南明离火
移动应用检测平台

ANDROID 静态分析报告

91短视频 • v7.1.0

分析日期: 2025-07-07 11:54:15

应用概览

文件名称:	dsp_lite_7.1.0_250701_6 (1).apk
文件大小:	30.57MB
应用名称:	91短视频
软件包名:	cn.jsyhd.uubmgk
主活动:	com.dft.shot.android.ui.LaunchActivity
版本号:	7.1.0
最小SDK:	21
目标SDK:	30
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	45/100 (中风险)
跟踪器检测:	1/432
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	c0b15e45c4d005648e5498db5a1334a5
SHA1:	52fc9db281b8aed1ae0126539417bb775e4b1c40
SHA256:	feae91137d0e244e877861e1cde7c176f4c716c33b8189374867a666f4115ee3

本报告由南明离火移动安全分析平台生成

分析结果严重性分布

高危	中危	信息	安全	关注
3	15	3	1	5

四大组件导出状态统计

Activity组件：32个，其中export的有： 0个
Service组件：4个，其中export的有： 0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

应用签名证书信息

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: C=Singapore, ST=Singapore, L=Singapore, O=., OU=., CN=.
签名算法: rsassa_pkcs1v15
有效期自: 2025-07-01 23:08:12+00:00
有效期至: 2026-07-01 23:08:12+00:00
发行人: C=Singapore, ST=Singapore, L=Singapore, O=., OU=., CN=.
序列号: 0x53eadf57
哈希算法: sha256
证书MD5: e8bfdd3934cfb6b429c69cc175a0fe98
证书SHA1: adb919c60836d71d1e8f9b08a0101599c23d5c47
证书SHA256: 5b1e52d58a2d315512b4e67c34c3a2262113fe707988904f485de146dbf2ae63
证书SHA512:
9add4a6d797a923ca7b0920c4729b42d01a53bfaf5d8684477c574e714052110261f82f685577ef5[illegible]52bcb5fe35132a46b6a515520[illegible]208eab616e52f9082856

公钥算法: rsa
密钥长度: 2048
指纹: 6595b65aa329a0b81767fe487057e63bb8222ba325d9d1abb98f16d831f73[illegible]
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.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.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.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.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.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。
android.permission.READ_PRIVILEGED_PHONE_STATE	签名(系统)	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.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.WRITE_MEDIA_STORAGE	签名(系统)	获取外置SD卡的写权限	允许应用程序在外置SD卡中进行写入操作。

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.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.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
android.permission.ACCESS_DOWNLOAD_MANAGER	签名(系统)	访问下载管理器	这个权限是允许应用访问下载管理器，以便管理大型下载操作。
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.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看到的图像。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
android.permission.RECORD_VIDEO	未知	未知权限	来自 android 引用的未知权限。
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.CAPTURE_AUDIO_OUTPUT	签名(系统)	允许捕获音频输出	允许应用程序捕获音频输出。
android.permission.CAPTURE_VIDEO_OUTPUT	普通	允许捕获视频输出	允许应用程序捕获视频输出。
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.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.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.NETWORK_PROVIDER	未知	未知权限	来自 android 引用的未知权限。
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.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.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.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.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.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
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.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.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加、删除帐户及删除其密码之类的操作。
android.permission.RECEIVE_USER_PRESENT	普通	允许程序唤醒机器	允许应用可以接收点亮屏幕或解锁广播。
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.ACCESS_LOCATION_EXTRA_COMMANDS	普通	访问定位额外命令	访问额外位置提供程序命令，恶意应用程序可能会使用它来干扰GPS或其他位置源的操作。
android.permission.READ_PROFILE	危险	读取用户资料	允许应用程序读取用户个人信息。
android.permission.DISABLE_KEYGUARD	危险	禁用键盘锁	允许应用程序停用键锁和任何关联的密码安全设置。例如，在手机上接听电话时停用键锁，在通话结束后重新启用键锁。
android.permission.ACCESS_COARSE_UPDATES	未知	未知权限	来自 android 引用的未知权限。

