南明离火
移动应用检测平台

ANDROID 静态分析报告

网课学习 • v1.0.7

分析日期: 2025-05-16 17:21:01

应用概览

文件名称:	网课学习 v1.01.apk
文件大小:	53.08MB
应用名称:	网课学习
软件包名:	plus.H5A21C719
主活动:	io.dcloud.PandoraEntry
版本号:	1.01
最小SDK:	19
目标SDK:	26
加固信息:	未加壳
开发框架:	DCloud
应用程序安全分数:	23/100 (重大风险)
跟踪器检测:	1/432
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	1d57c114ee89a79cc6400803025e357c
SHA1:	21e494af8f909307a33c3204feef02300b59df81
SHA256:	0c78822271408200[illegible]a6e756736aa9057f538c24f098325679472e9af98

分析结果严重性分布

高危	中危	信息	安全	关注
16	11	1	1	0

四大组件导出状态统计

Activity组件：62个，其中export的有： 0个
Service组件：15个，其中export的有： 1个
Receiver组件：7个，其中export的有： 0个
Provider组件：7个，其中export的有： 0个

应用签名证书信息

本报告由南明离火移动安全分析平台生成

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=CN, ST=Guangdong, L=Zhongshan, O=Junyang, OU=JunyangSoft, CN=Luo Yifeng
签名算法: rsassa_pkcs1v15
有效期自: 2021-02-15 12:37:10+00:00
有效期至: 2121-01-22 12:37:10+00:00
发行人: C=CN, ST=Guangdong, L=Zhongshan, O=Junyang, OU=JunyangSoft, CN=Luo Yifeng
序列号: 0x7ef317c0
哈希算法: sha256
证书MD5: 0993a4d223806223ee205a32e33410f5
证书SHA1: 6c6dbb712d86123955e44b90f806a3746c2d3859
证书SHA256: 8e2184a692ece5217e0aeaad751c77d0648c5a0e0a8e946a0463fc838afcc779
证书SHA512:
a110c7087e08fb4c49dbf0aad3f39b7457e511740e100d32c72fe80d8d416121b9b19ddccf58e20a74731b55e42678e61d508ad4e7cfe0f78caf5481b106d4a8

公钥算法: rsa
密钥长度: 2018
指纹: c073448ab4727b75606e1440b5966b800658832f74ee6797894dcbf4160df598
共检测到 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.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.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.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.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.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户粗略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
android.permission.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
android.permission.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
android.permission.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
android.permission.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。

android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
android.permission.READ_CONTACTS	危险	读取联系人信息	允允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
android.permission.READ_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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.VIBRATE	普通	控制振动器	允许应用程序控制振动器，用于消息通知振动功能。
android.permission.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
android.permission.WRITE_CONTACTS	危险	写入联系人信息	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。
android.permission.WRITE_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.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.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.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.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.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
plus.H5A21C719.permission.KW_SDK_BROADCAST	未知	未知权限	来自 android 引用的未知权限。
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。
plus.H5A21C719.openads.sdk.permission.TT_PANGOLIN	未知	未知权限	来自 android 引用的未知权限。
android.permission.SET_WALLPAPER	普通	设置壁纸	允许应用程序设置壁纸。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	普通	桌面图标角标	vivo平台桌面图标角标，接入vivo平台后需要用户手动开启，开启完成后收到新消息时，在已安装的应用桌面图标右上角显示“数字角标”。

可浏览 Activity 组件分析

ACTIVITY	INTENT
io.dcloud.PandoraEntry	Schemes: h53d2d9cc://,

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: **0** | 警告: **1** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用已使用代码签名证书进行签名。

Manifest 配置安全分析

高危: **15** | 警告: **4** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用、28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	Activity (io.dcloud.PandoraEntryActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
3	Activity（io.dcloud.PandoraEntryActivity）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（26） 升级至 28 及以上以获得平台级防护。
4	Activity (com.ss.android.downloadlib.activity.TTDelegateActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
5	Activity（com.ss.android.downloadlib.activity.TTDelegateActivity）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（26） 升级至 28 及以上以获得平台级防护。
6	Activity (com.ss.android.downloadlib.activity.JumpKllkActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
7	Activity（com.ss.android.downloadlib.activity.JumpKllkActivity）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（26） 升级至 28 及以上以获得平台级防护。

8	Activity (com.ss.android.socialbase.appdownloader.view.DownloadTaskDeleteActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
9	Activity（com.ss.android.socialbase.appdownloader.view.DownloadTaskDeleteActivity）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（26） 升级至 28 及以上以获得平台级防护。
10	Activity (com.ss.android.socialbase.appdownloader.view.JumpUnknownSourceActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
11	Activity（com.ss.android.socialbase.appdownloader.view.JumpUnknownSourceActivity）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（26） 升级至 28 及以上以获得平台级防护。
12	Activity (com.kwad.sdk.api.proxy.app.BaseFragmentActivity$FragmentActivitySingleInstance1) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
13	Activity (com.kwad.sdk.api.proxy.app.BaseFragmentActivity$FragmentActivitySingleInstance2) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
14	Activity (com.kwad.sdk.api.proxy.app.BaseFragmentActivity$DeveloperConfigActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
15	Service (com.kwad.sdk.api.proxy.VideoWallpaperService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_WALLPAPER [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
16	Activity 设置了 TaskAffinity 属性 (io.dcloud.WebAppActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
17	Activity (io.dcloud.WebAppActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
18	Activity（io.dcloud.WebAppActivity）易受 Android Task Hijacking/StrandHogg 攻击	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（26） 升级至 28 及以上以获得平台级防护。

本报告由南明离火移动安全分析平台生成

19	高优先级 Intent（1000） - {1} 个命中 [android:priority]	警告	通过设置较高的 Intent 优先级，应用可覆盖其他请求，可能导致安全风险。

代码安全漏洞检测

高危: **1** | 警告: **5** | 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	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
4	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
5	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
6	SSL的不安全实现。信任所有证书或接受自签名证书是一个关键的安全漏洞。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
7	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
8	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

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/libEncryptor.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 不能执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码，这使得面向返回的编程（ROP）攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个随机哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出。	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	True info 符号被剥离

2	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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用。	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
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
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
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
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
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	网络	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00013	读取文件并将其放入流中	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
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
00130	获取当前WIFI信息	WiFi 信息收集	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
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	15/30	android.permission.REQUEST_INSTALL_PACKAGES android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.CAMERA android.permission.GET_ACCOUNTS android.permission.MODIFY_AUDIO_SETTINGS android.permission.READ_CONTACTS android.permission.READ_PHONE_STATE android.permission.RECORD_AUDIO android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.WRITE_CONTACTS android.permission.WRITE_SETTINGS android.permission.GET_TASKS android.permission.SET_WALLPAPER
其它常用权限	10/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.FLASHLIGHT android.permission.REORDER_TASKS android.permission.READ_EXTERNAL_STORAGE android.permission.BLUETOOTH

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。

URL 链接安全分析

URL信息	源码文件
• http://www.google.com/chrome/frame • https://github.com/whatwg/html/issues/2369 • http://mmbiz.qpic.cn/mmbiz/22pp2iaH4HWH1yXgXFpLGQUslEPjMCgyiaPwtk7cgdzTZGz2hylQv3Jz3yAEtXDyVh5NOdYJaF6M8kU86RipFAmQ/640 • https://github.com/schteppe/p2.js/issues • https://infra.spec.whatwg.org • http://www.pixijs.com • http://192.76.60.110:8080/mystudy • https://html.spec.whatwg.org/multipage/scripting.html • https://html.spec.whatwg.org/multipage/forms.html • https://connect.microsoft.com/IE/feedback/details/1736512 • http://phaser.io • https://ykt.eduyun.cn • https://www.5yoo.cc • http://www.greensock.com • https://promises-aplus.com • http://google.com • http://flappy2048.com • https://web.archive.org/web/20141116233347/http • http://buzz.jaysalvat.com • http://www.microsoft.com/windows/internet-explorer/default.aspx	

