南明离火
移动应用检测平台

ANDROID 静态分析报告

海王视频 v3.1.0

分析日期: 2025-07-07 14:54:14

应用概览

文件名称:	haiwang_h3gu14pw4_3.1.0.apk
文件大小:	26.99MB
应用名称:	海王视频
软件包名:	com.haiwang.dfskj0624
主活动:	com.jbzd.media.fiveonehl.ui.splash.SplashActivity
版本号:	3.1.0
最小SDK:	21
目标SDK:	28
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	47/100 (中风险)
杀软检测:	AI评估：可能有安全隐患
MD5:	3f7c7ced23eae7e02a22be581f109f43
SHA1:	bf6ed954c3e0b559f892e27e275af20e060e1dd1
SHA256:	ce2395cddd88[illegible]d7bdae456ac0f9[illegible]c1b81c8dd08e8bfad8df5871e2

分析结果严重性分布

高危	中危	信息	安全	关注
6	22	5	3	10

四大组件导出状态统计

Activity组件：128个，其中export的有： 6个
Service组件：7个，其中export的有： 1个
Receiver组件：9个，其中export的有： 2个
Provider组件：8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: True
v4 签名: False
主题: CN=Cohan
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-24 12:58:35+00:00
有效期至: 2050-06-18 12:58:35+00:00
发行人: CN=Cohan
序列号: 0x1
哈希算法: sha256
证书MD5: 4a68b0e12f844974618a63d2507066da
证书SHA1: 638d9cd23d04099b321291b9ce669a26131c309d
证书SHA256: b09e33c019ebdc399b616aca820bb1e755b15895b69bc40e9d2ed8044d9711db
证书SHA512:
bd8514f85f0a93976a99a6342bd38b402f6fc228dc381117ae9ff8ea5f1d546b473aa82f3ceee220ee73e0aca91f2dfceb6d42f10207d9f714f615e7f4e509f

公钥算法: rsa
密钥长度: 2048
指纹: a807ab46552816377c68a21a68e2d2eb07354b30825fc5f6254eadc39e07ad4f
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.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.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.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_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.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.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.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.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.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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
android.permission.KILL_BACKGROUND_PROCESSES	普通	结束进程	允许应用程序结束其他应用程序的后台进程。
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.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.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（推送最受播放，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: **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: **1** | 警告: **10** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已配置网络安全策略 [android:networkSecurityConfig=@7F130001]	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。
2	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。
3	Broadcast Receiver (com.ibzd.media.fiveonehl.ui.appstore.DownloadCompleteReceiver) 未受保护。存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。

4	Activity-Alias (com.jbzd.media.fiveonehl.aliasFour) 未受保护。 存在 intent-filter。	警告	检测到 Activity-Alias 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity-Alias 被显式导出，存在安全风险。
5	Activity-Alias (com.jbzd.media.fiveonehl.aliasThree) 未受保护。 存在 intent-filter。	警告	检测到 Activity-Alias 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity-Alias 被显式导出，存在安全风险。
6	Activity-Alias (com.jbzd.media.fiveonehl.aliasTwo) 未受保护。 存在 intent-filter。	警告	检测到 Activity-Alias 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity-Alias 被显式导出，存在安全风险。
7	Activity-Alias (com.jbzd.media.fiveonehl.aliasOne) 未受保护。 存在 intent-filter。	警告	检测到 Activity-Alias 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity-Alias 被显式导出，存在安全风险。
8	Activity (com.alipay.sdk.app.PayResultActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
9	Activity (com.alipay.sdk.app.AlipayResultActivity) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。
10	Activity (com.alipay.sdk.app.AlipayResultActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
11	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_JOB_SERVICE [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。
12	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 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。

代码安全漏洞检测

高危: **5** | 警告: **11** | 信息: **5** | 安全: **2** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	应用程序可以写入应用程序目录。敏感信息应加密	信息	CWE: CWE-276: 默认权限不正确 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
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	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了被破坏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
6	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
7	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
8	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

9	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
10	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
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	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
13	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
14	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
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	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

17	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
18	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
19	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
20	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
21	此应用程序使用SQL Cipher。SQLCipher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
22	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
23	此应用侦听剪贴板更改。一些恶意软件也会监听剪贴板更改	信息	OWASP MASVS: MSTG-PLATFORM-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)	SYMBOLS STRIPPED(裁剪符号表)
1	arm64-v8a/libavutil.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金丝雀值（canary）。这种技术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	True info 符号被剥离

