南明离火
移动应用检测平台

ANDROID 静态分析报告

红AR辅 助 器 • v1.96.00

分析日期: 2024-06-07 09:25:11

应用概览

文件名称:	com.saturn.foundation.disorientation_dad9f973.apk
文件大小:	9.4MB
应用名称:	红AR辅 助 器
软件包名:	com.Saturn.foundation.disorientation
主活动:	com.foundation.disorientation.start.SplashActivity
版本号:	1.96.00
最小SDK:	21
目标SDK:	28
加固信息:	未加壳
应用程序安全分数:	39/100 (高风险)
跟踪器检测:	2/432
杀软检测:	13 个杀毒软件报毒
MD5:	5510369350f1c291df829258eec612ae
SHA1:	6c3fc54eb1860f1540c03379f9[illegible]3550[illegible]ff723d4
SHA256:	c6bc2263010533b3b4e21[illegible]9b5ced5b302ddbb3c8e312d4175015ccc1d4595b8

分析结果严重性分布

高危	中危	信息	安全	关注
4	5	1	0	15

四大组件导出状态统计

Activity组件：68个，其中export的有：1个
Service组件：8个，其中export的有：0个
Receiver组件：2个，其中export的有：2个
Provider组件：1个，其中export的有：0个

应用签名证书信息

二进制文件已签名

v1 签名: True
v2 签名: False
v3 签名: False
v4 签名: False
主题: C=CN, ST=GD, L=Guangzhou, O=Tencent, OU=3G, CN=WilsonWu
签名算法: rsassa_pkcs1v15
有效期自: 2023-04-12 08:58:38+00:00
有效期至: 2570-11-10 08:58:38+00:00
发行人: C=CN, ST=GD, L=Guangzhou, O=Tencent, OU=3G, CN=WilsonWu
序列号: 0xc8c3118
哈希算法: sha256
证书MD5: 68869ab3d78295412dcef8f157320773
证书SHA1: 3a077304cf1fd3870afa54c8a986303a694791c4
证书SHA256: 5c77c01a584207f1c47739bd3a9deec36e798a8ae6cfaf66935ffd837cbab143
证书SHA512:
5fa5c3b0bbca42fa3efdcbec13882951ea24f0ebbab7feae3c7b14745c74b4da6deaba6f9ca5276c8a3409eba6a2364f6b201c71e094d6d8eedb930544f714a5

找到 1 个唯一证书

权限声明与风险分级

权限名称	安全等级	权限内容	权限描述
android.permission.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.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
android.permission.ACCESS_NETWORK_STATE	普通	获取网络状态	允许应用程序查看所有网络的状态。
android.permission.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.READ_PRIVILEGED_PHONE_STATE	未知	未知权限	来自 android 引用的未知权限。
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储。
android.permission.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
android.permission.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_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.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.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.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.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.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.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。
com.Saturn.foundation.disorientation.permission.KW_SDK_BROADCAST	未知	未知权限	来自 android 引用的未知权限。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
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。
freemme.permission.msa	未知	未知权限	来自 android 引用的未知权限。
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）

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全合规分析

高危: **1** | 警告: **0** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序已使用代码签名证书进行签名
应用程序存在Janus漏洞	高危	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

Manifest 配置安全分析

高危: **0** | 警告: **4** | 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 5.0-5.0.2, [minSdk=21]	信息	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	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，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。
3	Broadcast Receiver (com.foundation.disorientation.mod.service.MammonReceiver) 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。

4	Broadcast Receiver (com.anythink.china.common.NotificationBroadcaseReceiver) 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。
5	Activity (com.kwad.sdk.api.proxy.app.BaseFragmentActivity$RequestInstallPermissionActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。

代码安全漏洞检测

高危: **2** | 警告: **9** | 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-STORAGE-3	升级会员：解锁高级权限
2	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限
3	文件可能包含硬编码的敏感信息，如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
4	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	升级会员：解锁高级权限
5	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	升级会员：解锁高级权限

6	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
7	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
8	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
9	该文件是World Writable。任何应用程序都可以写入文件	高危	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
10	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	升级会员：解锁高级权限
11	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
12	应用程序使用不安全的随机数发生器	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

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED(裁剪符号表)
1	armeabi-v7a/libPlatform.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。		False high 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项-fstack-protector-all来启用栈哨兵。这对于Dart/Flutter库不适用，除非使用了Dart FFI	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/libsgcore.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/libString.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。		False high 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项 -fstack-protector-all 来启用栈哨兵。这对于 Dart/Flutter 库不适用，除非使用了 Dart FFI	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	7/30	android.permission.READ_PHONE_STATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.GET_TASKS android.permission.WAKE_LOCK android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.VIBRATE