• http://www.iana.org/assignments/media-types • http://ucren.com • http://cdn.szzyb.site/tongbushipin • http://games.vdcom.cn/index.html • http://github.com/zynga/viewporter • http://m.softgames.de • https://web.archive.org/web/20100324014747/http • http://www.html5star.com • http://d1bjj4kazoovdg.cloudfront.net/assets/sg_ig_logo.png • http://raphaeljs.com • https://sizzlejs.com • https://jsperf.com/getall-vs-sizzle/2 • https://github.com/jrburke/requirejs/wiki/Updating-existing-libraries • https://raw.github.com/zynga/viewporter/master/MIT-LICENSE.txt • http://www.scirra.com • http://61.132.228.101:7001/datdownload/MP4/ • http://scotty-staging.softgames.de/assets/api/voyager.js • http://www.5you.cc • http://raphaeljs.com/license.html • https://bugzilla.mozilla.org/show_bug.cgi?id=687787 • https://html.spec.whatwg.org/multipage/syntax.html • http://www.61ertong.com • http://192.168.0.112/mystudy • http://www.whatbrowser.org • https://jsperf.com/thor-indexof-vs-for/5 • http://api.zyabcd.com/api/resdownload/baseinfo?category= • rtmp://live.hkstv.hk.lxdns.com/live/hks • http://playtomax.com • http://www.zzfriend.com/api.php?mod=js&bid=52 • http://games.vdcom.cn/games/qqppp • http://mp.weixin.qq.com/s?__biz=MzA4NTk2MzgxNg==&mid=200512824&idx=1&sn=fb2c29f97e9[illegible]8eb672d9e733750b96 • http://www.greensock.com/terms_of_use.html • https://lagged.com • http://www.mozilla.com/firefox • https://js.foundation • http://data.zyabcd.com/MP4 • http://www.google.com/chrome • https://github.com/schteppe/p2.js.git • http://www.jq22.com • http://61.132.228.101:8080/data/LuoTemp/mystudy/version.txt • http://tajs.qq.com/stats?sId=36313[illegible] • https://html.spec.whatwg.org • http://cdn.szzyb.site/tongbushipin2/ • http://jaysalvat.com • http://ejohn.org • http://steffe.se	自研引擎-A

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。
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。
IJKPlayer	Bilibili	IJKPlayer 是一款基于 FFmpeg 的轻量级 Android/iOS 视频播放器，具有 API 易于集成、编译配置可裁剪、支持硬件加速解码、DanmakuFlameMaster 架构清晰、简单易用等优势。

讯飞 SDK	科大讯飞	讯飞开放平台作为全球首个开放的智能交互技术服务平台，致力于为开发者打造一站式智能人机交互解决方案。
android-gif-drawable	koral--	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。
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。
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。

第三方追踪器检测

名称	类别	网址
Pangle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/363

敏感凭证泄露检测

可能的密钥
DCloud（数字天堂）的=> "DCLOUD_AD_ID" : "1.20069087E11"
DCLOUD的 "AD_ID" : "120069090002"
DCLOUD的 "CHANNEL" : "common"
DCLOUD的 "ApplicationId" : "plus.H5A21C719"
凭证信息=> "IFLY_APPKEY" : "53feacdd"
DCLOUD的 "DCLOUD_STREAMAPP_CHANNEL" : "plus.H5A21C719|H53D2D9CC|120069090002|common"
DCLOUD的 "APPID" : "H53D2D9CC"
"dcloud_permissions_reauthorization" : "reauthorize"

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。