南明离火

——移动应用检测平台——

ANDROID 静态分析报告

X8 Speeder • v3.3.6.8

分析日期: 2024-05-02 20:08:27

概述

文件名称:	x8s.apk
文件大小:	13.97MB
应用名称:	X8 Speeder
软件包名:	com.x8zs.ds2
主活动:	com.x8zs.ui.SplashActivity
版本号:	3.3.6.8
最小SDK:	22
目标SDK:	26
加固信息:	未加壳
MD5:	aa37d3a091cd7cb4c81fe778a047cb34
SHA1:	691b3692c3f4bd0538d1137388fc9ef916e21964
SHA256:	436b32ebfad4c27cfbdda65a3dd083b2bce0b076823f40ec494ddc3fbd5d17f0
应用程序安全分数:	32/100 (高风险)
跟踪器检测:	9/432
杀软检测:	8 个杀毒软件报毒

分析结果严重性

高危	中危	信息	安全	关注
20	26	1	2	22

四大组件信息

Activity组件：54个，其中export的有： 12个
Service组件：6个，其中export的有： 1个
Receiver组件：0个，其中export的有： 0个
Provider组件：6个，其中export的有： 0个

证书信息

二进制文件没有签名
缺少代码签名证书
v1 签名: False
v2 签名: False
v3 签名: False
v4 签名: False

应用权限

权限名称	安全等级	权限内容	权限描述
android.permission.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
android.permission.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.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.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_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.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.SYSTEM_OVERLAY_WINDOW	未知	未知权限	来自 android 引用的未知权限。
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.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
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.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.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.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。

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.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.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.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.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_PHONE_NUMBERS	危险	允许读取设备的电话号码	允许读取设备的电话号码。这是READ PHONE STATE授予的功能的一个子集，但对即时应用程序公开。
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错略的经纬度信息，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.INSTALL_PACKAGES	签名(系统)	请求安装APP	允许应用程序安装全新的或更新的 Android 包。恶意应用程序可能会借此添加其具有任意权限的新应用程序。

android.permission.PACKAGE_USAGE_STATS	签名	更新组件使用统计	允许修改组件使用情况统计
android.permission.MODIFY_PHONE_STATE	签名(系统)	修改手机状态	允许应用程序控制设备的电话功能。拥有此权限的应用程序可自行切换网络、打开和关闭无线通信等，而不会通知您。
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.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.INJECT_EVENTS	签名	按键和控制按钮	允许应用程序将其自己的输入活动（按键等）提供给其他应用程序。恶意应用程序可借此掌控手机。
android.permission.STOP_APP_SWITCHES	签名	禁止切换应用程序	禁止用户切换到另一应用程序。
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。
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。

VIRUSTOTAL 扫描

扫描结果： 8 个厂商报毒

反病毒引擎	检出结果

Fortinet	Android/Syringe.AG!tr
Google	Detected
Ikarus	Trojan.AndroidOS.Agent
K7GW	Trojan (0055846f1)
McAfee	Artemis!0638073A6180
Microsoft	Trojan:Script/Wacatac.B!ml
Sophos	Andr/Xgen4-B
Varist	AndroidOS/Helir.D.gen!Eldorado

网络安全配置

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。

证书分析

高危: **1** | 警告: **0** | 信息: **0**

标题	严重程度	描述信息
缺少代码签名证书	高危	未找到代码签名证书

MANIFEST分析

高危: **13** | 警告: **16** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 5.1-5.1.1, [minSdk=22]	警告	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	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。
3	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。
4	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。
5	Activity (com.x8zs.ui.task.TaskManagerActivity) is vulnerable to StrandHogg 2.0	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 (26) 更新到 29 或更高版本以在平台级别修复此问题。

6	Activity (com.x8zs.ui.task.TaskManagerActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
7	Activity (com.x8zs.ui.WebViewActivity) is vulnerable to StrandHogg 2.0	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 (26) 更新到 29 或更高版本以在平台级别修复此问题。
8	Activity (com.x8zs.ui.WebViewActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
9	Activity (com.x8zs.ui.FeedbackActivity) is vulnerable to StrandHogg 2.0	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 (26) 更新到 29 或更高版本以在平台级别修复此问题。
10	Activity (com.x8zs.ui.FeedbackActivity) 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，因此使其对设备上的任何其他应用程序都可访问。

11	Activity (com.x8zs.ui.AppDetailActivity) is vulnerable to StrandHogg 2.0	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 (26) 更新到 29 或更高版本以在平台级别修复此问题。
12	Activity (com.x8zs.ui.AppDetailActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
13	Activity (com.x8zs.ui.search.SearchActivity) is vulnerable to StrandHogg 2.0	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 (26) 更新到 29 或更高版本以在平台级别修复此问题。
14	Activity (com.x8zs.ui.search.SearchActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
15	Activity (com.x8zs.ui.open.OpenActivity) is vulnerable to StrandHogg 2.0	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 (26) 更新到 29 或更高版本以在平台级别修复此问题。

16	Activity (com.x8zs.ui.open.OpenActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
17	Activity (com.x8zs.ui.AllAppActivity) is vulnerable to StrandHogg 2.0	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 (26) 更新到 29 或更高版本以在平台级别修复此问题。
18	Activity (com.x8zs.ui.AllAppActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
19	Activity (com.x8zs.ui.list.HotListActivity) is vulnerable to StrandHogg 2.0	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 (26) 更新到 29 或更高版本以在平台级别修复此问题。
20	Activity (com.x8zs.ui.list.HotListActivity) 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，因此使其对设备上的任何其他应用程序都可访问。

21	Activity (com.x8zs.ui.LatestActivity) is vulnerable to StrandHogg 2.0	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 (26) 更新到 29 或更高版本以在平台级别修复此问题。
22	Activity (com.x8zs.ui.LatestActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
23	Activity (com.x8zs.ui.InjectActivity) is vulnerable to StrandHogg 2.0	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 (26) 更新到 29 或更高版本以在平台级别修复此问题。
24	Activity (com.x8zs.ui.InjectActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
25	Activity (com.x8zs.ad.AdStubActivity) is vulnerable to StrandHogg 2.0	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 (26) 更新到 29 或更高版本以在平台级别修复此问题。

26	Activity (com.x8zs.ad.AdStubActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
27	Activity (com.x8zs.sandbox.ad.AdProxyActivity) is vulnerable to StrandHogg 2.0	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 (26) 更新到 29 或更高版本以在平台级别修复此问题。
28	Activity (com.x8zs.sandbox.ad.AdProxyActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
29	Service (com.blankj.utilcode.util.MessengerUtils$ServerService) 未被保护。存在一个intent-filter。	警告	发现 Service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Service是显式导出的。
30	Activity （com.anythink.core.activity.AnyThinkGdprAuthActivity）容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这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”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (26) 更新到 28 或更高版本以在平台级别修复此问题。

</> 源代码分析

高危: 3 | 警告: 9 | 信息: 1 | 安全: 2 | 屏蔽: 0

序号	问题	等级	参考标准	文件位置
				a6/a.java a6/b.java a6/c.java cn/jzvd/JZTextureView.java cn/jzvd/Jzvd.java cn/jzvd/JzvdStd.java com/anythink/banner/api/ATBannerView.java com/anythink/interstitial/api/ATInterstitial.java com/apm/insight/b/j.java com/apm/insight/h/a.java com/apm/insight/k/k.java com/apm/insight/l/q.java com/applovin/impl/sdk/u.java com/bykv/vk/openvk/component/video/a/b/b.java com/bykv/vk/openvk/component/video/a/b/d.java com/bykv/vk/openvk/component/video/a/b/e.java com/bykv/vk/openvk/component/video/a/b/f.java com/bykv/vk/openvk/component/video/a/b/g.java com/bykv/vk/openvk/component/video/a/c/a.java com/bykv/vk/openvk/component/video/api/e/d.java com/iab/omid/library/inmobi/d/c.java com/inmobi/media/g.java com/inmobi/media/he.java com/mbridge/msdk/foundation/same/b/e.java com/mbridge/msdk/foundation/same/report/b/a.java com/mbridge/msdk/foundation/tools/n.java

