



ANDROID 静态分析报告



◆ Coloring Book • v1.2.5

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: 2025-03-10 22:45:23

i应用概览

文件名称:	Coloring Book v1.2.5.apk
文件大小:	23.22MB
应用名称:	Coloring Book
软件包名:	com.dtnntech.kidsacademy.coloringbook
主活动:	org.cocos2dx.cpp.AppActivity
版本号:	1.2.5
最小SDK:	21
目标SDK:	33
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	42/100 (中风险)
跟踪器检测:	6/432
杀软检测:	经检测, 该文件安全
MD5:	5a62c962a272b920cefc25f46ca80e6e
SHA1:	509abe20db2453ed4fbb9d150d463b967b34fe8d
SHA256:	a1aab73c3a394250c0a4b2e349ab16627a30fbaa487a3da5f7372d89e123a1ac

分析结果严重性

 高危	 中危	 信息	 安全	 关注
6	14	1	2	0

四大组件信息

Activity组件: 11个, 其中export的有: 0个
Service组件: 8个, 其中export的有: 1个
Receiver组件: 2个, 其中export的有: 1个
Provider组件: 5个, 其中export的有: 0个

证书信息

二进制文件已签名

v1 签名: True

v2 签名: True

v3 签名: True

v4 签名: False

主题: C=HK, ST=HONGKONG, L=KOWLOON, O=dtnttech, OU=dtnttech, CN=dtnttech

签名算法: rsassa_pkcs1v15

有效期自: 2023-10-21 05:52:04+00:00

有效期至: 2123-09-27 05:52:04+00:00

发行人: C=HK, ST=HONGKONG, L=KOWLOON, O=dtnttech, OU=dtnttech, CN=dtnttech

序列号: 0x3c8b6197

哈希算法: sha256

证书MD5: 6d1ac977a94c3aef550ff948b9968590

证书SHA1: eb0647bd2ef846d4c7df758ef8c1a34f3a681a8c

证书SHA256: cf8c832f2f26d24362753882908ee28dff20f43b2f92c7256d11955d3ae8c67e

证书SHA512:

8db11f5938ba20a1383d218a8a41d0604817e976387f153839a12aa2acc5ebf696aa55c7eaf0125ba84a51e95db483ddc385b6c8e16c1f898966dbe740b73fd8

公钥算法: rsa

密钥长度: 2048

指纹: 44ddc01ce8b151150fa1eb8442cc936c2d85ba9028e51b8b359a7171374309fc

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.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_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.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.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.ACCESS_AD_SERVICES_AD_ID	普通	允许应用访问设备的广告 ID。	此 ID 是 Google 广告服务提供的唯一、用户可重置的标识符，允许应用出于广告目的跟踪用户行为，同时维护用户隐私。
android.permission.ACCESS_AD_SERVICES_ATTRIBUTION	普通	允许应用程序访问广告服务归因	这使应用能够检索与广告归因相关的信息，这些信息可用于有针对性的广告目的。应用程序可以收集有关用户如何与广告互动的数据，例如点击或展示，以衡量广告活动的有效性。
android.permission.ACCESS_AD_SERVICES_TOPICS	普通	允许应用程序访问广告服务主题	这使应用程序能够检索与广告主题或兴趣相关的信息，这些信息可用于有针对性的广告目的。
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。
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）
com.dtntech.hk.hk.sacademy.coloringbook.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

网络通信安全

序号	范围	严重级别	描述
----	----	------	----

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: 0 | 警告: 3 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	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。
2	Service (androidx.work.impl.background.systemjob.SystemJobService) 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。
3	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver 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。

安全漏洞检测

高危: 5 | 警告: 10 | 信息: 1 | 安全: 1 | 屏蔽: 0

序号	问题	等级	参考标准	文件位置
1	应用程序记录日志信息, 不得记录敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MSTG-STORAGE-3	升级会员: 解锁高级权限
2	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

3	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员: 解锁高级权限
4	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
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	升级会员: 解锁高级权限
6	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	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-100: 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。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
9	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员: 解锁高级权限
10	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