2	arm64-v8a/libjeffmony.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
3	arm64-v8a/libtmp_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

应用行为分析

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
00036	从 res/raw 目录获取资源文件	反射	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
00054	从文件安装其他APK	反射	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
00033	查询IMEI号	信息收集	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
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
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
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
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
00091	从广播中检索数据	信息收集	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
00025	监视要执行的一般操作	反射	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
00104	检查给定路径是否是目录	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
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
00028	从assets目录中读取文件	文件	升级会员：解锁高级权限
00162	创建 InetSocketAddress 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
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
00130	获取当前WIFI信息	WiFi 信息收集	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
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
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

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.VIBRATE android.permission.SYSTEM_ALERT_WINDOW android.permission.READ_PHONE_STATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.CAMERA android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	7/46	android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.FLASHLIGHT 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

ddghsdjax.t17b347crb.com	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
haiapiback.mcago5l1rfd4.com	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
xjsbhcdvj.thtuh07nuh.com	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
debsuchyg.bp8qsawr3v.com	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
api.buzhidaoxiesha.com	安全	否	No Geolocation information available.
dxtfzvhgj.mcz5kb8sp2.com	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
dashif.org	安全	否	**IP地址:** 185.199.108.153 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
haiapiback.xt8yjguh759g.com	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

tmapi.tmsangewg.com	安全	否	No Geolocation information available.
api.telegram.org	安全	否	**IP地址:** 149.154.167.220 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 英格兰 **城市:** 伦敦 **纬度:** 51.508530 **经度:** -0.125740 **查看:** Google 地图
h5.m.taobao.com	安全	是	**IP地址:** 221.228.32.13 **国家:** 中国 **地区:** 江苏 **城市:** 扬州 **纬度:** 32.397221 **经度:** 119.435000 **查看:** 高德地图
haiapiback.4mf1yevh2txr.com	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
98ghvbjkn.vnffliud9u.com	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
haiapiback.srguggh5iosx.com	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

URL 链接安全分析

URL信息	源码文件
• https://haiapiback.srguggh5iosx.com/tkapi/ • https://debsuchyn.o8qsawr3v.com/tkapi/ • https://dxtfzvhgj.mc75kb8sp2.com/tkapi/ • https://ddghcdax.t17b347crb.com/tkapi/ • https://haiapiback.4mf1yevh2txr.com/tkapi/ • https://98ghvbjkn.vnffliud9u.com/tkapi/ • https://haiapiback.xt8yjguh759g.com/tkapi/ • https://haiapiback.mcago5l1rfd4.com/tkapi/ • https://xjsbhcdvj.thtuh07nuh.com/tkapi/	com/jbzd/media/fiveonehl/utils/LineUtils.java