				com/mbridge/msdk/foundation/tools/q.java com/mbridge/msdk/mbnative/controller/NativeController.java com/mbridge/msdk/mbnative/controller/b.java com/mbridge/msdk/playercommon/exoplayer2/DefaultRenderersFactory.java com/mbridge/msdk/playercommon/exoplayer2/ExoPlayerImpl.java com/mbridge/msdk/playercommon/exoplayer2/ExoPlayerImplInternal.java com/mbridge/msdk/playercommon/exoplayer2/MediaPeriodHolder.java com/mbridge/msdk/playercommon/exoplayer2/SimpleExoPlayer.java com/mbridge/msdk/playercommon/exoplayer2/audio/DefaultAudioSink.java com/mbridge/msdk/playercommon/exoplayer2/drm/ClearKeyUtil.java com/mbridge/msdk/playercommon/exoplayer2/drm/DefaultDrmSession.java com/mbridge/msdk/playercommon/exoplayer2/drm/DefaultDrmSessionManager.java com/mbridge/msdk/playercommon/exoplayer2/extractor/mkv/MatroskaExtractor.java com/mbridge/msdk/playercommon/exoplayer2/extractor/mp3/VbriSeeker.java com/mbridge/msdk/playercommon/exoplayer2/extractor/mp3/XingSeeker.java com/mbridge/msdk/playercommon/exoplayer2/extractor/mp4/AtomParsers.java com/mbridge/msdk/playercommon/exoplayer2/extractor/mp4/FragmentedMp4Extractor.java

				com/mbridge/msdk/playercommon/exoplayer2/extractor/mp4/MetadataUtil.java com/mbridge/msdk/playercommon/exoplayer2/extractor/mp4/PsshAtomUtil.java com/mbridge/msdk/playercommon/exoplayer2/extractor/mp4/TrackEncryptionBox.java com/mbridge/msdk/playercommon/exoplayer2/extractor/ogg/VorbisUtil.java com/mbridge/msdk/playercommon/exoplayer2/extractor/ts/AdtsReader.java com/mbridge/msdk/playercommon/exoplayer2/extractor/ts/H265Reader.java com/mbridge/msdk/playercommon/exoplayer2/extractor/ts/Id3Reader.java com/mbridge/msdk/playercommon/exoplayer2/extractor/ts/PesReader.java com/mbridge/msdk/playercommon/exoplayer2/extractor/wav/WavHeaderReader.java com/mbridge/msdk/playercommon/exoplayer2/mediacodec/MediaCodecInfo.java com/mbridge/msdk/playercommon/exoplayer2/mediacodec/MediaCodecRenderer.java com/mbridge/msdk/playercommon/exoplayer2/mediacodec/MediaCodecUtil.java com/mbridge/msdk/playercommon/exoplayer2/metadata/id3/Id3Decoder.java com/mbridge/msdk/playercommon/exoplayer2/offline/DownloadManager.java com/mbridge/msdk/playercommon/exoplayer2/offline/DownloadService.java

				com/mbridge/msdk/playercommon/exoplayer2/source/chunk/BaseMediaChunkOutput.java com/mbridge/msdk/playercommon/exoplayer2/source/chunk/ChunkSampleStream.java com/mbridge/msdk/playercommon/exoplayer2/source/chunk/ChunkedTrackBlacklistUtil.java com/mbridge/msdk/playercommon/exoplayer2/text/cea/Cea708Decoder.java com/mbridge/msdk/playercommon/exoplayer2/text/cea/CeaUtil.java com/mbridge/msdk/playercommon/exoplayer2/text/dvb/DvbParser.java com/mbridge/msdk/playercommon/exoplayer2/text/ssa/SsaDecoder.java com/mbridge/msdk/playercommon/exoplayer2/text/subrip/SubripDecoder.java com/mbridge/msdk/playercommon/exoplayer2/text/ttml/TtmlDecoder.java com/mbridge/msdk/playercommon/exoplayer2/text/webvtt/WebvttCue.java com/mbridge/msdk/playercommon/exoplayer2/text/webvtt/WebvttCueParser.java com/mbridge/msdk/playercommon/exoplayer2/upstream/DefaultDataSource.java com/mbridge/msdk/playercommon/exoplayer2/upstream/DefaultHttpDataSource.java com/mbridge/msdk/playercommon/exoplayer2/upstream/Loader.java com/mbridge/msdk/playercommon/exoplayer2/upstream/cache/CachedRegionTracker.java com/mbridge/msdk/playercommon/exoplayer2/upstream/cache/SimpleCache.java

				com/mbridge/msdk/playercommon/exoplayer2/util/AtomicFile.java com/mbridge/msdk/playercommon/exoplayer2/util/EventLogger.java com/mbridge/msdk/playercommon/exoplayer2/util/NalUnitUtil.java com/mbridge/msdk/playercommon/exoplayer2/util/Util.java com/mbridge/msdk/playercommon/exoplayer2/video/DummySurface.java com/mbridge/msdk/playercommon/exoplayer2/video/MediaCodecVideoRenderer.java com/mbridge/msdk/video/module/MBridgeBaseView.java com/mbridge/msdk/widget/FeedbackRadioGroup.java com/moat/analytics/mobile/inm/m.java com/moat/analytics/mobile/inm/p.java com/pgl/sys/ces/b.java com/unity3d/ads/UnityAdsBaseOptions.java com/unity3d/ads/metadata/InAppPurchaseMetaData.java com/unity3d/ads/metadata/MetaData.java com/unity3d/services/UnityServices.java com/unity3d/services/ads/UnityAdsImplementation.java com/unity3d/services/ads/adunit/AdUnitActivity.java com/unity3d/services/ads/adunit/VideoPlayerHandler.java com/unity3d/services/ads/api/AdUnit.java com/unity3d/services/ads/api/VideoPlayer.java com/unity3d/services/ads/api/WebPlayer.java com/unity3d/services/ads/configurati

				on/AdsModuleConfiguration.java com/unity3d/services/ads/gmascar/adapters/ScarAdapterFactory.java com/unity3d/services/ads/gmascar/bridges/AdapterStatusBridge.java com/unity3d/services/ads/gmascar/bridges/InitializeListenerBridge.java com/unity3d/services/ads/gmascar/bridges/MobileAdsBridge.java com/unity3d/services/ads/gmascar/finder/GMAInitializer.java com/unity3d/services/ads/gmascar/finder/ScarVersionFinder.java com/unity3d/services/ads/video/VideoPlayerView.java com/unity3d/services/ads/webplayer/WebPlayerView.java com/unity3d/services/ar/ARUtils.java com/unity3d/services/ar/view/ARView.java com/unity3d/services/ar/view/GLSurfaceView.java com/unity3d/services/ar/view/ShaderLoader.java com/unity3d/services/banners/BannerView.java com/unity3d/services/banners/UnityBanners.java com/unity3d/services/core/api/Cache.java com/unity3d/services/core/api/DeviceInfo.java com/unity3d/services/core/api/Intent.java com/unity3d/services/core/api/Request.java com/unity3d/services/core/api/Sdk.java com/unity3d/services/core/broadcast/BroadcastEventReceiver.java com/unity3d/services/core/cache/CacheDirectory.java com/unity3d/services/core/cache/Cac
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	

				heThread.java com/unity3d/services/core/cache/CacheThreadHandler.java com/unity3d/services/core/configuration/Configuration.java com/unity3d/services/core/configuration/EnvironmentCheck.java com/unity3d/services/core/configuration/InitializationNotificationCenter.java com/unity3d/services/core/configuration/InitializeThread.java com/unity3d/services/core/connectivity/ConnectivityMonitor.java com/unity3d/services/core/device/AdvertisingId.java com/unity3d/services/core/device/Device.java com/unity3d/services/core/device/OpenAdvertisingId.java com/unity3d/services/core/device/Storage.java com/unity3d/services/core/log/DeviceLog.java com/unity3d/services/core/misc/JsonStorage.java com/unity3d/services/core/misc/Utilities.java com/unity3d/services/core/misc/ViewUtilities.java com/unity3d/services/core/preferences/AndroidPreferences.java com/unity3d/services/core/properties/ClientProperties.java com/unity3d/services/core/properties/SdkProperties.java com/unity3d/services/core/reflection/GenericBridge.java com/unity3d/services/core/request/SDKMetrics.java com/unity3d/services/core/request/WebRequest.java com/unity3d/services/core/request/W