本报告由南明离火移动安全分析平台生成

其它常用权限	9/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.CHANGE_NETWORK_STATE android.permission.REORDER_TASKS com.google.android.gms.permission.AD_ID 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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
da.anythinktech.com	病毒 **URL:** da.anythinktech.com **IP:** NA **Description:** Maltrail 标记的恶意域	是	**IP地址:** 117.91.199.31 **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:** 117.91.199.31 **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
www.toponad.com	安全	是	**IP地址:** 42.192.176.82 **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
static.yximgs.com	安全	是	**IP地址:** 117.91.199.31 **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
pitk.bird...	安全	是	**IP地址:** 117.91.199.31 **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

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
adxtk.anythinktech.com	安全	否	No Geolocation information available.
p1-lm.adkwai.com	安全	是	**IP地址:** 117.91.199.31 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492163 **经度:** 119.970767 **查看:** 高德地图
open.e.kuaishou.com	安全	是	**IP地址:** 117.91.199.31 **国家:** 中国 **地区:** 江苏 **城市:** 无锡 **纬度:** 31.569349 **经度:** 120.288738 **查看:** 高德地图
adx.anythinktech.com	安全	是	**IP地址:** 117.91.199.31 **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
img.toponad.com	安全	否	**IP地址:** 13.225.131.123 **国家:** 大韩民国 **地区:** 京畿道 **城市:** 利川市 **纬度:** 37.279179 **经度:** 127.442421 **查看:** Google 地图
apps.samsung.com	安全	是	**IP地址:** 49.79.233.19 **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
tk.anythinktech.com	安全	是	**IP地址:** 117.91.199.31 **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

aa.birdgesdk.com	安全	是	**IP地址:** 117.91.199.31 **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
ulogs.umengcloud.com	安全	是	**IP地址:** 117.91.199.31 **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
mores.toponad.com	安全	是	**IP地址:** 117.91.199.31 **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
cdn-adn-https.rayjump.com	安全	是	**IP地址:** 61.147.211.151 **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
img.anythinktech.com	安全	否	**IP地址:** 13.225.131.8 **国家:** 大韩民国 **地区:** 京畿道 **城市:** 利川市 **纬度:** 37.279179 **经度:** 127.442421 **查看:** Google 地图
qq.ahaozhuan.com	安全	是	**IP地址:** 47.107.40.90 **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

URL 链接安全分析

URL信息	源码文件
• https://github.com/lingochamp/filedownloader/wiki/filedownloader.properties	com/kwai/filedownloader/services/a.java
• https://github.com/lingochamp/filedownloader/wiki/filedownloader.properties	b/g/a/p0/a.java
• https://aa.birdgesdk.com/v1/d_api • https://ptk.birdgesdk.com/v1/ptk	b/h/a/a/a/a.java
• https://qq.ahaozhuan.com/wodezhubogongsi/	b/d/a/f/a.java

- https://img.anythinktech.com/gdpr/privacypolicysetting.html
- https://tk.anythinktech.com/ss/rrd
- https://static.yximgs.com/udata/pkg/ks-android-ksadsdk/adlive/3.3.26.1/ks_so-adlivearm64v8arelease-3.3.26.1.apk
- http://apps.samsung.com/appquery/appdetail.as?appid=
- https://img.toponad.com/sdk/app-permissions.html?key=
- https://gist.github.com/atk/1020396
- http://%s:%d/%s
- https://adx.anythinktech.com/openapi/req
- http://da.anythinktech.com/v1/open/da
- http://adx.anythinktech.com/bid
- https://mores.toponad.com/image/default/mintegral_logo.png
- http://api.anythinktech.com/v2/open/placement
- https://static.yximgs.com/udata/pkg/ks-android-ksadsdk/tachikoma/3.3.34/ks_so-tachikomasoarmeabiv7arelease-3.3.34.apk
- javascript:window.navigator.vibrate
- https://adx.anythinktech.com/request
- https://aa.birdgesdk.com/v1/d_api
- 10.0.0.200
- https://static.yximgs.com/udata/pkg/ks-android-ksadsdk/ks_so-appstatusarmeabiv7arelease-3.3.14.apk
- http://whatwg.org/html/webappapis.html#dom-windowbase64-btoa
- https://pitk.birdgesdk.com/v1/ptk
- https://adxtk.anythinktech.com/v1
- 10.0.0.172
- https://ulogs.umengcloud.com
- http://api.anythinktech.com/v2/open/app
- https://play.google.com/
- https://static.yximgs.com/udata/pkg/ks-android-ksadsdk/tachikoma/3.3.34/ks_so-tachikomalitesoarmeabiv7arelease-3.3.34.apk
- https://cdn-adn-https.rayjump.com/cdn-adn/v2/portal/19/08/20/11/06/5d5b63cb457e2.js
- http://whatwg.org/html/webappapis.html#dom-windowbase64-atob
- javascript:window.mraidbridge.firereadyevent
- https://play.google.com/store/apps/details?id=
- https://static.yximgs.com/udata/pkg/ks-android-ksadsdk/adlive/3.3.26.1/ks_so-adlivearmeabiv7arelease-3.3.26.1.apk
- 3.3.38.1
- https://static.yximgs.com/udata/pkg/ks-android-ksadsdk/ks_so-appstatusarm64v8arelease-3.3.14.apk
- http://whatwg.org/c#alphanumeric-ascii-characters
- https://static.yximgs.com/udata/pkg/ks-android-ksadsdk/ks_so-exceptionarm64v8arelease-3.3.23.apk
- https://static.yximgs.com/udata/pkg/ks-android-ksadsdk/tachikoma/3.3.34/ks_so-tachikomalitesoarm64v8arelease-3.3.34.apk
- http://api.anythinktech.com/v2/open/eu
- https://adx.anythinktech.com/bid
- http://tk.anythinktech.com/ss/rrd
- https://play.google.com
- http://www.toponad.com
- http://adx.anythinktech.com/openapi/req
- http://whatwg.org/html/common-microsyntaxes.html#space-character
- https://p1-lm.adkwai.com/udata/pkg/ks-android-ksadsdk/offline_components/tk/ks_so-tachikomanosorelease-3.3.38.1-a469423ad-256.zip
- https://p1-lm.adkwai.com/udata/pkg/ks-android-ksadsdk/offline_components/adlive/ks_so-adlivenosorelease-3.3.38-9333b7151-254.zip
- https://api.anythinktech.com/v2/open/app
- https://github.com/lingochamp/filedownloader/wiki/filedownloader.properties
- 3.2.0.4
- https://qq.ahaozhuan.com/wodezhubogongsi/
- https://tk.anythinktech.com/v1/open/tk
- http://adxtk.anythinktech.com/v1
- https://static.yximgs.com/udata/pkg/ks-android-ksadsdk/offline_components/obiwan/ks_so-obiwannosorelease-3.3.34-773cd6541-80.zip
- http://tk.anythinktech.com/v1/open/tk
- https://api.anythinktech.com/v2/open/placement

自研引擎-S

本报告由南明离火移动安全分析平台生成

• 6.1.55.1 • http://adx.anythinktech.com/request • http://api.anythinktech.com/v2/open/area • https://static.yximgs.com/udata/pkg/ks-android-ksadsdk/tachikoma/3.3.34/ks_so-tachikomasoarm64v8arelease-3.3.34.apk • https://api.anythinktech.com/v2/open/area • https://open.e.kuaishou.com/rest/e/v3/open/sdk2 • https://static.yximgs.com/udata/pkg/ks-android-ksadsdk/ks_so-exceptionarmeabiv7arelease-3.3.23.apk • 10.244.154.152 • https://da.anythinktech.com/v1/open/da • https://api.anythinktech.com/v2/open/eu • 127.0.0.1	

第三方 SDK 组件分析

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。
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。
阿里聚安全	Alibaba	阿里聚安全是面向开发者，以移动应用安全为核心的开放平台。
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。
快手广告 SDK	快手	快手信息流广告为您和用户搭建桥梁。
腾讯广告 SDK	Tencent	腾讯广告汇聚腾讯公司全量的应用场景，拥有核心行业数据、营销技术与专业服务能力。
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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
FileDownloader	LingoChamp	Android 文件下载引擎，稳定、高效、灵活、简单易用。

邮箱地址敏感信息提取

EMAIL	源码文件
.apk@classes.dex	自研引擎-S

第三方追踪器检测

名称	类别	网址
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119
Yueying Crash SDK	Crash reporting, Analytics	https://reports.exodus-privacy.eu.org/trackers/448

敏感凭证泄露检测

可能的密钥
"dyStrategy.privateAddress" : "privateAddress"
"anythink_myoffer_feedback_violation_of_laws" : "Illegal"
b496f2beb340c9b0065ce3f825109f1c
60b981e1799cce47f934505d

免责声明及风险提示: