com.bly.chaos.plugin.stub.DialogStub\$P18) 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”并设置空 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。
214	Activity (com.bly.chaos.plugin.stub.DialogStub\$P18) 未被保护。 [android:exported=true]	警告	发现 Activity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。
215	Activity设置了TaskAffinity属性 (com.bly.chaos.plugin.stub.DialogStub\$P19)	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
216	Activity (com.bly.chaos.plugin.stub.DialogStub\$P19) 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”并设置空 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。
217	Activity (com.bly.chaos.plugin.stub.DialogStub\$P19) 未被保护。 [android:exported=true]	警告	发现 Activity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。
218	Content Provider (com.bly.chaos.plugin.stub.ProviderStub\$P0) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
219	Content Provider (com.bly.chaos.plugin.stub.ProviderStub\$P1) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。

220	Content Provider (com.bly.c haos.plugin.stub.ProviderStub\$P2) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
221	Content Provider (com.bly.c haos.plugin.stub.ProviderStub\$P3) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
222	Content Provider (com.bly.c haos.plugin.stub.ProviderStub\$P4) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
223	Content Provider (com.bly.c haos.plugin.stub.ProviderStub\$P5) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
224	Content Provider (com.bly.c haos.plugin.stub.ProviderStub\$P6) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
225	Content Provider (com.bly.c haos.plugin.stub.ProviderStub\$P7) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
226	Content Provider (com.bly.c haos.plugin.stub.ProviderStub\$P8) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
227	Content Provider (com.bly.c haos.plugin.stub.ProviderStub\$P9) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
228	Content Provider (com.bly.c haos.plugin.stub.ProviderStub\$P10) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
229	Content Provider (com.bly.c haos.plugin.stub.ProviderStub\$P11) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
230	Content Provider (com.bly.c haos.plugin.stub.ProviderStub\$P12) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
231	Content Provider (com.bly.c haos.plugin.stub.ProviderStub\$P13) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。

232	Content Provider (com.bly.c haos.plugin.stub.ProviderStub\$P14) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
233	Content Provider (com.bly.c haos.plugin.stub.ProviderStub\$P15) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
234	Content Provider (com.bly.c haos.plugin.stub.ProviderStub\$P16) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
235	Content Provider (com.bly.c haos.plugin.stub.ProviderStub\$P17) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
236	Content Provider (com.bly.c haos.plugin.stub.ProviderStub\$P18) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
237	Content Provider (com.bly.c haos.plugin.stub.ProviderStub\$P19) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
238	Service (com.bly.chaos.plugin.stub.ServiceStub\$P0) 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。
239	Service (com.bly.chaos.plugin.stub.ServiceStub\$P1) 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。
240	Service (com.bly.chaos.plugin.stub.ServiceStub\$P2) 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。
241	Service (com.bly.chaos.plugin.stub.ServiceStub\$P3) 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。
242	Service (com.bly.chaos.plugin.stub.ServiceStub\$P4) 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。
243	Service (com.bly.chaos.plugin.stub.ServiceStub\$P5) 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。

244	Service (com.bly.chaos.plugin.stub.ServiceStub\$P6) 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。
245	Service (com.bly.chaos.plugin.stub.ServiceStub\$P7) 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。
246	Service (com.bly.chaos.plugin.stub.ServiceStub\$P8) 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。
247	Service (com.bly.chaos.plugin.stub.ServiceStub\$P9) 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。
248	Service (com.bly.chaos.plugin.stub.ServiceStub\$P10) 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。
249	Service (com.bly.chaos.plugin.stub.ServiceStub\$P11) 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。
250	Service (com.bly.chaos.plugin.stub.ServiceStub\$P12) 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。
251	Service (com.bly.chaos.plugin.stub.ServiceStub\$P13) 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。
252	Service (com.bly.chaos.plugin.stub.ServiceStub\$P14) 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。
253	Service (com.bly.chaos.plugin.stub.ServiceStub\$P15) 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。
254	Service (com.bly.chaos.plugin.stub.ServiceStub\$P16) 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。
255	Service (com.bly.chaos.plugin.stub.ServiceStub\$P17) 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。

256	Service (com.bly.chaos.plugin.stub.ServiceStub\$P18) 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。
257	Service (com.bly.chaos.plugin.stub.ServiceStub\$P19) 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。
258	Content Provider (com.bly.chaos.host.provider.InnerProviderProxy) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
259	Content Provider (com.bly.chaos.host.provider.EmptyProviderProxy) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
260	Broadcast Receiver (com.bly.chaos.host.receiver.DkplatPluginReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享, 因此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Broadcast Receiver是显式导出的。
261	Broadcast Receiver (com.bly.dkplat.PackageReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。

</> 安全漏洞检测

高危: 2 | 警告: 8 | 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: MSTG-CRYPTO-3	升级会员: 解锁高级权限
2	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
3	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

4	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
5	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
6	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
7	不安全的WebView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
8	可能存在跨域漏洞。在WebView中启用从URL访问文件可能会泄露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
9	不安全的WebView实现。WebView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
10	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
11	使用弱加密算法	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-4	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	arm64-v8a/libchaos.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

2	arm64-v8a/libchaos1.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。	No ne info 二进制文件没有设置运行时搜索路径或RPATH	No n o 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。	Tr u e info 符号被剥离
3	arm64-v8a/libpine.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。	No n e info 二进制文件没有设置运行时搜索路径或RPATH	No n e info 二进制文件没有设置RUNPATH	True info 二进制文件有以下加固函数:['_strlcat_chk', '_strcat_chk']	Tr u e info 符号被剥离

行为分析

编号	行为	标签	文件
00092	发送广播	命令	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
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
00054	从文件安装其他APK	反射	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
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
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
00039	启动网络服务器	控制网络	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
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
00033	查询IMEI号	信息收集	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
00053	监视给定内容 URI 标识的数据更改 (SMS、MMS 等)	短信	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
00128	查询用户账户信息	信息收集 账号	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
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
00130	获取当前WiFi信息	WiFi 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
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
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
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
00023	从当前应用程序启动另一个应用程序	反射 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
00034	查询当前数据网络类型	信息收集 网络	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	18/30	android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.CAMERA android.permission.GET_ACCOUNTS android.permission.GET_TASKS android.permission.MODIFY_AUDIO_SETTINGS android.permission.READ_CALENDAR android.permission.READ_CONTACTS android.permission.READ_PHONE_STATE android.permission.RECEIVE_BOOT_COMPLETED android.permission.RECORD_AUDIO android.permission.SYSTEM_ALERT_WINDOW android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.WRITE_CALENDAR android.permission.WRITE_CONTACTS android.permission.WRITE_SETTINGS android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	21/46	android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_AUDIO android.permission.READ_MEDIA_VIDEO android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.AUTHENTICATE_ACCOUNTS android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.BROADCAST_STICKY android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.FLASHLIGHT android.permission.READ_EXTERNAL_STORAGE android.permission.ACTIVITY_RECOGNITION android.permission.WRITE_EXTERNAL_STORAGE com.google.android.gms.permission.ACTIVITY_RECOGNITION android.permission.REORDER_TASKS com.android.launcher.permission.INSTALL_SHORTCUT android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.FOREGROUND_SERVICE

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
www.91ishare.cn	安全	否	No Geolocation information available.
wq.91ishare.cn	安全	是	IP地址: 106.75.138.93 国家: 中国 地区: 上海 城市: 上海 纬度: 31.224333 经度: 121.468948 查看: 高德地图

chaos.91ishare.cn	安全	是	IP地址: 106.75.137.46 国家: 中国 地区: 上海 城市: 上海 纬度: 31.224333 经度: 121.468948 查看: 高德地图
-------------------	----	---	---

URL链接分析

URL信息	源码文件
• http://chaos.91ishare.cn/serverv110?fn=svv	com/bly/dkplat/n.java
• http://chaos.91ishare.cn/server?fn=report	com/bly/chaos/b/a/n.java
• http://www.91ishare.cn	com/bly/chaosapp/activity/SplashActivity.java
• 127.0.0.1	c/a/a/a.java
• http://chaos.91ishare.cn/serverv60?fn=clonelog	com/bly/dkplat/e.java
• http://chaos.91ishare.cn/page/v60/migrate.html • http://chaos.91ishare.cn/permission/readapplist/temp.html	b/b/n/a/a.java
• http://chaos.91ishare.cn/server?fn=report	com/bly/chaos/host/v/j.java
• http://chaos.91ishare.cn/serverv45?fn=report	com/bly/chaos/b/c/g.java
• 127.0.0.1	com/bly/dkplat/q.java
• http://wq.91ishare.cn/iflyserver	com/bly/dkplat/j.java
• https://github.com/canyie/pine/issues/8	lib/arm64-v8a/libpine.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。
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
RMymjQc45jtxv1lkjuaD782pJdMZ+sa1yb9l7OAH74=
c2hqb6aMBKLO3tzuN4snasNBW3PzpJ8k
V5p4qDrowsCh3bl+t1vPsNoBrZxW2U2i

URtIIBSvO9XqeutiJxxmhhdMyIp2ZG1jpG2m6ne4jrg=
meMERqYssrSMnwfko0txooxHQXzIDtXGQDhVU7vpkbw7DfQF6OnF2tF/biz3IQB5
dYYrTOnt4o9seb7DGKXFvaRtpup3ul64
BCYaty3UxPW7QGJRuj4BfNbrYZDmc2mbfvc0UXt+aU=
cmxqvEUicuOT4IEFhSIWS435AfBRZ6Cj
cdOnQW6OEUM6K7HAf1TCnwolxG74rTfv
P7iqTWI03CUR1Oz6cliS/JnIQYobZFZ6
Wd+FU4fkiDTu5D6k0aCyXbsl19kp+T5CS19sfOtUCJs=
FObRWbWHQ8XLjMw8OyapSQEaEbmdYzgSxR+oJdLsm64=
nqyPYiDE2yeK9isCIZL0x9cLpeQ4fmus
F9074EBEBDDADEE08A78D36EFCCE9393802853C6
Twhk07wcHJKAXtWREISzeqyNPhhCk5xwx7dy414kzTI=
G7j2Aprdx3TNV5cbEKUrl6Rtpup3ul64
OT2APtZbpMa2sbDsk5cOB+zGiMbJF2l4Sdx92y48nk0e/K2z5QSwxA==
FJSpmOpZO2YAHbfmG/gakBGs77uNjxy1
8s7xqcAl7d50dzmKK8VmDH8EPkULQYfrbxX3pK29bSTXNA+4JY+R97zWBGQzOu
yuRww0hVWC9IoY9IMGsUB4w/pzz5fttVsprL6823Pml=
hisb6tNnr4j7ihxEkobOXLmn2SLtpFEw
BbgD5wGsd4pHI75/zfHdgKAILHV83oEt
Twhk07wcHJKAXtWREISzejuMI9mJePz1
JFdkATiL2gOPRQL84+0K1vW7ZtasD2ld
B8omV5JyRO/VnaJnnFGxNg5o3Uz6SwZM
NxT vz+T2f2nCdvPVohu5JBT6mNA87PzjKcYyvauzwc1
wC4m08boork3dk3RtInPW1f/ahwbcxO
32A821507D9e5673CDE3C713ACF553E2703CD40ED6BEBB101B484CEE83D537806C6CB691AEE86ED2CA8C97BBE95CF8476066D419E8E833376B850172107844D394016715B2E47E0A62FCB3E83A361FA7DFA44693F90D38C6A62029FCD8EA395ED868F9D718293E9C0E33194E87
HVwGc/0CNTM0tiHn1Pedmp12cgM8K1
lEnObd01CDfUis2QCL/H4lx2ixA4Y6jy
lthWDsjX9n3geY/TCQLqW6Rtpup3ul64
aCs/RtayGpUqZRh+fhwI5UIW8eiGQUJ
VoarWu0Jmeegkvz6MMSq34cXD8FRroWipG2m6ne4jrg=

lr5u0329dhyWnQvJy8wSbo+QY38Lyfil
rZ6038xJeAALy4+3BkD04x/XzsGFp2nG
ba/D2rZo5u9oGF33wmX9kc0G1dnoRUCo6cXfGt8fuVT9EYWgFsGlcg==
8s7xqcAl7d4kWJHIQBrLuHExEVtpb+K9
nKrQGMmH1VjAAcxz4r6ECFWpktDQHOLK
D6D2102F1C98E208FF5E863AA29334BD65AE1

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