				ebRequestRunnable.java com/unity3d/services/core/request/WebRequestThread.java com/unity3d/services/core/sensorinfo/SensorInfoListener.java com/unity3d/services/core/webview/WebView.java com/unity3d/services/core/webview/WebViewApp.java com/unity3d/services/core/webview/bridge/Invocation.java com/unity3d/services/core/webview/bridge/NativeCallback.java com/unity3d/services/core/webview/bridge/WebViewBridge.java com/unity3d/services/core/webview/bridge/WebViewBridgeInterface.java com/unity3d/services/core/webview/bridge/WebViewCallback.java com/unity3d/services/store/core/StoreLifecycleListener.java com/unity3d/services/store/gpbl/bridges/CommonJsonResponseBridge.java com/unity3d/services/store/gpbl/bridges/PurchaseBridge.java com/x8zs/ad/AdManagerEx.java com/x8zs/ad/AdStubActivity.java com/x8zs/apkbuilder/ApkBuilder.java com/x8zs/apkbuilder/parser/ApkParser.java com/x8zs/app/X8Application.java com/x8zs/app/a.java com/x8zs/bridge/BridgeService.java com/x8zs/model/ScheduleService.java com/x8zs/model/ServerApi.java com/x8zs/model/X8DataModel.java com/x8zs/model/a.java com/x8zs/model/b.java com/x8zs/morgoo/droidplugin/MyCrashHandler.java com/x8zs/morgoo/droidplugin/Plugin

				Helper.java com/x8zs/morgoo/droidplugin/am/BaseActivityManagerService.java com/x8zs/morgoo/droidplugin/am/MyActivityManagerService.java com/x8zs/morgoo/droidplugin/am/RunningProcesList.java com/x8zs/morgoo/droidplugin/core/PluginClassLoader.java com/x8zs/morgoo/droidplugin/core/PluginProcessManager.java com/x8zs/morgoo/droidplugin/hook/HookFactory.java com/x8zs/morgoo/droidplugin/hook/HookedMethodHandler.java com/x8zs/morgoo/droidplugin/hook/handle/IPackageManagerHookHandle.java com/x8zs/morgoo/droidplugin/hook/handle/PluginCallback.java com/x8zs/morgoo/droidplugin/hook/proxy/IActivityManagerHook.java com/x8zs/morgoo/droidplugin/hook/proxy/LibCoreHook.java com/x8zs/morgoo/droidplugin/hook/proxy/PluginCallbackHook.java com/x8zs/morgoo/droidplugin/pm/IPluginManagerImpl.java com/x8zs/morgoo/droidplugin/pm/PluginManager.java com/x8zs/morgoo/droidplugin/pm/parser/PackageParserApi21.java com/x8zs/morgoo/droidplugin/pm/parser/PackageParserApi22.java com/x8zs/morgoo/droidplugin/pm/parser/PackageParserApi22Preview1.java com/x8zs/morgoo/droidplugin/stub/AbstractContentProviderStub.java com/x8zs/morgoo/droidplugin/stub/AbstractServiceStub.java com/x8zs/morgoo/helper/Log.java com/x8zs/morgoo/helper/Utils.java

				com/x8zs/morgoo/helper/compat/VMRuntimeCompat.java com/x8zs/plugin/client/ClientInfo.java com/x8zs/plugin/mta/MtaManager.java com/x8zs/plugin/patcher/MonkeyPatcher.java com/x8zs/plugin/utils/CrashHandler.java com/x8zs/plugin/utils/FLog.java com/x8zs/plugin/utils/HttpUtil.java com/x8zs/plugin/utils/LogUtil.java com/x8zs/plugin/utils/PkgUtil.java com/x8zs/plugin/utils/SLog.java com/x8zs/plugin/utils/UIUtil.java com/x8zs/plugin/volley/CacheDispatcher.java com/x8zs/plugin/volley/NetworkDispatcher.java com/x8zs/plugin/volley/Request.java com/x8zs/plugin/volley/VolleyLog.java com/x8zs/plugin/volley/toolbox/BasicNetwork.java com/x8zs/plugin/volley/toolbox/DiskBasedCache.java com/x8zs/plugin/volley/toolbox/HttpHeaderParser.java com/x8zs/plugin/volley/toolbox/ImageRequest.java com/x8zs/plugin/volley/toolbox/JsonRequest.java com/x8zs/plugins/FloatBallContainer.java com/x8zs/plugins/FloatWindowManager.java com/x8zs/plugins/PluginLoader.java com/x8zs/sandbox/ad/AdManager.java com/x8zs/sandbox/ad/AdProxyActivity.java com/x8zs/sandbox/ad/AdStubActivity

				.java com/x8zs/sandbox/ad/content/ContentManager.java com/x8zs/sandbox/ad/topon/ToponAdProvider.java com/x8zs/shell/AppInstallListener.java com/x8zs/shell/MainApplication.java com/x8zs/shell/ProxyApplication.java com/x8zs/shell/X8MiscApplication.java com/x8zs/ui/AppDetailActivity.java com/x8zs/ui/FeedbackActivity.java com/x8zs/ui/InjectActivity.java com/x8zs/ui/InstallOrInjectFlowActivity.java com/x8zs/ui/view/AppStateButton.java d1/b.java d1/f.java d1/l.java d1/m.java d1/o.java d1/r.java e/a.java g1/i.java g1/j.java g4/g.java h3/b.java i/p.java i4/a.java j4/d.java k2/h.java k2/m.java k2/n.java l1/a.java m2/i.java n1/k.java o0/g.java o2/b.java o2/f.java p0/a.java p1/a.java

				q0/a.java q0/d.java r/s.java r0/a.java s2/b.java t0/a.java t0/f.java t0/g.java t3/a.java u0/a.java u0/c.java u0/i.java u1/b.java u5/g.java v0/d.java w/f.java w0/e.java w0/i.java x0/a.java x4/k.java z0/f.java z0/n.java z0/o.java z5/a.java

2	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	com/applovin/impl/sdk/k.java com/applovin/mediation/ads/MaxAdView.java com/applovin/mediation/ads/MaxInterstitialAd.java com/applovin/mediation/ads/MaxRewardedAd.java com/applovin/mediation/ads/MaxRewardedInterstitialAd.java com/applovin/sdk/AppLovinSdk.java com/applovin/sdk/AppLovinWebViewActivity.java com/bykv/vk/openvk/component/video/a/b/i.java com/inmobi/media/ar.java com/inmobi/media/fd.java com/mbridge/msdk/MBridgeConstans.java com/mbridge/msdk/foundation/db/l.java com/mbridge/msdk/foundation/entity/CampaignEx.java com/mbridge/msdk/foundation/entity/m.java com/mbridge/msdk/foundation/same/report/c.java com/mbridge/msdk/playercommon/exoplayer2/drm/DefaultDrmSessionManager.java com/mbridge/msdk/video/dynview/endcard/moffer/MOfferModel.java com/mbridge/msdk/videocommon/download/a.java com/pgl/sys/ces/c/a.java com/pgl/sys/ces/c/b.java com/unity3d/ads/metadata/InAppPurchaseMetaData.java com/x8zs/BuildConfig.java com/x8zs/plugin/apache/commons/logging/LogFactory.java u1/b.java

3	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	com/apm/insight/h.java com/inmobi/media/al.java com/inmobi/media/ay.java com/mbridge/msdk/playercommon/exoplayer2/source/ShuffleOrder.java com/mbridge/msdk/playercommon/exoplayer2/trackselection/RandomTrackSelection.java com/mbridge/msdk/playercommon/exoplayer2/upstream/cache/CachedContentIndex.java com/mbridge/msdk/thrid/okhttp/OkHttpClient.java com/mbridge/msdk/thrid/okhttp/internal/ws/RealWebSocket.java com/mbridge/msdk/thrid/okhttp/internal/ws/WebSocketWriter.java com/unity3d/services/core/request/SDKMetrics.java com/x8zs/ui/main/SimpleSearchBar.java o2/f.java t/i.java

4	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	com/applovin/impl/adview/b.java com/mbridge/msdk/advanced/js/NativeAdvancedExpandDialog.java com/mbridge/msdk/click/f.java com/mbridge/msdk/mbbanner/common/bridge/BannerExpandDialog.java com/mbridge/msdk/mbbanner/common/c/c.java com/mbridge/msdk/nativex/view/MBMediaView.java com/mbridge/msdk/splash/signal/SplashExpandDialog.java com/mbridge/msdk/video/bt/module/MBridgeBTWebView.java com/mbridge/msdk/video/module/MBridgeAlertWebview.java com/mbridge/msdk/video/module/MBridgeH5EndCardView.java com/unity3d/services/core/webview/WebViewApp.java

5	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	com/apm/insight/entity/d.java com/apm/insight/l/w.java com/apm/insight/nativecrash/b.java com/apm/insight/runtime/o.java com/bykv/vk/openvk/component/video/api/e/a.java com/mbridge/msdk/foundation/same/report/b/a.java com/mbridge/msdk/foundation/tools/s.java com/pgl/sys/ces/a/a.java com/unity3d/services/core/cache/CacheDirectory.java com/x8zs/ad/AdManagerEx.java com/x8zs/model/X8DataModel.java com/x8zs/model/a.java com/x8zs/morgoo/droidplugin/MyCrashHandler.java com/x8zs/morgoo/helper/Log.java com/x8zs/plugin/utils/OSUtil.java com/x8zs/ui/SplashActivity.java com/x8zs/ui/task/BackupFragment.java k2/i.java l2/a.java o2/f.java w2/f.java

6	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/mbridge/msdk/playercommon/exoplayer2/util/Util.java
7	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	com/apm/insight/e/b/a.java com/apm/insight/e/b/b.java com/bykv/vk/openvk/component/video/a/b/b/d.java com/inmobi/media/gs.java com/mbridge/msdk/foundation/db/BatchReportDao.java com/mbridge/msdk/foundation/db/b.java com/mbridge/msdk/foundation/db/e.java com/mbridge/msdk/foundation/db/g.java com/mbridge/msdk/foundation/download/database/DatabaseHelper.java com/x8zs/model/X8DataModel.java k2/b.java

8	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	com/inmobi/media/o.java com/unity3d/services/ads/webplayer/WebPlayerView.java com/unity3d/services/core/webview/WebView.java
9	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	com/inmobi/media/cs.java com/mbridge/msdk/thrid/okhttp/internal/Util.java
10	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/applovin/impl/sdk/utils/StringUtils.java com/inmobi/media/hk.java com/pgl/sys/ces/c.java com/unity3d/services/core/device/Device.java j/f.java j2/c.java j2/d.java n0/n.java q5/g.java x5/b.java
11	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	com/mbridge/msdk/advanced/view/a.java com/x8zs/BuildConfig.java com/x8zs/shell/BuildConfig.java com/x8zs/shell/ProxyApplication.java com/x8zs/shell/XApp.java com/x8zs/ui/main/MainActivity.java s1/e.java

12	WebView域控制不严格漏洞	高危	CWE: CWE-73: 外部控制文件名或路径	com/mbridge/msdk/mbsignalcommon/base/BaseWebView.java com/unity3d/services/core/webview/WebView.java
13	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/apm/insight/l/v.java com/bykv/vk/openvk/component/video/api/e/b.java com/mbridge/msdk/foundation/download/resource/MBResourceManager.java com/mbridge/msdk/foundation/tools/SameMD5.java com/mbridge/msdk/foundation/tools/n.java com/x8zs/morgoo/helper/Utils.java com/x8zs/plugin/utils/MiscUtil.java com/x8zs/plugin/utils/PkgUtil.java k2/a.java k2/i.java o2/f.java w2/d.java
14	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	com/apm/insight/nativecrash/b.java
15	已启用远程WebView调试	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	com/applovin/impl/adview/d.java

动态库分析

序号	动态库	NX(堆栈禁止执行)	STACK CANARY(栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED（裁剪符号表）

1	armeabi-v7a/libantitrace.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。	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	False warning 符号可用

2	armeabi-v7a/libapminsighta.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。	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	False warning 符号可用

3	armeabi-v7a/libapminsightb.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。	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	False warning 符号可用

4	armeabi-v7a/libEncryptorP.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。	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	False warning 符号可用

5	armeabi-v7a/libnms.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。	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	False warning 符号可用

6	armeabi-v7a/libpkgparser.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。	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	False warning 符号可用

滥用权限

类型	匹配	权限

恶意软件常用权限	9/30	android.permission.SYSTEM_ALERT_WINDOW android.permission.REQUEST_INSTALL_PACKAGES android.permission.GET_TASKS android.permission.WAKE_LOCK android.permission.READ_PHONE_STATE android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.PACKAGE_USAGE_STATS android.permission.WRITE_SETTINGS
其它常用权限	10/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE android.permission.REORDER_TASKS android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS com.google.android.gms.permission.AD_ID

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

da.anythinktech.com	病毒 **URL:** da.anythinktech.com **IP:** N/A **Description:** Maltrail 标记的恶意域	是	**IP地址:** 47.107.73.83 **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
ads.inmobi.com	安全	否	**IP地址:** 20.157.16.64 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289987 **经度:** 103.850281 **查看:** Google 地图
i.l.inmobicdn.net	安全	是	**IP地址:** 152.199.39.108 **国家:** 中国 **地区:** 香港 **城市:** 香港 **纬度:** 22.285521 **经度:** 114.157692 **查看:** 高德地图
sf16-scmcdn-sg.ibytedtos.com	安全	否	**IP地址:** 23.33.33.176 **国家:** 日本 **地区:** 东京 **城市:** 东京 **纬度:** 35.689499 **经度:** 139.692322 **查看:** Google 地图

monetization-support.applovin.com	安全	否	**IP地址:** 34.110.151.135 **国家:** 美利坚合众国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
a.applovin.com	安全	否	**IP地址:** 34.117.147.68 **国家:** 美利坚合众国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
rt.applvn.com	安全	否	**IP地址:** 104.17.2.3 **国家:** 美利坚合众国 **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
ms.applvn.com	安全	否	**IP地址:** 104.17.2.3 **国家:** 美利坚合众国 **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
d.applvn.com	安全	否	**IP地址:** 104.17.1.3 **国家:** 美利坚合众国 **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

analytics.rayjump.com	安全	是	**IP地址:** 182.92.120.219 **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
unif-id.ssp.inmobi.com	安全	否	**IP地址:** 20.157.16.64 **国家:** 美利坚合众国 **地区:** 弗吉尼亚州 **城市:** 华盛顿 **纬度:** 38.713848 **经度:** -78.159439 **查看:** Google 地图
assets.applovin.com	安全	否	**IP地址:** 34.120.175.182 **国家:** 美利坚合众国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
api.x8zs.com	安全	是	**IP地址:** 182.92.120.219 **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
hb.rayjump.com	安全	是	**IP地址:** 112.126.29.58 **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

crash-metrics.sdk.inmobi.com	安全	否	**IP地址:** 34.120.175.182 **国家:** 美利坚合众国 **地区:** 弗吉尼亚州 **城市:** 华盛顿 **纬度:** 38.713848 **经度:** -78.159439 **查看:** Google 地图
www.x8speeder.com	安全	否	**IP地址:** 104.21.0.101 **国家:** 美利坚合众国 **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
api16-endcard-pack-sg.pangle.io	安全	否	**IP地址:** 23.45.50.163 **国家:** 日本 **地区:** 东京 **城市:** 东京 **纬度:** 35.689499 **经度:** 139.692322 **查看:** Google 地图
www.x8ds.com	安全	是	**IP地址:** 112.126.29.58 **国家:** 中国 **地区:** 江苏 **城市:** 南通 **纬度:** 32.030296 **经度:** 120.874779 **查看:** 高德地图
px.moatads.com	安全	否	**IP地址:** 23.207.173.242 **国家:** 日本 **地区:** 东京 **城市:** 东京 **纬度:** 35.689499 **经度:** 139.692322 **查看:** Google 地图

tk.anythinktech.com	安全	是	**IP地址:** 47.112.186.43 **国家:** 中国 **地区:** 广东 **城市:** 深圳 **纬度:** 22.545673 **经度:** 114.068108 **查看:** 高德地图
bds-sg.byteoversea.com	安全	否	**IP地址:** 103.136.220.205 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289987 **经度:** 103.850281 **查看:** Google 地图
net.rayjump.com	安全	是	**IP地址:** 112.126.29.58 **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
sdfp-sg.byteoversea.com	安全	否	**IP地址:** 23.45.51.25 **国家:** 日本 **地区:** 东京 **城市:** 东京 **纬度:** 35.689499 **经度:** 139.692322 **查看:** Google 地图
www.inmobi.com	安全	否	**IP地址:** 20.81.69.107 **国家:** 美利坚合众国 **地区:** 弗吉尼亚州 **城市:** 华盛顿 **纬度:** 38.713848 **经度:** -78.159439 **查看:** Google 地图

pangle-global.io	安全	否	**IP地址:** 103.224.182.252 **国家:** 澳大利亚 **地区:** 维多利亚 **城市:** 博马里斯 **纬度:** -37.982201 **经度:** 145.038940 **查看:** Google 地图
img.anythinktech.com	安全	否	**IP地址:** 13.225.131.60 **国家:** 大韩民国 **地区:** 京畿道 **城市:** Icheon **纬度:** 37.279179 **经度:** 127.442421 **查看:** Google 地图
d1tru86qrby720.cloudfront.net	安全	否	**IP地址:** 20.81.69.107 **国家:** 大韩民国 **地区:** 京畿道 **城市:** Icheon **纬度:** 37.279179 **经度:** 127.442421 **查看:** Google 地图
cn-adxtk.anythinktech.com	安全	否	No Geolocation information available.
cn-adx.anythinktech.com	安全	是	**IP地址:** 39.105.168.45 **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
log-mva.isnssdk.com	安全	否	**IP地址:** 23.45.50.192 **国家:** 日本 **地区:** 东京 **城市:** 东京 **纬度:** 35.689499 **经度:** 139.692322 **查看:** Google 地图

cn-da.anythinktech.com	安全	是	**IP地址:** 47.115.0.205 **国家:** 中国 **地区:** 广东 **城市:** 深圳 **纬度:** 22.545673 **经度:** 114.068108 **查看:** 高德地图
adxtk.anythinktech.com	安全	否	No Geolocation information available.
bds-va.byteoversea.com	安全	否	No Geolocation information available.
policy.rayjump.com	安全	是	**IP地址:** 112.126.23.181 **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
p16-sign-sg.tiktokcdn.com	安全	否	**IP地址:** 23.33.33.75 **国家:** 日本 **地区:** 东京 **城市:** 东京 **纬度:** 35.689499 **经度:** 139.692322 **查看:** Google 地图
lazy.rayjump.com	安全	是	**IP地址:** 49.71.77.86 **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

check.rayjump.com	安全	是	**IP地址:** 112.126.23.181 **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
cdn-adn-https.rayjump.com	安全	是	**IP地址:** 49.71.77.86 **国家:** 中国 **地区:** 江苏 **城市:** 扬州 **纬度:** 32.397221 **经度:** 119.435600 **查看:** 高德地图
log.sgsnssdk.com	安全	否	**IP地址:** 114.108.166.90 **国家:** 大韩民国 **地区:** 首尔teukbyeolsi **城市:** 首尔 **纬度:** 37.566311 **经度:** 126.977203 **查看:** Google 地图
d.applovin.com	安全	否	**IP地址:** 34.110.179.88 **国家:** 美利坚合众国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
cn-tk.anythinktech.com	安全	是	**IP地址:** 47.112.186.43 **国家:** 中国 **地区:** 广东 **城市:** 深圳 **纬度:** 22.545673 **经度:** 114.068108 **查看:** 高德地图
prod-a.applovin.comhttps	安全	否	No Geolocation information available.

sf-tb-sg.ibytedtos.com	安全	否	**IP地址:** 23.33.33.121 **国家:** 日本 **地区:** 东京 **城市:** 东京 **纬度:** 35.689499 **经度:** 139.692322 **查看:** Google 地图
z.moatads.com	安全	否	**IP地址:** 23.207.173.242 **国家:** 日本 **地区:** 东京 **城市:** 东京 **纬度:** 35.689499 **经度:** 139.692322 **查看:** Google 地图
x8speeder.com	安全	否	**IP地址:** 172.67.150.221 **国家:** 美利坚合众国 **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
cn-api.anythinktech.com	安全	是	**IP地址:** 47.112.152.30 **国家:** 中国 **地区:** 广东 **城市:** 深圳 **纬度:** 22.545673 **经度:** 114.068108 **查看:** 高德地图
api.anythinktech.com	安全	是	**IP地址:** 47.112.152.30 **国家:** 中国 **地区:** 广东 **城市:** 深圳 **纬度:** 22.545673 **经度:** 114.068108 **查看:** 高德地图

configure.rayjump.com	安全	是	**IP地址:** 112.126.23.181 **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
telemetry.sdk.inmobi.com	安全	否	**IP地址:** 20.39.59.149 **国家:** 美利坚合众国 **地区:** 弗吉尼亚州 **城市:** 华盛顿 **纬度:** 38.713848 **经度:** -78.159439 **查看:** Google 地图
sdfp-va.byteoversea.com	安全	否	**IP地址:** 114.108.166.80 **国家:** 大韩民国 **地区:** 首尔teukbyeolsi **城市:** 首尔 **纬度:** 37.566311 **经度:** 126.977203 **查看:** Google 地图
schemas.microsoft.com	安全	否	**IP地址:** 13.107.213.74 **国家:** 美利坚合众国 **地区:** 华盛顿 **城市:** 雷德蒙 **纬度:** 47.682899 **经度:** -122.120903 **查看:** Google 地图
config.inmobi.com	安全	否	**IP地址:** 20.39.59.188 **国家:** 美利坚合众国 **地区:** 弗吉尼亚州 **城市:** 华盛顿 **纬度:** 38.713848 **经度:** -78.159439 **查看:** Google 地图

a.applvn.com	安全	否	**IP地址:** 104.17.2.3 **国家:** 美利坚合众国 **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
pagead2.googlesyndication.com	安全	是	**IP地址:** 180.163.150.38 **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
lf-hs-sg.ibytedtos.com	安全	否	**IP地址:** 23.200.75.28 **国家:** 大韩民国 **地区:** 首尔teukbyeolsi **城市:** 首尔 **纬度:** 37.566311 **经度:** 126.977203 **查看:** Google 地图
p0.ipstatp.com	安全	否	**IP地址:** 18.244.61.44 **国家:** 美利坚合众国 **地区:** 华盛顿 **城市:** 西雅图 **纬度:** 47.627499 **经度:** -122.346199 **查看:** Google 地图
sf16-muse-va.ibytedtos.com	安全	否	**IP地址:** 72.246.103.16 **国家:** 大韩民国 **地区:** 首尔teukbyeolsi **城市:** 首尔 **纬度:** 37.566311 **经度:** 126.977203 **查看:** Google 地图

ms.applovin.com	安全	否	**IP地址:** 34.102.162.219 **国家:** 美利坚合众国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
schemas.applovin.com	安全	否	No Geolocation information available.
whatwg.org	安全	否	**IP地址:** 165.227.248.76 **国家:** 美利坚合众国 **地区:** 新泽西州 **城市:** 克利夫顿 **纬度:** 40.858585 **经度:** -74.163605 **查看:** Google 地图
config.unityads.unitychina.cn	安全	是	**IP地址:** 36.25.253.110 **国家:** 中国 **地区:** 浙江 **城市:** 湖州 **纬度:** 30.870550 **经度:** 120.093300 **查看:** 高德地图
config.unityads.unity3d.com	安全	否	**IP地址:** 18.67.51.83 **国家:** 大韩民国 **地区:** 京畿道 **城市:** Icheon **纬度:** 37.279179 **经度:** 127.442421 **查看:** Google 地图
adx.anythinktech.com	安全	是	**IP地址:** 39.105.168.45 **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

ulogs.umengcloud.com	安全	是	**IP地址:** 223.109.148.177 **国家:** 中国 **地区:** 江苏 **城市:** 南京 **纬度:** 32.061668 **经度:** 118.777992 **查看:** 高德地图
applovin.com	安全	否	**IP地址:** 18.67.51.83 **国家:** 美利坚合众国 **地区:** 得克萨斯州 **城市:** 奥斯丁 **纬度:** 30.271158 **经度:** -97.741699 **查看:** Google 地图
rt.applovin.com	安全	否	**IP地址:** 34.117.147.68 **国家:** 美利坚合众国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
vid.applovin.com	安全	否	**IP地址:** 34.160.64.118 **国家:** 美利坚合众国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图

网址

网址信息	源码文件

• https://x8speeder.com/ • https://www.facebook.com/x8speeder • https://www.x8ds.com/ • https://www.iana.org/assignments/media-types/	自研引擎-A
• 3.3.6.8	自研引擎-M
• http://schemas.applovin.com/android/1.0	com/applovin/adview/AppLovinAdView.java
• javascript:al_onfailedexpand • javascript:al_onadviewrendered	com/applovin/impl/adview/b.java
• javascript:al_onclosebuttontapped • javascript:al_onpoststitialdismiss • javascript:al_onbackpressed • javascript:al_onapppaused • javascript:al_onappresumed • javascript:al_muteswitchon • javascript:al_muteswitchoff • javascript:al_onwindowfocuschanged • javascript:al_onpoststitialshow	com/applovin/impl/adview/p.java
• javascript:al_onclosetapped • javascript:al_onbackpressed	com/applovin/impl/adview/w.java
• https://applovin.com	com/applovin/impl/mediation/debugger/ui/b/a.java
• data:a.data}};function	com/inmobi/media/eg.java
• https://ads.inmobi.com/sdk • https://i.l.inmobicdn.net/sdk/sdk/500/android/mraid.js • https://i.l.inmobicdn.net/sdk/sdk/omid/omsdk-v1.js	com/inmobi/media/fd.java
• https://config.inmobi.com/config-server/v1/config/secure.cfg	com/inmobi/media/fk.java

• https://crash-metrics.sdk.inmobi.com/trace	com/inmobi/media/fn.java
• https://config.inmobi.com/config-server/v1/config/secure.cfg	com/inmobi/media/fr.java
• https://unif-id.ssp.inmobi.com/fetch	com/inmobi/media/fs.java
• https://telemetry.sdk.inmobi.com/metrics	com/inmobi/media/ft.java
• http://www.google.com	com/inmobi/media/g.java
• https://www.inmobi.com/products/sdk/#downloads	com/inmobi/media/gz.java
• 127.0.0.1	com/mbridge/msdk/advanced/view/a.java
• http://whatwg.org/html/common-microsyntaxes.html#space-character • http://whatwg.org/html/webappapis.html#dom-windowbase64-atob • https://gist.github.com/atk/1020396 • http://whatwg.org/c#alphanumeric-ascii-characters • http://whatwg.org/html/webappapis.html#dom-windowbase64-btoa	com/mbridge/msdk/b/b/b.java
• https://play.google.com/	com/mbridge/msdk/click/a.java
• javascript:window.navigator.vibrate	com/mbridge/msdk/click/f.java
• https://{}hb.rayjump.com • https://analytics.rayjump.com • https://net.rayjump.com • https://configure.rayjump.com • https://d1tru86qrby720.cloudfront.net/hostsetting • https://policy.rayjump.com • https://lazy.rayjump.com • https://check.rayjump.com	com/mbridge/msdk/foundation/same/net/g/d.java

• https://play.google.com/store/apps/details?id= • https://play.google.com/	com/mbridge/msdk/foundation/tools/t.java
• javascript:window.mraidbridge.firereadyevent	com/mbridge/msdk/mbsignalcommon/mraid/a.java
• https://play.google.com	com/mbridge/msdk/mbsignalcommon/windvane/WindVaneWebView.java
• https://z.moatads.com/' • https://z.moatads.com/	com/moat/analytics/mobile/inm/g.java
• javascript:%s.dispatchmany	com/moat/analytics/mobile/inm/j.java
• https://px.moatads.com/pixel.gif?e=0&i=moatsdk1&ac=1	com/moat/analytics/mobile/inm/m.java
• https://z.moatads.com/	com/moat/analytics/mobile/inm/w.java
• https://bds-va.byteoversea.com • https://bds-sg.byteoversea.com • https://sdfp-va.byteoversea.com • https://sdfp-sg.byteoversea.com	com/pgl/a/a/a.java
• javascript:window.nativebridge.receiveevent	com/unity3d/services/ads/webplayer/WebPlayerView.java
• https://config.unityads.unitychina.cn/webview/ • https://config.unityads.unity3d.com/webview/	com/unity3d/services/core/properties/SdkProperties.java
• 3.3.6.8 • https://x8speeder.com/?p=94	com/x8zs/BuildConfig.java
• 3.3.6.8	com/x8zs/apkbuilder/ApkBuilder.java

• https://api.x8zs.com/api/feedback/ • https://api.x8zs.com/api/viewsconfig/ • https://api.x8zs.com/api/appdetail/?aid= • https://api.x8zs.com/api/carousel/ • https://api.x8zs.com/api/getlatestappinfo/ • https://api.x8zs.com/api/comconf/ • https://api.x8zs.com/api/abnormal/?page= • https://api.x8zs.com/api/search/?q= • https://api.x8zs.com/api/gamesfilter/ • https://api.x8zs.com/api/hotacc/ • https://api.x8zs.com/api/ranklist/?t= • https://api.x8zs.com/api/runrule/ • https://api.x8zs.com/api/latestrelease/?p= • https://api.x8zs.com/api/shellrulev2/ • https://api.x8zs.com/api/keywords/ • https://api.x8zs.com/api/patchlog/ • https://api.x8zs.com/api/notgame/ • https://api.x8zs.com/api/apps/	com/x8zs/model/ServerApi.java
• https://www.facebook.com/x8speeder	com/x8zs/plugin/utils/SocialUtil.java
• https://www.x8ds.com/ • https://x8speeder.com/	com/x8zs/shell/AppInstallListener.java
• 3.3.6.8	com/x8zs/shell/BuildConfig.java
• 3.3.6.8	com/x8zs/shell/ProxyApplication.java
• 3.3.6.8	com/x8zs/shell/XApp.java
• https://www.x8ds.com/?p=50 • https://x8speeder.com/?p=12	com/x8zs/ui/b.java
• 3.3.6.8	com/x8zs/ui/main/MainActivity.java
• https://ms.applovin.com/ • https://ms.applvn.com/	j0/a.java

• https://assets.applovin.com/gdpr/flow_v1/gdpr-flow-1.html • https://prod-a.applovin.com,https://rt.applovin.com/4.0/pix • https://rt.applvn.com/4.0/pix,https://ms.applovin.com/,https://ms.applvn.com/ • https://ms.applovin.com/ • https://ms.applvn.com/ • https://a.applovin.com/ • https://a.applvn.com/ • https://d.applovin.com/ • https://d.applvn.com/ • https://rt.applovin.com/ • https://rt.applvn.com/ • https://vid.applovin.com/,https://pdn.applovin.com/,https://img.applovin.com/,https://d.applovin.com/,https://assets.applovin.com/,https://cdnjs.cloudflare.com/,http://vid.applovin.com/,http://pdn.applovin.com/,http://img.applovin.com/,http://d.applovin.com/,http://assets.applovin.com/,http://cdnjs.cloudflare.com/	j0/b.java
• https://monetization-support.applovin.com/hc/en-us/articles/236114328-how-can-i-expose-verbose-logging-for-the-sdk	l0/o.java
• https://api.x8zs.com/api/updateapk/	m2/i.java
• https://www.facebook.com/x8speeder	o2/f.java
• https://play.google.com/store/apps/details?id=	q1/b.java
• javascript:al_muteswitchon • javascript:al_muteswitchoff • javascript:al_onclosebuttontapped • javascript:al_onwindowfocuschanged • javascript:al_onappresumed • javascript:al_onapppaused • javascript:al_onpoststitialdismiss • javascript:onbackpressed	w/a.java
• javascript:al_onpoststitialshow	w/b.java

• javascript:al_onpoststitialshow	w/e.java
• javascript:al_onpoststitialshow	w/f.java
• javascript:al_showpostitial • javascript:al_setvideomuted	w/g.java
• https://www.x8ds.com/?p=50 • javascript:al_onapppaused • https://api.x8zs.com/api/runrule/ • http://whatwg.org/html/common-microsyntaxes.html#space-character • http://whatwg.org/html/webappapis.html#dom-windowbase64-atob • https://gist.github.com/atk/1020396 • http://whatwg.org/c#alphanumeric-ascii-characters • http://whatwg.org/html/webappapis.html#dom-windowbase64-btoa • https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps • javascript:al_onclosebuttontapped • https://ms.applovin.com/ • https://{}hb.rayjump.com • https://z.moatads.com/' • 3.2.0.4 • data:a.data}};function • https://px.moatads.com/pixel.gif?e=0&i=moatsdk1&ac=1 • javascript:al_muteswitchon • https://a.applovin.com/ • https://adx.anythinktech.com/request • https://api.x8zs.com/api/carousel/ • javascript:al_setvideomuted • https://api.x8zs.com/api/gamesfilter/ • https://cn-da.anythinktech.com/v1/open/da • https://ads.inmobi.com/sdk • https://api.x8zs.com/api/comconf/ • https://d1tru86qrby720.cloudfront.net/hostsetting • https://config.unityads.unity3d.com/webview/ • https://api.x8zs.com/api/shellrulev2/ • 10.0.0.200 • https://cn-api.anythinktech.com/v1/open/app • javascript:al_onclosetapped	

- www.x8speeder.com
- https://unif-id.ssp.inmobi.com/fetch
- https://cn-tk.anythinktech.com/v1/open/tk
- https://bds-sg.byteoversea.com
- https://ms.applvn.com/
- javascript:al_onpoststitialdismiss
- javascript:al_showpostitial
- javascript:window.mraidbridge.firereadyevent
- https://assets.applovin.com/gdpr/flow_v1/gdpr-flow-1.html
- https://cn-adx.anythinktech.com/request
- https://rt.applovin.com/
- https://bds-va.byteoversea.com
- https://a.applvn.com/
- https://img.anythinktech.com/gdpr/privacypolicysetting.html
- https://configure.rayjump.com
- https://cn-api.anythinktech.com/v1/open/area
- https://api.anythinktech.com/v1/open/placement
- 4.1.1.8
- https://api.x8zs.com/api/search/?q=
- 3.3.6.8
- https://i.l.inmobicdn.net/sdk/sdk/omid/omsdk-v1.js
- https://telemetry.sdk.inmobi.com/metrics
- https://cdn-adn-https.rayjump.com/cdn-adn/v2/portal/19/08/20/11/06/5d5b63cb457e2.js
- https://tk.anythinktech.com/ss/rrd
- https://play.google.com/
- https://api.x8zs.com/api/hotacc/
- javascript:window.navigator.vibrate
- javascript:al_muteswitchoff
- https://lf-hs-sg.ibytedtos.com/obj/union-platform-i18n/union_platform_gdpr_607_en.html
- https://api.x8zs.com/api/keywords/
- 3.9.0.5
- 10.0.0.172
- https://ulogs.umengcloud.com
- https://sdfp-va.byteoversea.com
- javascript:al_onfailedexpand
- https://api.x8zs.com/api/notgame/
- https://rt.applvn.com/
- https://d.applovin.com/
- https://config.inmobi.com/config-server/v1/config/secure.cfg
- https://www.facebook.com/x8speeder
- javascript:%s.dispatchmany

• javascript:window.nativebridge.receiveevent • https://cn-adx.anythinktech.com/bid • https://api.x8zs.com/api/latestrelease/?p= • https://z.moatads.com/ • 127.0.0.1 • https://applovin.com • https://play.google.com • https://lazy.rayjump.com • https://api.x8zs.com/api/updateapk/ • javascript:al_onappresumed • https://pangle-global.io/ • https://plus.google.com/ • http://schemas.applovin.com/android/1.0 • https://cn-tk.anythinktech.com/ss/rrd • https://api.x8zs.com/api/patchlog/ • javascript:onbackpressed • https://api.x8zs.com/api/ranklist/?t= • https://prod-a.applovin.com,https://rt.applovin.com/4.0/pix • https://rt.applvn.com/4.0/pix,https://ms.applovin.com/,https://ms.applvn.com/ • https://x8speeder.com/?p=12 • javascript:al_onpoststitialshow • https://log-mva.isnssdk.com/service/2/app_log/ • https://p0.ipstatp.com/origin/ad-site-i18n-sg/202011255d0d219920adb0fd474eac28 • https://p0.ipstatp.com/origin/v0201/fd71964ced204df586b63b9d8fa3198a.webp • https://p16-sign-sg.tiktokcdn.com/v0201/fd71964ced204df586b63b9d8fa3198a~tplv-noop.image?x-expires=1618223773&x-signature=kfdr%2fbhupok2d9%2byonsv0inuemk%3d • https://api16-endcard-pack-sg.pangle.io/union/endcard/1695802627329057/?rit=901121365&req_id=68ebda22-9cbd-423f-98ce-78f571b6308bu5599&ad_sdk_version=3.6.0.0&os=android&lang=zh&union_imei=702f89a658bd1f189c6e8e24587cd9ce&app_version=%e8%a1%a5%e5%85%85%e4%b8%ad&app_name=&developer_name=%e8%a1%a5%e5%85%85%e4%b8%ad%ef%bc%8c%e5%8f%af%e4%ba%8e%e5%ba%94%e7%94%a8%e5%ae%98%e7%bd%91%e6%9f%a5%e7%9c%8b&is_dsp=false&lpt=1&style_id=1535776&comment_num=92&like_num=109&share_num=96 • https://sf16-scmcdn-sg.ibytedtos.com/obj/goofy-sg/ad/pangle/homepage/_next/static/assets/images/reward.c7cdf2f9.mp4 • javascript:al_onadviewrendered • https://da.anythinktech.com/v1/open/da	自研引擎-S

- https://policy.rayjump.com
- javascript:al_onbackpressed
- https://www.x8ds.com/?p=1043
- https://www.x8ds.com/?p=1038
- http://x8speeder.com
- https://api.x8zs.com/api/appdetail/?aid=
- https://log.sgsnssdk.com/service/2/app_log/
- https://cn-adx.anythinktech.com/openapi/req
- https://api.x8zs.com/api/abnormal/?page=
- https://sf16-muse-va.ibytedtos.com/obj/ad-pattern-va/renderer/package_va.json
- https://api.anythinktech.com/v1/open/area
- https://i.l.inmobicdn.net/sdk/sdk/500/android/mraid.js
- https://net.rayjump.com
- https://x8speeder.com/?p=94
- https://cn-api.anythinktech.com/v1/open/placement
- https://monetization-support.applovin.com/hc/en-us/articles/236114328-how-can-i-expose-verbose-logging-for-the-sdk
- https://api.x8zs.com/api/getlatestappinfo/
- https://check.rayjump.com
- https://sdfp-sg.byteoversea.com
- https://api.x8zs.com/api/feedback/
- https://tk.anythinktech.com/v1/open/tk
- https://config.unityads.unitychina.cn/webview/
- https://cn-api.anythinktech.com/v1/open/eu
- https://play.google.com/store/apps/details?id=
- https://api.x8zs.com/api/viewsconfig/
- https://adxtk.anythinktech.com/v1
- javascript:al_onwindowfocuschanged
- https://crash-metrics.sdk.inmobi.com/trace
- https://adx.anythinktech.com/bid
- https://sf-tb-sg.ibytedtos.com/obj/ad-pattern-sg/renderer/package_sg.json
- https://adx.anythinktech.com/openapi/req
- https://www.inmobi.com/products/sdk/#downloads
- https://vid.applovin.com/,https://pdn.applovin.com/,https://img.applovin.com/,https://d.applovin.com/,https://assets.applovin.com/,https://cdnjs.cloudflare.com/,http://vid.applovin.com/,http://pdn.applovin.com/,http://img.applovin.com/,http://d.applovin.com/,http://assets.applovin.com/,http://cdnjs.cloudflare.com/
- https://api.anythinktech.com/v1/open/app
- https://analytics.rayjump.com
- https://api.anythinktech.com/v1/open/eu

• https://cn-adxtk.anythinktech.com/v1 • http://www.google.com • https://d.applvn.com/ • https://api.x8zs.com/api/apps/	

第三方SDK

SDK名称	开发者	描述信息
EasyProtector	lamster2018	一行代码检测 XP/调试/多开/模拟器/root。
APMInsight / 应用性能监控全链路版	Volcengine (火山引擎)	应用性能监控全链路版是火山引擎提供的针对应用服务的品质、性能以及自定义埋点的 APM 服务。应用性能监控全链路版可帮助客户发现多类异常问题，并及时报警，做分配处理，同时平台提供了丰富的归因能力，包括且不限于堆栈分析、调度分析、维度分析、埋点分析、单点日志查询等，结合灵活的报表能力可了解各类指标的趋势变化。更多功能介绍，详见各子监控服务的功能模块说明。
Pangle SDK	ByteDance	穿山甲是巨量引擎旗下全球应用变现与增长平台，合作优质媒体超 30,000 家，日请求突破 607 亿，日均展示达 100 亿，覆盖 7 亿日活用户，为全球应用和广告主提供高效的用户增长和变现解决方案。
岳鹰全景监控	Alibaba	岳鹰全景监控，是阿里 UC 官方出品的先进移动应用线上监控平台，为多家知名企业提供服务。
android-gif-drawable	koral--	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。
移动统计分析	Umeng	U-App 作为一款专业、免费的移动统计分析产品。在日常业务中帮您解决多种数据相关问题，如数据采集与管理、业务监测、用户行为分析、App 稳定性监控及实现多种运营方案等。助力互联网企业充分挖掘用户行为数据价值，找到产品更新迭代方向，实现精细化运营，全面提升业务增长效能。
AndroidUtilCode	Blankj	AndroidUtilCode 是一个强大易用的安卓工具类库，它合理地封装了安卓开发中常用的函数，具有完善的 Demo 和单元测试，利用其封装好的 APIs 可以大大提高开发效率。

Unity Ads	Unity Technologies	Unity Ads SDK 由领先的移动游戏引擎创建，无论您是在 Unity、xCode 还是 Android Studio 中进行开发，都能为您的游戏提供全面的变现服务框架。
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。库开发人员和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。
AppLovin	AppLovin	AppLovin 为移动游戏开发者提供变现、游戏发行、分析和业务发展等全方位服务。AppLovin 的营销平台和分析套件帮助开发者获取新用户并最大化营收能力，旗下独立运营的媒介部门 Lion Studios 为开发者的游戏发行和推广提供可靠的资源。
Picasso	Square	一个强大的 Android 图片下载缓存库。

邮箱

EMAIL	源码文件
framework@boot.oat	o2/f.java
framework@boot.oat	自研引擎-S

追踪器

名称	类别	网址
AppLovin (MAX and SparkLabs)	Analytics, Profiling, Identification, Advertisement	https://reports.exodus-privacy.eu.org/trackers/72

IAB Open Measurement	Identification, Advertisement	https://reports.exodus-privacy.eu.org/trackers/328
Inmobi		https://reports.exodus-privacy.eu.org/trackers/106
Mintegral	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/200
Moat	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/61
Pangle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/363
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119
Unity3d Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/121
Yueying Crash SDK	Crash reporting, Analytics	https://reports.exodus-privacy.eu.org/trackers/448

🔑 密钥凭证

可能的密钥
"anythink_myoffer_feedback_violation_of_laws" : "Illegal"
0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78
DFKwWgtuDkKwLZPwD+z8H+N/xj26Vjcdx5KanjKnxVN=
appwB9eJrCeo7nVPl2wizRu5MBk=
609390b853b6726499eb44a2

Uo5Y0Q4Z1gIsQqLXLPyZA5NJ+H4FBqaXIScaigHJEb8=
ySbKB1Je0gprhfpajdfDRMnvkT4=
q8sT2eKqr1KMUdoGOvkCFk0ZHSo=
3A0+kbNR4TZHPi66PzKd/2+HUe6h+5RXTmJRMMAeZG8=
936dcbdd57fe235fd7cf61c2e93da3c4
Y29tLmFuZHJvaWQudmVuZGluZy5saWNlbnNpbmcuSUxpY2Vuc2luZ1NlcnZpY2U=
aQiXYXDxj9INlSqgQzBlGWFZJzawcLNWKha1PV5aceA=
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
DFKwWgtuDkKwLZPwD+z8H+N/xj26Vjcdx5KyVj5GxVN=
HSrCHRtOan6wp2kwOIGJC1RDtuSrF2mWVbio2aBcMHX9KF3iTJ1lLSzCKP1ZSo5yNolPNw1kCTtWpxELFF4ah1
8f1d08a2d6496191a5ebae8f0590f513e2619489
92762936dcbdd57fe235fd7cf61c2e93da3c4
c334ae83accfebb8da23104450c896463c9cfab7
DFKwWgtuDkKwLZPwD+z8H+N/xjQZxVfV+T2SZVe6V2xS5c5n

3082033b30820223a003020102020467094 22c300d06092a864886f70d01010b0500304e310b300906035504061302353 1310b3009060355040813023531310b3009060355040713023531310b3009060355040a13023531310b3009060355040b13023531310b3009060355040313023531301e170d313531313239303831323134 5a170d343330343136303831323134 5a304e310b3009060355040613023531310b3009060355040813023531310b3009060355040713023531310b3009060355040a13023531310b3009060355040b13023531310b3009060355040313023531308201223 00d06092a864886f70d01010105000382010f003082010a0282010100d1cdf71fa6254da5a2fa99ce20e4863e40db4e1531ca8cff3c5a1029b492b1244ef0196f09cea1d06191264c1d1b7053b9ce913f1d25ecec98df26fb712971b8f0a4253be3089b28314579e5dd6a58a6fec914536188a1c01ff0d0321077783a0eea10051bc1522bf7ff27d2a91d294ebd103f9c7f30228087c0a3b8dc08af0eabf8bcc0659504df603484213ac7cecc84e647c3b028b7d4b8dded55e2d4edc2e922e6696698d265088ca7ad6bf4e6f782777e56238fe67683d44fd0de37fe580e072324ab0382da9ad7881b5cce4ccf7a79b20392d2430e24c1094e1d731ac0a0bcca90b025a36330507e085915f7bd5f887a7ef4fca579beaca3cf8df155570203010001a321301f301d0603551d0e041604145f7725d45df0f5588610ad238f5e2fd483cc563f300d06092a864886f70d01010b05000382010100017bf40f88c99841ba38793da7347df8f1794facaf15d6945672086d9c3dc24d0f478af189c3800c0af2f8faef6106644e0ac6fa23901d2ee85490c7c3ce2757d2032da91661ba832d94ff5ec7df948b79b0e572698ef8e67648751c4f84e3ae443a40be16a384fb27c2c310476772be62313d4991dd75886f7a54a81799488e1f0f2ef8824319deb02f3fef70610ebe733139f3665fac764f826ce98b997ab0bef3f5e1e9b7826f8b950350a2e38780b1e48ca2c622c630e502f9fff3b7425223b0c7a161ec7506ac8efa4f700a3e51c3347ef8da73614eef90126ab18599bf3762de491188cf046ded1ca383c812addef456f78be83d4d0a8fe40ccba0c48b
08C424D49777D5A45AFB89A06DA6F798
E72409364B865B757E1D6B8DB73011BBB1D20C1A9F931ADD3C4C09E2794CE102F8AA7F2D50EB88F9880A576E6C7B0E95712CAE9416F7BACB798564627846E93B
b3a5feea12676085ecfa0c2d0594a781
EV5iFShcCXFyNKonSsCu+eEPb+vZyPzr7TLOKOnPGkc=

免责声明及风险提示:

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

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