• https://api.telegram.org/bot6086117813:aafwil2rn_qzbwa_a6dkeggeax1gijorqza/sendmessage	af/aq/aa/fiveonehl/CustomizedExceptionHandler.java
• https://api.telegram.org/bot6086117813:aafwil2rn_qzbwa_a6dkeggeax1gijorqza/sendmessage	com/jbzd/media/fiveonehl/CustomizedExceptionHandler.java
• https://haiapiback.srguggh5iosx.com/tkapi/ • https://debsuchyg.bp8qsawr3v.com/tkapi/ • https://dxtfzvhgj.mcz5kb8sp2.com/tkapi/ • https://ddghsdjax.t17b347crb.com/tkapi/ • https://haiapiback.4mf1yevh2txr.com/tkapi/ • https://98ghvbjkn.vnffliud9u.com/tkapi/ • https://haiapiback.xt8yjguh759g.com/tkapi/ • https://haiapiback.mcago5l1rfd4.com/tkapi/ • https://xjsbhcdvj.thtuh07nuh.com/tkapi/	af/aq/aa/fiveonehl/utils/UrlUtils.java
• 127.0.0.1	af/bb/aa/ae/ab.java
• http://m.alipay.com/?action=h5quit	af/aa/ab/aj/ah.java
• https://loggw-exsdk.alipay.com/loggw/logupload.do	af/aa/ab/af/aa/ai.java
• https://mcgw.alipay.com/sdklog.do	af/aa/ab/af/ad/ac.java
• https://mobilegw.alipay.com/mgw.htm	af/aa/ab/af/ac.java
• 127.0.0.1 • http://%s:%d/%s	af/ag/aa/ag.java
• https://h5.m.taobao.com/mlapp/olist.html	af/aa/ab/ac/aa.java
• http://api.buzhidaoxiesha.com/cxapi/ • http://tmapi.tmsangewg.com/cxapi/	com/jbzd/media/fiveonehl/net/NetConfig.java
• http://127.0.0.1:	com/jbzd/media/fiveonehl/ui/download/MergeTsToMp4Helper.java
• https://mobilegw.alipay.com/mgw.htm	af/aa/ab/ac/ad.java
• http://%s:%d/%s	af/ag/aa/al.java
• 2.13.1.48	af/aq/aa/fiveonehl/net/interceptor/HeaderInterceptor.java
• http://api.buzhidaoxiesha.com/cxapi/ • http://tmapi.tmsangewg.com/cxapi/	af/aq/aa/fiveonehl/net/NetConfig.java
• http://dashif.org/guidelines/last-segment-number	af/ak/aa/aa/chi/bl/ak/ac.java
• 2.13.1.48	com/jbzd/media/fiveonehl/net/interceptor/HeaderInterceptor.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
FFmpeg	FFmpeg	FFmpeg 是领先的多媒体框架，能够解码，编码，转码，MUX，DEMUX，流式，过滤和播放人类和机器创建的几乎所有内容。
Conscrypt	Google	Conscrypt 是一个 Java 安全提供程序 (JSP)，它实现了部分 Java 加密扩展 (JCE) 和 Java 安全套接字扩展 (JSSE)。 它使用 BoringSSL 为 Android 和 OpenJDK 上的 Java 应用程序提供加密原语和传输层安全性 (TLS)。 有关所提供内容的详细信息，请参阅功能文档。
PlayerSDK	JeffMony	提供一个高效的播放器库。
支付宝 SDK	Alipay	支付宝开放平台基于支付宝海量用户，将强大的支付、营销、数据能力，通过接口等形式开放给第三方合作伙伴，帮助第三方合作伙伴创建更具竞争力的应用。
AndroidUtilCode	Blankj	AndroidUtilCode 是一个强大易用的安卓工具类库，它合理地封装了安卓开发中常用的函数，具有完善的 Demo 和单元测试，利用其封装好的 APIs 可以大大提高开发效率。
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。
Jetpack Lifecycle	Google	生命周期感知型组件可执行操作来响应另一个组件（如 Activity 和 Fragment）的生命周期状态的变化。这些组件有助于您写出更有条理且往往更精简的代码，这样的代码更易于维护。
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 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。
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。
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，获享更强健的数据库访问机制。

敏感凭证泄露检测

可能的密钥
b6cbad6cbd5ec0d209afc69ad3b7a617efaac9b3c47eabe0be42d924936fa78c8001b1fd74b079e5ff9690061dacfa4768e981a526b9ca77156ca36251cf2f90e1054813749987e6e6e18b75ca98b8ed2eaf86ff402c874cca0a263053f22237858206867d210020daa38c48b20cc9dfd82b44a51aeb5db459b22794e2e649
812968f2d6b12831ccd1ef7580fa508d
edef8ba9-79d6-4ece-a3c8-27dcd51d21ed
e6b1bdcb89037af2f2419fe06d0fdf7628ad0083d52da1ecfe991164711bbf9297e75353de96f1740695d07610567b1240549af9cbd87d06919ac31c859ad37ab3807c311b4756e1e208775989a4f691bff4bbbc58174d2a96b1d0d970a05114d7ee57dfc33b1bafaf6e0d820e838427018b6435f903df04ba7fd34d73f8f5df9434b164e0220baabb10c8978c3f4c6b7da79d8220a968356d15090dea07df9606f665cbec14d218dd3d691cce2866a58840971b6a57b76af88b1a65fdffd2c080281a6ab20be5879e0330eb7ff70871ce684e7174ada5dc3159c461375a0796b17ce7beca83cf34f65976d237aee993db48d34a4e344f4d8b7e99119168bdd7

f319490bedd9d936b7d2576139cc413b

免责声明及风险提示: