南明离火
移动应用检测平台

ANDROID 静态分析报告

笔趣阁破解版2023 • v4.18.00

分析日期: 2024-03-18 13:18:14

应用概览

文件名称:	笔趣阁.apk
文件大小:	8.98MB
应用名称:	笔 趣 阁 破 解 版2023
软件包名:	com.aspires.arabic.butchery
主活动:	com.bar.shift.main.ui.activity.StartActivity
版本号:	4.18.00
最小SDK:	21
目标SDK:	28
加固信息:	未加壳
应用程序安全分数:	41/100 (中风险)
跟踪器检测:	2/432
杀软检测:	3 个杀毒软件报毒
MD5:	35c48a89f5572ff5a659afd7c5a81cad
SHA1:	fa560125c61ec1843b78f6fd6f94e5d1d7407317
SHA256:	a26fefa321fb2283d92f8075651454e0269cb7fa66c6b81b57cfaef13e63f6a

分析结果严重性分布

高危	中危	信息	安全	关注
7	15	1	2	13

四大组件导出状态统计

Activity组件：73个，其中export的有：9个
Service组件：8个，其中export的有：0个
Receiver组件：2个，其中export的有：1个
Provider组件：6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: 2023-10-21 01:25:08+00:00
有效期至: 2571-05-21 01:25:08+00:00
发行人: C=CN, ST=GD, L=Guangzhou, O=Tencent, OU=3G, CN=WilsonWu
序列号: 0x315af4ca
哈希算法: sha256
证书MD5: 81fff99e157e9aede497e4ce2f44cc65
证书SHA1: d866572e71576ef853663061f1518ff39789cdbd
证书SHA256: 8d67a8afa99fc2a8414ce29ca2d7d22beeedd21595172774491c6579e692f681
证书SHA512:
7da09b4281ad0c5bf728de1e9b6da6d40db02165ce374319f551bd44a07de4266f51e80148e603f15f755d561189db74a52100cd70c0a3140892c17bc47a165f

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.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.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
android.permission.ACCESS_WIFI_STATE	普通	查看Wi-Fi状态	允许应用程序查看有关Wi-Fi状态的信息。
android.permission.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.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.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
android.permission.GET_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。
com.aspires.arabic.butchery.permission.KW_SDK_BROADCAST	未知	未知权限	来自 android 引用的未知权限。
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。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
android.permission.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.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.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.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: **3** | 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]	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	Broadcast Receiver (com.baoshift.reward.service.MammonReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。

代码安全漏洞检测

高危: **5** | 警告: **10** | 信息: **1** | 安全: **2** | 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
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	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	WebView域控制不严格漏洞	高危	CWE: CWE-73: 外部控制文件名或路径	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	不安全的Web视图实现。WebView忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
8	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
9	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

10	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
11	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-2	升级会员：解锁高级权限
12	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
13	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
14	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
15	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
16	此应用程序可能会请求Root（超级用户）权限	警告	CWE: CWE-250: 以不必要的权限执行 OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
17	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
18	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

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)	SYMBOLSSTRIPPED(裁剪符号表)
1	armeabi-v7a/libBook.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阻止攻击者覆盖返回地址的一种技术。使用选项 -stack-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/libIPlugin.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	6/30	android.permission.READ_PHONE_STATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.WAKE_LOCK android.permission.GET_TASKS android.permission.ACCESS_COARSE_LOCATION android.permission.VIBRATE
其它常用权限	9/46	android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE com.google.android.gms.permission.AD_ID android.permission.CHANGE_NETWORK_STATE android.permission.REORDER_TASKS 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:** N/A **Description:** Maltrail标记的恶意域	是	**IP地址:** 47.115.0.205 **国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看:** 高德地图
tk.anythinktech.com	安全	是	**IP地址:** 112.74.188.11 **国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看:** 高德地图
adxtk.anythinktech.com	安全	否	No Geolocation information available.
www.toponad.com	安全	是	**IP地址:** 42.192.176.82 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
qq.ahaozhuan.com	安全	是	**IP地址:** 47.107.40.90 **国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看:** 高德地图
img.anythinktech.com	安全	否	**IP地址:** 18.154.206.40 **国家:** United States of America **地区:** Washington **城市:** Seattle **纬度:** 47.627499 **经度:** -122.346199 **查看:** Google 地图
pitk.birdgesdk.com	安全	是	**IP地址:** 39.108.103.199 **国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看:** 高德地图
adx.anythinktech.com	安全	是	**IP地址:** 39.105.168.45 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图