11	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变处理不恰当 ('跨站脚本') OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员: 解锁高级权限
12	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
13	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
14	应用程序在加密算法中使用ECB模式。ECB模式是已知的弱模式，因为它对相同的明文块[UNK]产生相同的密文	高危	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	升级会员: 解锁高级权限
15	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员: 解锁高级权限
16	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
17	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

行为分析

编号	行为	标签	文件
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
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

00036	从 res/raw 目录获取资源文件	反射	升级会员: 解锁高级权限
00014	将文件读入流并将其放入 JSON 对象中	文件	升级会员: 解锁高级权限
00013	读取文件并将其放入流中	文件	升级会员: 解锁高级权限
00025	监视要执行的一般操作	反射	升级会员: 解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员: 解锁高级权限
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
00012	读取数据并放入缓冲流	文件	升级会员: 解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	升级会员: 解锁高级权限
00153	通过 HTTP 发送二进制数据	http	升级会员: 解锁高级权限
00162	创建 InetAddress 对象并连接到它	socket	升级会员: 解锁高级权限
00163	创建新的 Socket 并连接到它	socket	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
00091	从广播中检索数据	信息收集	升级会员: 解锁高级权限
00078	获取网络运营商名称	信息收集 电话服务	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
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员: 解锁高级权限
00072	将 HTTP 输入流写入文件	命令 网络 文件	升级会员: 解锁高级权限
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
00094	连接到 URL 并从中读取数据	命令 网络	升级会员: 解锁高级权限
00108	从给定的 URL 读取输入流	网络 命令	升级会员: 解锁高级权限
00171	将网络运算符与字符串进行比较	网络	升级会员: 解锁高级权限
00132	查询ISO国家代码	电话服务 信息收集	升级会员: 解锁高级权限
00001	初始化位图对象并将数据 (例如JPEG) 压缩为位图对象	相机	升级会员: 解锁高级权限

00114	创建到代理地址的安全套接字连接	网络命令	升级会员: 解锁高级权限
00112	获取日历事件的日期	信息收集 日历	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
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
00009	将游标中的数据放入JSON对象	文件	升级会员: 解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	2/30	android.permission.VIBRATE android.permission.WAKE_LOCK
其它常用权限	6/46	android.permission.INTERNET android.permission.READ_MEDIA_IMAGES android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE 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
init.supersonicads.com	安全	否	IP地址: 18.65.25.20 国家: 美国 地区: 加利福尼亚 城市: 洛杉矶 纬度: 34.052570 经度: -118.243904 查看: Google 地图
prebid-adapter.devenv.kidoz.net	安全	否	IP地址: 34.231.162.78 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图

crash-metrics.sdk.inmobi.com	安全	否	IP地址: 35.212.101.248 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图
www.supersonicads.com	安全	否	No Geolocation information available.
spadsync.com	安全	否	IP地址: 34.231.162.78 国家: 美国 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
devenv.kidoz.net	安全	否	IP地址: 52.206.19.187 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图
i.l.inmobicdn.net	安全	否	IP地址: 34.36.52.227 国家: 美国 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
prebid-adapter.kidoz.net	安全	否	IP地址: 34.36.56.125 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图
log-activity.templates.inmobi.com	安全	否	IP地址: 20.237.24.215 国家: 美国 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
sdk-api-utest.kidoz.net	安全	否	IP地址: 3.231.134.241 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图

accounts.kidoz.net	安全	否	IP地址: 34.228.149.31 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图
sdk-api-test.kidoz.net	安全	否	IP地址: 3.224.30.126 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图
outcome-crash-report.supersonicads.com	安全	否	No Geolocation information available.
vast-utest.kidoz.net	安全	否	IP地址: 3.231.134.241 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图
www.inmobi.com	安全	否	IP地址: 20.31.69.107 国家: 美国 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
analytics.kidoz.net	安全	否	IP地址: 54.197.123.45 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图
doc-hosting.flycricket.in	安全	否	IP地址: 18.154.206.46 国家: 美国 地区: 加利福尼亚 城市: 洛杉矶 纬度: 34.052570 经度: -118.243904 查看: Google 地图
outcome-ssp.supersonicads.com	安全	否	IP地址: 54.230.21.92 国家: 美国 地区: 加利福尼亚 城市: 洛杉矶 纬度: 34.052570 经度: -118.243904 查看: Google 地图

prebid-adapter-test.kidoz.net	安全	否	IP地址: 3.224.30.126 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图
config.inmobi.com	安全	否	IP地址: 35.212.73.115 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图
sdk-api.kidoz.net	安全	否	IP地址: 4.226.138.85 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图
kidoz.net	安全	否	IP地址: 34.226.149.21 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图
unif-id.ssp.inmobi.com	安全	否	IP地址: 35.212.84.49 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图
vast.kidoz.net	安全	否	IP地址: 52.206.19.187 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图
resource.cdn.vii.com	安全	否	IP地址: 13.33.21.11 国家: 美国 地区: 加利福尼亚 城市: 洛杉矶 纬度: 34.052570 经度: -118.243904 查看: Google 地图
sdk-api.devenv.kidoz.net	安全	否	IP地址: 34.231.162.78 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图

vast-test.kidoz.net	安全	否	IP地址: 3.224.30.126 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图
prebid-adapter-utest.kidoz.net	安全	否	IP地址: 3.231.134.241 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图
telemetry.sdk.inmobi.com	安全	否	IP地址: 35.212.238.21 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图
outcome-arm-ext-med-ext.sonic-us.supersonicads.com	安全	否	No Geolocation information available.
ads.inmobi.com	安全	否	IP地址: 35.212.77.200 国家: 美国 地区: 弗吉尼亚州 城市: 阿什本 纬度: 39.039474 经度: -77.491806 查看: Google 地图

URL链接分析

URL信息	源码文件
• https://outcome-crash-report.supersonicads.com/reporter	com/ironsource/environment/e.java
• https://outcome-arm-ext-med-ext.sonic-us.supersonicads.com/aemdata	com/ironsource/mediationsdk/utills/b.java
• https://kidoz.net/v3policy/	com/kidoz/sdk/api/dialogs/AboutKidozDialog.java
• data:a.data}};function	com/inmobi/media/m9.java
• https://outcome-ssp.supersonicads.com/mediation?adunit=3	com/ironsource/mediationsdk/utills/l.java
• http://www.google.com	com/inmobi/media/f3.java
• javascript:toonswebapi.appbackground • javascript:kidoz.maximize • javascript:kidoz.minimize • javascript:toonswebapi.appforeground	com/kidoz/sdk/api/ui_views/html_view/HtmlViewWrapper.java
• https://%s/%s/%s	d2/c.java
• https://init.supersonicads.com/sdk/v	com/ironsource/mediationsdk/server/ServerURL.java

<ul style="list-style-type: none"> 127.0.0.255 	u3/d.java
<ul style="list-style-type: none"> https://prebid-adapter.kidoz.net/api/test-waterfall?offer_id={offer_id_placeholder}& https://devenv.kidoz.net/ https://prebid-adapter-test.kidoz.net/api/test-waterfall?offer_id={offer_id_placeholder}& https://prebid-adapter-utest.kidoz.net/api/test-waterfall?offer_id={offer_id_placeholder}& https://sdk-api-utest.kidoz.net https://sdk-api.kidoz.net https://vast-utest.kidoz.net https://sdk-api.devenv.kidoz.net https://prebid-adapter.devenv.kidoz.net/api/test-waterfall?offer_id={offer_id_placeholder}& https://vast-test.kidoz.net https://sdk-api-test.kidoz.net https://vast.kidoz.net 	com/kidoz/sdk/api/general/Utils/TestUtils.java
<ul style="list-style-type: none"> https://sdk-api.kidoz.net/api/initsdk http://accounts.kidoz.net/api/cc https://analytics.kidoz.net/parents/kidozrestmobile.php 	com/kidoz/sdk/api/server_connect/SdkAPIManager.java
<ul style="list-style-type: none"> https://www.supersonicads.com/mobile/sdk5/log?method= 	com/ironsource/sdk/constants/a.java
<ul style="list-style-type: none"> https://unif-id.ssp.inmobi.com/fetch https://spadsync.com/sync 	com/inmobi/commons/core/configs/SignalsConfig.java
<ul style="list-style-type: none"> https://outcome-ssp.supersonicads.com/mediation?adunit=3 	com/ironsource/mediationsdk/events/g.java
<ul style="list-style-type: none"> https://outcome-ssp.supersonicads.com/mediation?adunit=2 	com/ironsource/mediationsdk/events/f.java
<ul style="list-style-type: none"> https://log-activity.templates.inmobi.com/api/v1/ingest https://telemetry.sdk.inmobi.com/metrics 	com/inmobi/commons/core/configs/TelemetryConfig.java
<ul style="list-style-type: none"> https://crash-metrics.sdk.inmobi.com/trace 	com/inmobi/commons/core/configs/CrashConfig.java
<ul style="list-style-type: none"> https://play.google.com/store/apps/details?id= 	org/cocos2dx/cpp/AppActivity.java
<ul style="list-style-type: none"> https://www.inmobi.com/products/sdk/#downloads https://config.inmobi.com/config-server/v1/config/secure.cfg 	com/inmobi/commons/core/configs/RootConfig.java
<ul style="list-style-type: none"> https://i.l.inmobicdn.net/sdk/sdk/commonsdk-v1.3.17.js https://i.l.inmobicdn.net/sdk/sdk/1053/android/mraid.js https://ads.inmobi.com/sdk 	com/inmobi/commons/core/configs/AdConfig.java
<ul style="list-style-type: none"> javascript:initvideoplayer javascript:requestcurrentvideotime 	com/kidoz/sdk/api/dialogs/WebDialog/VideoEnabledWebView.java
<ul style="list-style-type: none"> https://outcome-arm-ext-med-ext-ionic-us.supersonicads.com/aemdata 	com/ironsource/mediationsdk/impressionData/b.java
<ul style="list-style-type: none"> javascript:toonswebapi.appbackground javascript:toonswebapi.appforeground 	com/kidoz/sdk/api/players/web_player/WebPlayerDialog.java
<ul style="list-style-type: none"> https://play.google.com/store/apps/details?id=com.dtnntech.kidsacademy.coloringbook https://resource.zciilav.com/ads/apps/%s/config.json https://play.google.com/store/apps/developer?id=dtnntech https://doc-hosting.flycricket.io/kids-academy-coloring-book-privacy-policy/9ffa1b76-fae4-49b2-bf8c-b85411342102/privacy 	自研引擎-S

标题	严重程度	描述信息
Firebase远程配置已禁用	安全	<p>Firebase远程配置URL (https://firebaseremoteconfig.googleapis.com/v1/projects/79369112383/namespaces/firebase:fetch?key=AlzaSyBx-xn8Pefu8ZiPqC8zlbX6VEWd6FNiilUY) 已禁用。响应内容如下所示：</p> <pre>{ "state": "NO_TEMPLATE" }</pre>

第三方SDK

SDK名称	开发者	描述信息
Google Play Service	Google	借助 Google Play 服务, 您的应用可以利用由 Google 提供的最新功能, 例如地图, Google+ 等, 并通过 Google Play 商店以 APK 的形式分发自动平台更新。这样一来, 您的用户可以更快地接收更新, 并且可以更轻松地集成 Google 必须提供的最新信息。
IronSource	ironSource Mobile	Turn your app into a business with ironSource. Maximize your ad revenue, grow your user base and optimize your monetization strategy, all from one powerful platform.
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。
Jetpack WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能, 可助您快速采取行动并专注于您的用户。
Picasso	Square	一个强大的 Android 图片下载缓存库。
Firebase Analytics	Google	Google Analytics (分析) 是一款免费的应用衡量解决方案, 可提供关于应用使用情况和用户互动度的分析数据。
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层, 让用户能够在充分利用 SQLite 的强大功能的同时, 获得更强大的数据查询访问机制。

邮箱

EMAIL	源码文件
this@abstracttypeconstructor.builtins this@abstracttypeconstructor.parameter	s7/h.java
this@createcapturedifneeded.type	f7/d.java

追踪器

名称	类别	网址
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

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患。

© 2025 南明离火 - 移动安全分析平台自动生成

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