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: **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	应用已配置网络安全策略 [android:networkSecurityConfig=@7F150001]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。
3	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
4	Broadcast Receiver (com.dft.shot.android.im.websocket.NotificationReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
5	高优先级 Intent（2147483647） - {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: **3** | 警告: **9** | 信息: **3** | 安全: **1** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	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	应用程序记录日志信息，不应记录敏感信息	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
4	可能存在漏洞。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
5	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

6	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
7	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
8	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
9	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
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	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
12	此应用程序使用SQL Cipher。SQL Cipher为sqlite数据库文件提供256位AES加密	信息	OWASP MASVS: MSTG-CRYPTO-1	升级会员：解锁高级权限
13	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

14	默认情况下，调用Cipher.getInstance("AES")将返回AES ECB模式。众所周知，ECB模式很弱，因为它导致相同明文块的密文相同	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	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
16	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

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	arm64-v8a/librtmp-jni.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
2	arm64-v8a/libs[illegible]jni.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	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。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	True info 符号被剥离

3	arm64-v8a/libWatermark.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
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
00202	打电话	控制	升级会员：解锁高级权限
00203	将电话号码放入意图中	控制	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
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
00054	从文件安装其他APK	反射	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
00121	创建目录	文件 命令	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
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

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
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
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	短信	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
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限
00183	获取当前相机参数并更改设置	相机	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
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
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
00011	从 URI 查询数据（SMS、CALLLOGS）	短信 通话记录 信息收集	升级会员：解锁高级权限
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	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
00091	从广播中检索数据	信息收集	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
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
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
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

00115	获取设备的最后已知位置	信息收集 位置	升级会员：解锁高级权限
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00119	将IMEI号写入文件	信息收集 文件 电话服务 命令	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
00002	打开相机并拍照	相机	升级会员：解锁高级权限
00104	检查给定路径是否是目录	文件	升级会员：解锁高级权限
00031	检查当前正在运行的应用程序列表	反射 信息收集	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

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.VIBRATE android.permission.ACCESS_COARSE_LOCATION android.permission.RECEIVE_BOOT_COMPLETED android.permission.GET_TASKS android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.SYSTEM_ALERT_WINDOW android.permission.WAKE_LOCK android.permission.READ_PHONE_STATE android.permission.ACCESS_FINE_LOCATION android.permission.MODIFY_AUDIO_SETTINGS android.permission.CALL_PHONE android.permission.GET_ACCOUNTS android.permission.WRITE_SETTINGS
其它常用权限	10/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.FLASHLIGHT android.permission.CHANGE_WIFI_STATE android.permission.REORDER_TASKS android.permission.CHANGE_NETWORK_STATE android.permission.ACCESS_LOCATION_EXTRA_COMMANDS

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
video.7k.cn	安全	否	No Geolocation information available.
pfzpnj.lhyiyqr.xyz	安全	是	**IP地址:** 106.63.15.10 **国家:** 中国 **地区:** 江苏 **城市:** 无锡 **纬度:** 31.569349 **经度:** 120.288788 查看: 高德地图
www.weiju.ba	安全	否	No Geolocation information available.
img.miseyl.com	安全	否	No Geolocation information available.
api.eu.amplitude.com	安全	否	**IP地址:** 3.64.52.0 **国家:** 德国 **地区:** 黑森 **城市:** 美因河畔法兰克福 **纬度:** 50.110882 **经度:** 8.681996 查看: Google 地图
api.t.sina.com.cn	安全	是	**IP地址:** 49.67.73.135 **国家:** 中国 **地区:** 云南 **城市:** 昆明 **纬度:** 25.038891 **经度:** 102.718330 查看: 高德地图
jvtijg.lcjsujyb.xyz	安全	是	**IP地址:** 106.63.15.10 **国家:** 中国 **地区:** 江苏 **城市:** 无锡 **纬度:** 31.569349 **经度:** 120.288788 查看: 高德地图
xx.125.com	安全	否	No Geolocation information available.
static.meiqia.com	安全	是	**IP地址:** 49.67.73.135 **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