cdn-adn-https.rayjump.com	安全	是	**IP地址:** 49.71.77.86 **国家:** China **地区:** Jiangsu **城市:** Yangzhou **纬度:** 32.397221 **经度:** 119.435829 **查看:** 高德地图
api.anythinktech.com	安全	是	**IP地址:** 47.112.152.30 **国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看:** 高德地图
mores.toponad.com	安全	是	**IP地址:** 49.71.77.86 **国家:** China **地区:** Jiangsu **城市:** Yangzhou **纬度:** 32.397221 **经度:** 119.435829 **查看:** 高德地图
apps.samsung.com	安全	是	**IP地址:** 49.79.233.19 **国家:** China **地区:** Jiangsu **城市:** Nantong **纬度:** 32.030281 **经度:** 120.874718 **查看:** 高德地图
open.e.kuaishou.com	安全	是	**IP地址:** 58.215.85.78 **国家:** China **地区:** Jiangsu **城市:** Wuxi **纬度:** 31.568871 **经度:** 120.288567 **查看:** 高德地图
whatwg.org	安全	否	**IP地址:** 165.227.248.76 **国家:** United States of America **地区:** New Jersey **城市:** Clifton **纬度:** 40.858429 **经度:** -74.163757 **查看:** Google 地图
static.yximgs.com	安全	是	**IP地址:** 58.222.37.130 **国家:** China **地区:** Jiangsu **城市:** Taizhou **纬度:** 32.493328 **经度:** 119.910629 **查看:** 高德地图
aa.birdges[illegible]com	安全	是	**IP地址:** 120.78.94.142 **国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看:** 高德地图

img.toponad.com	安全	否	**IP地址:** 99.84.203.13 **国家:** United States of America **地区:** California **城市:** Los Angeles **纬度:** 34.052860 **经度:** -118.243568 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://qq.ahaozhuan.com/wmfw-ylqq/	b/b/a/a.java
• data:image	b/c/a/n/e.java
• https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties	b/g/a/q0/a.java
• https://aa.birdgesdk.com/v1/d_api • https://pitk.birdgesdk.com/v1/ptk	b/k/a/a/a/a.java
• https://img.anythinktech.com/gdpr/PrivacyPolicySetting.html	com/anythink/core/common/i.java

• http://api.anythinktech.com/v2/open/area • https://api.anythinktech.com/v2/open/app • https://api.anythinktech.com/v2/open/placement • https://da.anythinktech.com/v1/open/da • https://tk.anythinktech.com/v1/open/tk • https://api.anythinktech.com/v2/open/eu • https://adx.anythinktech.com/bid • https://adx.anythinktech.com/request • https://adxtk.anythinktech.com/v1 • https://adx.anythinktech.com/openapi/req • https://tk.anythinktech.com/ss/rrd • https://api.anythinktech.com/v2/open/area • http://api.anythinktech.com/v2/open/app • http://api.anythinktech.com/v2/open/placement • http://da.anythinktech.com/v1/open/da • http://tk.anythinktech.com/v1/open/tk • http://api.anythinktech.com/v2/open/eu • http://adx.anythinktech.com/bid • http://adx.anythinktech.com/request • http://adxtk.anythinktech.com/v1 • http://adx.anythinktech.com/openapi/req • http://tk.anythinktech.com/ss/rrd • https://img.anythinktech.com/gdpr/PrivacyPolicySetting.html	• com/anythink/core/common/b/g.java
• http://www.topon.com	com/anythink/core/common/k/h.java
• https://mores.toponad.com/image/default/mmegral_logo.png	com/anythink/expressad/a.java
• javascript:window.navigator.vibrate(	com/anythink/expressad/a/g.java
• file:////	com/anythink/expressad/advanced/c/a.java
• file:///	com/anythink/expressad/advanced/c/c.java
• file:///	com/anythink/expressad/advanced/js/NativeAdvancedJsUtils.java

• javascript:window.mraidbridge.audioVolumeChange(%s); • javascript:window.mraidbridge.fireChangeEvent(%s); • javascript:window.mraidbridge.fireErrorEvent('%1s', • javascript:window.mraidbridge.nativeCallComplete('%s'); • javascript:window.mraidbridge.fireReadyEvent(); • javascript:window.mraidbridge.setCurrentPosition(%.1f, • javascript:window.mraidbridge.setDefaultPosition(%.1f, • javascript:window.mraidbridge.setIsViewable(%s); • javascript:window.mraidbridge.setMaxSize(%.1f, • javascript:window.mraidbridge.setPlacementType(%s); • javascript:window.mraidbridge.setScreenSize(%.1f, • javascript:window.mraidbridge.notifySizeChangeEvent(%.1f,	com/anythink/expressad/atsignalcommon/mraid/CallMraidJS.java
• javascript:window.MvBridge.onFailure(%s,''); • javascript:window.MvBridge.onFailure(%s,'%s'); • javascript:window.MvBridge.fireEvent('%s', • javascript:window.MvBridge.fireEvent('%s','%s'); • javascript:window.OW.onSuccess(%s,''); • javascript:window.OW.onSuccess(%s,'%s');	com/anythink/expressad/atsignalcommon/windvane/g.java
• javascript:window.WindVane.onFailure(%s,''); • javascript:window.WindVane.onFailure(%s,'%s'); • javascript:window.WindVane.fireEvent('%s', • javascript:window.WindVane.fireEvent('%s','%s'); • javascript:window.WindVane.onSuccess(%s,''); • javascript:window.WindVane.onSuccess(%s,'%s');	com/anythink/expressad/atsignalcommon/windvane/j.java
• https://cdn-adn-https.rayjump.com/cdn-adn/v2/portal/19/08/20/11/06/5d5b63cb457e2.js	com/anythink/expressad/d/a/b.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/anythink/expressad/d/b/b.java
• https://img.toponad.com/sdk/app-permissions.html?key=	com/anythink/expressad/foundation/d/a.java
• 10.0.0.200 • 10.0.0.172	com/anythink/expressad/foundation/g/f/g/b.java
• file:////	com/anythink/expressad/mbbanner/a/a/c.java
• file:////	com/anythink/expressad/mbbanner/a/d/c.java
• file:///	com/anythink/expressad/splash/c/b.java
• file:///	com/anythink/expressad/splash/c/c.java
• file:////	com/anythink/expressad/splash/js/SplashJsUtils.java
• file:////	com/anythink/expressad/video/bt/a/c.java
• file:////	com/anythink/expressad/video/module/AnythinkH5EndCardView.java
• file:////	com/anythink/expressad/videocommon/b/h.java

• 6.1.31.3	com/anythink/network/gdt/BuildConfig.java
• 6.1.31.1	com/anythink/network/kuaishou/BuildConfig.java
• https://errlogos.umeng.com/api/crashsdk/logcollect • https://errlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/controller/ControllerCenter.java
• https://errlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/f/c.java
• 10.244.132.170	com/kwad/components/core/offline/init/kwai/d.java
• 3.3.32.1 • https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/offline_components/adLive/ks_so-adLiveNoSoRelease-3.3.32.1-f1f921211-59.zip	com/kwad/components/offline/adLive/a.java
• https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/adLive/3.3.26.1/ks_so-adLiveArm64v8aRelease-3.3.26.1.apk • https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/adLive/3.3.26.1/ks_so-adLiveArmeabiv7aRelease-3.3.26.1.apk	com/kwad/components/offline/adLive/kwai/a.java
• 3.3.32.1 • https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/offline_components/tk/ks_so-tachikomaNoSoRelease-3.3.32.1-c07a870c9-58.zip	com/kwad/components/offline/tk/b.java
• https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.24.2/ks_so-tachikomaLiteArm64v8aRelease-3.3.24.2.apk • https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.24.2/ks_so-tachikomaArm64v8aRelease-3.3.24.2.apk • https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.24.2/ks_so-tachikomaLiteArmeabiv7aRelease-3.3.24.2.apk • https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/tachikoma/3.3.24.2/ks_so-tachikomaArmeabiv7aRelease-3.3.24.2.apk • 3.3.24.2	com/kwad/components/offline/tk/a/a.java
• https://open.e.kuaishou.com/rest/e/v3/open/sdk2	com/kwad/sdk/api/loader/v.java
• https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks_so-appStatusArm64v8aRelease-3.3.14.apk • https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDk/ks_so-appStatusArmeabiv7aRelease-3.3.14.apk	com/kwad/sdk/collector/d.java
• http://%s:%d/%s	com/kwad/sdk/core/videocache/f.java
• https://github.com/danikula/AndroidVideoCache/issues/88. • https://github.com/danikula/AndroidVideoCache/issues/43. • https://github.com/danikula/AndroidVideoCache/issues.	com/kwad/sdk/core/videocache/h.java
• 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/ks_so-exceptionArmeabiv7aRelease-3.3.23.apk	com/kwad/sdk/crash/f.java
• http://apps.samsung.com/appquery/appDetail.as?appId=	com/kwad/sdk/utils/d.java
• https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties	com/kwai/filedownloader/services/a.java
• https://errlogos.umeng.com/upload • https://errlog.umeng.com/upload • 3.2.0.4	com/uc/crashsdk/e.java

本报告由南明离火移动安全分析平台生成

• https://errlogos.umeng.com • https://errlog.umeng.com • 3.2.0.4	com/uc/crashsdk/a/d.java
• 3.2.0.4 • https://errlogos.umeng.com/api/crashsdk/logcollect • https://errlog.umeng.com/api/crashsdk/logcollect	com/uc/crashsdk/a/h.java
• javascript:window.MvBridge.onFailure(%s,'%s'); • data:image • javascript:window.WindVane.onSuccess(%s,''); • https://cdn-adn-https.rayjump.com/cdn-adn/v2/portal/19/08/20/11/06/5d5b63cb457e2.js • javascript:window.mraidbridge.nativeCallComplete('%s'); • file:/// • http://www.toponad.com • 10.0.0.172 • https://api.anythinktech.com/v2/open/area • javascript:window.mraidbridge.setIsViewable(%s); • javascript:window.OW.onSuccess(%s,''); • https://api.anythinktech.com/v2/open/placement • javascript:window.mraidbridge.fireReadyEvent(); • https://tk.anythinktech.com/v1/open/tk • http://adx.anythinktech.com/bid • javascript:window.mraidbridge.setScreenSize(%.1f, • javascript:window.mraidbridge.fireChangeEvent(%s); • javascript:window.MvBridge.onFailure(%s,''); • javascript:window.WindVane.onSuccess(%s,'%s'); • https://api.anythinktech.com/v2/open/eu • http://da.anythinktech.com/v1/open/da • http://api.anythinktech.com/v2/open/placement • http://api.anythinktech.com/v2/open/eu • https://img.toponad.com/sdk/app-permissions.html?key= • https://api.anythinktech.com/v2/open/app • https://errlog.umeng.com/api/crashsdk/logcollect • 6.1.31.1 • https://errlogos.umeng.com/api/crashsdk/logcollect • http://adx.anythinktech.com/openapi/req • file://// • https://adx.anythinktech.com/request • javascript:window.OW.onSuccess(%s,'%s'); • javascript:window.mraidbridge.setMaxSize(%.1f, • javascript:window.mraidbridge.setPlacementType(%s); • http://adx.anythinktech.com/request • http://adxtk.anythinktech.com/v1 • javascript:window.mraidbridge.fireErrorEvent('%1s', • javascript:window.mraidbridge.setCurrentPosition(%.1f, • javascript:window.WindVane.fireEvent('%s', • javascript:window.MvBridge.fireEvent('%s','%s'); • http://api.anythinktech.com/v2/open/area • javascript:window.MvBridge.fireEvent('%s', • javascript:window.WindVane.fireEvent('%s','%s'); • 10.244.132.170 • https://mores.toponad.com/image/default/mintegral_logo.png • javascript:window.WindVane.onFailure(%s,'%s'); • javascript:window.navigator.vibrate(• https://tk.anythinktech.com/ss/rrd • http://api.anythinktech.com/v2/open/app • https://adxtk.anythinktech.com/v1 • http://tk.anythinktech.com/ss/rrd • javascript:window.mraidbridge.audioVolumeChange(%s); • javascript:window.mraidbridge.setDefaultPosition(%.1f, • https://da.anythinktech.com/v1/open/da • http://tk.anythinktech.com/v1/open/tk • javascript:window.WindVane.onFailure(%s,'');	自研引擎分析结果

• 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://qq.ahaozhuan.com/wmfw-ylqq/ • https://img.anythinktech.com/gdpr/PrivacyPolicySetting.html • https://adx.anythinktech.com/openapi/req • javascript:window.mraidbridge.notifySizeChangeEvent(%.1f, • 6.1.31.3 • 10.0.0.200 • https://adx.anythinktech.com/bid	

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性能监控平台，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	用于其他应用共享媒体内容和控件，已被 media2 取代。
FileDownloader	LingoChamp	一个 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	com/kuaishou/weapon/p0/ac.java
danikula@gmail.com	com/kwad/sdk/core/videocache/h.java
apk@classes.dex	自研引擎分析结果

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
"anythink_myoffer_feedback_violation_of_laws" : "违规违法"
"dyStrategy.privateAddress" : "privateAddress"
"anythink_myoffer_feedback_violation_of_laws" : "Illegal"
55ecca97822a39bc4b276d645ad35c09
e43929c76e20f091def8fe0579d16adc
ZGUucm9idi5hbmRyb2lkLnhwb3NlZC5pbnN0YWxsZXI=
644a9dacce49b4c3226f5129267c0dad
f118f1f9431de3a626df48d7302911
aW8udmlydHVhbGFwcC5zYW5kdnhwb3NlZDMy
Y29tLnRlbmNlbnQubWF0cml4Lk1hdHJpeA==
2711ba35c7345099edcc3f4526e0b59d
4a5bc9a30d53edd85d5dcc58905afb0d
d278819f65940c10a8b7313bf606bfff
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDKta2b5Vw5YK[illegible]HCAJ4rJCwS227
b60d5c17b0cc4aa03e8180bc5cedaf3d
Y2F0IC9wcm9jL3N5cy9rZXJuZWwvcmFuZG9tL2Jvb3RfaWQ=
40eb0d1d346cab7ced4d02a3065b7a94
40f3b3b81340519f51bfc19cb9ea2284
9798330679c11734503264cdfb[illegible]18e16
Y29tLnRlbmNlbnQubWF0cml4LnBsdWdpbi5QbHVnaW5MaXN0ZW5lcg==
ebb56fa9c5701350947e281c2446660f
69828b2[illegible]6d1c06552a81870a5d5e4[illegible]
dG9wLm5pdW5haWp1bi5ibGFja2JveGExMg==
db892c7b72a9636667bfc8ea7e9[illegible]0bc
31f065607e6da6b7[illegible]133[illegible]df0b35460
76308532f6[illegible]b68[illegible]5a930c42cceec22b
Y2F0IC9zeXMvZGV2aWNlcy9zb2MwL3NlcmlhbF9udW1iZXI=
WebKitFormBoundaryP0Rfzlf32iRoMhmb

本报告由南明离火移动安全分析平台生成

r/35FZ29e4I6pS2B8zSq2RgBpXUuMg7oZF1Qt3x0iyg8PeyblyNeCRB6gIMehFThe
ZE1XbmhiZXlLcjBKSXZMTk94M0JGa0V1bWw5Mlk1ZmpTcUdUN1I4cFpWY2lQSEFzdEM0VVhhNlFEdzFnb3orLw==
f5d9ed20ecd348d291dc742508036c00
005c29f4f5c26b21923dce9b72a0fc8d
71a9baa45905a6f0e527e5a2e06e8808
dWsuZGlnaXRhbHNxdWlkLm5ldHNwb29mZXI=
Y29tLnhpYW9taS5tYXJrZXQuRE1fUEFHRV9PUEVORUQ=
Y29tLnVuaXF1ZS5tb2JpbGVmYWtlcg==
Y29tLnRlbmNlbnQubWF0cml4LnRyYWNlLmNvcmUuTG9vcGVyTW9uaXRvcg==
c66bf3f78bd997bbd5b6e5038a23dff6
6ca7958ee0b0192a7c52c16faffaa8ba
e0f9628529f23e1928c8d3f61634c8f2
cbed106d3241121e1ccb6a8bc152d53e
b48f51dc240ddd4ffb5d8c75a5c5c820
8674972563d49769d5d9a64744ac5749
b9c0eff152a62bd5062844255107f3e0
9f22c0987957bb7abb016726b088ad78
b8ae143a7f66bd1fa8acac1f65402c0c
YW5kcm9pZC5hcHAuQWN0aXZpdHlUYXNrTWFnYWdlcg==
f12536c198aee4d8198aad2300827430
Y1dRJlUS0ggA8rDIzmTuSb18fETpsUSlIb8eUc8Cs7Tg08T72W0CbR0HtnL8mwiuorXs9F6RhwllueUNq7egw==
B92825C2BD5D6D6D1E7F39EE7D17843B7D9016F611136B754141BC6F4D3F00F05
aW8udmlydHVhbGFwcC52YW5kdnhwb3NlZDY0
03f870871950c1f48387b251894ed3e88
eff11be0b8a3c872fa30b0484b460d12
Y29tLnhpYW9taS5tYXJrZXQuREISKUNOX01BSUxfU1RBVFVT
601b51116a2a470e8f12847b
8f2f54c08600aa25d5f517fa1371441b
SUFjdGl2aXR5VGFza01hbmFnZXJTaW5nbGV0b24=
YW5kcm9pZC5hcHAuQWN0aXZpdHlNYW5hZ2VyTmF0aXZl
2c6f402c6a565d2e6912b0013fa59380

d2c9607f3ddbbefe6914f1e94e8c53ff
09a2c11101651aa5e866979ad43f3df0
310fad205107df839a5026968c232766
f118f1e84f0bf5ba3bd1579c6d35
Y29tLm1ldGFzcGxvaXQuc3RhZ2U=
dcd68cd059cb06a9596ba6839c2e8858
e3fdbf82716c2cb9b666a3880ab94003
OTUzc3E1N0w5NTIzMW80OUQxMGo3R1dFa0ZiandHT0w=
ec3e4937f3c114dd36ed0cbd10585d22
7cb16c2840085bbdf4be628e6604bac1
Y29tLnhpYW9taS5tYXJrZXQuRE1fUEFHRV9DTE9TRUQ=
Y29udGVudDovL2NvbS54aWFvbWkubWFya2V0LnByb3ZpZGVyLkRpcmVjdE1haWxQcm92aWRlcg==
Y1dRJlUS0ggA8rDIzmTuSdNPHbegnkXofklx4RRLaYJoK5uDjDZ2N7h9QqyTv9Qg
b496f2beb340c9b0065ce3f825109f1c

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。