api2.amplitude.com	安全	否	**IP地址:** 50.112.233.80 **国家:** 美国 **地区:** 俄勒冈 **城市:** 波特兰 **纬度:** 45.523460 **经度:** -122.676468 **查看:** Google 地图
jp-kao.aass4.top	安全	否	No Geolocation information available.
4399.com多发生部位	安全	否	No Geolocation information available.
imgpublic.ycomesc.com	安全	否	No Geolocation information available.
pfzpnj.lhyiyqr.xyzhttps	安全	否	No Geolocation information available.
www.docs.developers.amplitude.com	安全	否	**IP地址:** 76.76.21.142 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 核桃 **纬度:** 34.015400 **经度:** -117.858223 **查看:** Google 地图
greenrobot.org	安全	否	**IP地址:** 85.13.163.69 **国家:** 德国 **地区:** 图林根 **城市:** 弗里德斯多夫 **纬度:** 50.604919 **经度:** 11.035770 **查看:** Google 地图
jvtijg.lfdgilu.xyz	安全	是	**IP地址:** 221.228.32.13 **国家:** 中国 **地区:** 江苏 **城市:** 无锡 **纬度:** 31.569349 **经度:** 120.288788 **查看:** 高德地图
raw.githubusercontent.com	安全	否	**IP地址:** 185.199.109.133 **国家:** 美国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065647 **经度:** -79.891724 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• 127.0.0.1 • http://%s:%d/%s	com/danikula/videocache/i.java
• 127.0.0.1	org/nanohttpd/protocols/http/b.java

• http://%s:%d/%s	com/danikula/videocache/m.java
• http://jp-kao.aass4.top:8086/src2 • http://192.168.1.8/avweb • https://static.meiqia.com/dist/standalone.html?_=t&eid=121277	com/dft/shot/android/d.java
• https://pfzpnj.lhyiyqr.xyz,https://jvtijg.lfdgilu.xyz,https://jvtijg.lcjsujyb.xyz	com/dft/shot/android/uitls/h1.java
• http://imgpublic.ycomesc.com/	com/dft/shot/android/im/v2/ChatActivityV3.java
• https://raw.githubusercontent.com/little-5/backup/master/91.txt	com/dft/shot/android/network/a.java
• http://api.t.sina.com.cn/short_url/shorten.json?source=3271760578&url_long=	com/dft/shot/android/q/l.java
• https://www.docs.developers.amplitude.com/data/sdks/android-kotlin/#offline-mode	com/amplitude/android/utilities/AndroidNetworkConnectivityChecker.java
• http://img.miseyl.com/imgupload.php	com/dft/shot/android/network/f.java
• https://api.eu.amplitude.com/2/httpapi • https://api.eu.amplitude.com/batch • https://api2.amplitude.com/2/httpapi • https://api2.amplitude.com/batch	com/amplitude/core/Constants.java
• http://imgpublic.ycomesc.com/img.xiao/04c9fb02a8c30ae84aa2f942e873af2d.jpg	com/dft/shot/android/bean/home/HomeBean.java
• https://greenrobot.org/greendao/documentation/database-encryption/	org/greenrobot/greendao/j/b.java
• 1.0.0.1	com/szcx/lib/encrypt/e.java
• http://api.t.sina.com.cn/short_url/shorten.json?source=3271760578&url_long=	com/dft/shot/android/base/l.java
• http://www.baidu.com,这是测试哟 • ftp://4399.com多发生部位 • https://xx.125.com • www.weiju.ba/xx2/b54 • www.baidu.com/img/xxxx.jpg • www.baidu.com/?html=12354bhb35&ask=dasoiubao • www.baidu.com哈哈哈www.google.com垃圾都是泪放假啊是的佛i	com/vector/update_app/HttpTextView.java
• http://www.baidu.com,这是测试哟 • ftp://4399.com多发生部位 • https://xx.125.com • www.weiju.ba/xx2/b54 • www.baidu.com/img/xxxx.jpg • www.baidu.com/?html=12354bhb35&ask=dasoiubao • www.baidu.com哈哈哈www.google.com垃圾都是泪放假啊是的佛i	com/dft/shot/android/view/HttpView.java
• https://jvtijg.lfdgilu.xyz • https://pfzpnj.lhyiyqr.xyz • https://jvtijg.lcjsujyb.xyz	com/dft/shot/android/a.java

• http://127.0.0.1:%d%s	com/m3u8/download/j/b.java
• https://github.com/tootallnate/java-websocket/wiki/lost-connection-detection	g/a/a.java
• http://video.7k.cn/app_video/20171202/6c8cf3ea/v.m3u8.mp4	com/dft/shot/android/base/BaseVideoActivity.java
• https://github.com/vinc3m1 • https://github.com/vinc3m1/roundedimageview.git • https://github.com/vinc3m1/roundedimageview • https://github.com/vanniktech/emoji	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。
RenderScript	Android	RenderScript 是用于在 Android 上以高性能运行计算密集型任务的框架。RenderScript 主要用于数据并行计算，不过串行工作负载也可以从中受益。RenderScript 运行时可在设备上提供的多个处理器（如多核 CPU 和 GPU）上并行调度工作。这样您就能够专注于表达算法而不是调度工作。RenderScript 对于执行图像处理、计算摄影或计算机视觉的应用来说尤其有用。
AgentWeb	Justson	AgentWeb 是一个基于 Android WebView，极度容易使用以及功能强大的库，提供了 Android WebView 一系列的问题解决方案，并且轻量和极度灵活。
Dexter	Karumi	Dexter 是一个 Android 库，它简化了运行时请求权限的过程。
PictureSelector	LuckSiege	一款针对 Android 平台下的图片选择器，支持从相册获取图片、视频、音频 & 拍照，支持裁剪(单图 or 多图裁剪)、压缩、主题自定义配置等功能，支持动态获取权限&适配 Android 5.0+ 系统的开源图片选择框架。
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。
AndroidAutoSize	JessYanCoding	今日头条屏幕适配方案终极版，一个极低成本的 Android 屏幕适配方案。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

第三方追踪器检测

名称	类别	网址
Amplitude	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/125

敏感凭证泄露检测

可能的密钥
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"

c713c7f928203caedebcfbc98e3cc1d1
ef8f996997308cb294c89cdea1798a6a
caf36d4f5cbfb1229a0005f1df54426a
193154da93e7506ee4c91257f1931ddf
CA327CBA8080BEDB919A1BAA3713E018
b39372dfb1d739e9dffc919c44854fbe
c400bc1739f7c30b0c794b9b5a5070f5
b429ecf619c69bc650fccc18b86ae9fa
1046af6c7a9ca06a922b79d3b842e804
OTkZOVoPAAkIWAgICl1bDFgOXAkBSFwOAF8KDgBDX0oPDVhfAiQVNCE2AAkLKw==
04c9fb02a8c30ae84aa2f943e873af2d
22f1fdbcf448886ab9c1bff03d89656a
1566c6c800765625933d81df50b0892f
d20ba3fd602306a593cf8f56e9d91726
6BBBBAAD-3430-406E-A937-F47917E51112
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
DQ0dDWk4aT5rOzs4OD00Pms/OjoyCjAhITEJKjI=
ca3a2848d4e4417eb6ebfbffdc1f3212
1ed3b6ec19a32188da0d0e851bbe2a61

免责声明及风险提示:

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。