



ANDROID 静态分析报告



天美传媒 v5.1

分析日期: 2025-07-07 16:40:00

i应用概览

文件名称:	61b92246dad8a2445941e28a654fe437.apk
文件大小:	20.4MB
应用名称:	天美传媒
软件包名:	com.jbzd.media.blackliaos
主活动:	com.jbzd.media.blackliaos.ui.splash.SplashActivity
版本号:	5.1
最小SDK:	24
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	54/100 (中风险)
杀软检测:	AI评估: 可能有安全隐患
MD5:	61b92246dad8a2445941e28a654fe437
SHA1:	90e52a2a837ded52aac8a0733af49b9652fb15bd
SHA256:	9a61283a8292f1f55f2538935e9d6630d28f83e381fbc2c54643db75d986841

分析结果严重性分布

🚨 高危	⚠️ 中危	i 信息	✓ 安全	🔍 关注
1	18	4	2	0

四大组件导出状态统计

Activity组件: 64个, 其中export的有: 4个
Service组件: 0个, 其中export的有: 1个
Receiver组件: 12个, 其中export的有: 3个
Provider组件: 6个, 其中export的有: 0个

应用签名证书信息

APK已签名

v1 签名: False

v2 签名: True

v3 签名: False

v4 签名: False

主题: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown

签名算法: rsassa_pkcs1v15

有效期自: 2025-06-13 15:53:18+00:00

有效期至: 2052-10-29 15:53:18+00:00

发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown

序列号: 0x35e4f8a

哈希算法: sha256

证书MD5: 36cb86f0e3cec30a84e6996eb73a25f3

证书SHA1: 8ff600684e7b34e66d9145d24f843340ab12496b

证书SHA256: 03e73c42cdabfa52a50bb1ea20bc4fe2faab02b57e0fa5938c90803dba94a81a

证书SHA512: 6fcec6b2b50d2736663b9540aef198318bfbc4929d771e4b698583336974271632b42d8020412ffa5a6abcf33f1613b95429fffd871256b9a10c02d7af147128

公钥算法: rsa

密钥长度: 2048

指纹: 6e839a0614a8ba832ec3f912c67332b8055e15be24340eb60c24dcb8299614b8

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.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.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	写入/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.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.READ_MEDIA_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
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（推送悬浮播放，锁屏播放）
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。
com.jbzd.media.blackliaos.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

🔒 网络通信安全风险分析

序号	范围	严重程度	描述
----	----	------	----

📄 证书安全合规分析

高危: 0 | 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: 9 | 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=@7F160001]	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	应用数据存在泄露风险 未设置[android:allowBackup]标志	警告	建议将 [android:allowBackup] 显式设置为 false。默认值为 true，允许通过 adb 工具备份应用数据，存在数据泄露风险。
3	Broadcast Receiver (com.jbzd.media.blackliaos.ui.appstore.DownloadCompleteReceiver) 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。
4	Activity-Alias (com.jbzd.media.blackliaos.aliasFour) 未受保护。 [android:exported=true]	警告	检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。
5	Activity-Alias (com.jbzd.media.blackliaos.aliasThree) 未受保护。 [android:exported=true]	警告	检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。
6	Activity-Alias (com.jbzd.media.blackliaos.aliasTwo) 未受保护。 [android:exported=true]	警告	检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。
7	Activity-Alias (com.jbzd.media.blackliaos.aliasOne) 未受保护。 [android:exported=true]	警告	检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。
8	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。
9	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。
10	Broadcast Receiver (androidx.profileinstaller.ProfileInstallerReceiver) 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: 1 | 警告: 8 | 信息: 4 | 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
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
4	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-1	升级会员：解锁高级权限
5	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
6	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
7	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
8	MD5哈希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

9	不安全的Web视图实现。可能存在于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
10	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
11	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
12	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
13	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
14	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

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（ROPI）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，以防止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	True info 二进制文件有以下加固函数: ['_strchr_chk', '_vsnprintf_chk', '_memcpy_chk', '_strchr_chk', '_vsprintf_chk', '_strncpy_chk']	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
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

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
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
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00046	方法反射	反射	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
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
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
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
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
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

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.WRITE 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	10/46	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.READ_MEDIA_IMAGES android.permission.READ_MEDIA_AUDIO android.permission.READ_MEDIA_VIDEO android.permission.FOREGROUND_SERVICE android.permission.FLASHLIGHT

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
greenrobot.org	安全	否	IP地址: 85.13.163.69 国家: 德国 地区: 图林根 城市: 弗里德斯堡 纬度: 50.604919 经度: 11.035770 查看: Google 地图
api.s6pgls9ya8.com	安全	否	IP地址: 3.167.192.7 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
api.cssohi4n0w.com	安全	否	IP地址: 3.167.192.84 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
api.l9vgoxc7re.com	安全	否	No Geolocation information available.
api-tianmei.kicfoakjvf.com	安全	否	IP地址: 104.21.50.212 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.775700 经度: -122.395203 查看: Google 地图
api.i6g4br9576.com	安全	否	IP地址: 3.167.192.7 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
api.fl2fk7nrlm.com	安全	否	IP地址: 3.167.192.7 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

tianmei.tw	安全	否	IP地址: 13.226.225.62 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
api-tianmei.sljghdlqpa.com	安全	否	IP地址: 104.21.73.241 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.775700 经度: -122.395200 查看: Google 地图
api.ro0j0yq44m.com	安全	否	No Geolocation information available.

🌐 URL 链接安全分析

URL信息	源码文件
• https://plus.google.com/	o0/v0.java
• 127.0.0.1	d8/b.java
• http://%s:%d/%s • 127.0.0.1	s0/k.java
• 127.0.0.1	s0/i.java
• http://%s:%d/%s • 127.0.0.1	s0/f.java
• http://api.ro0j0yq44m.com/tiv1 • http://api-tianmei.kicfoakjvf.com/tiv1 • http://api-tianmei.sljghdlqpa.com/tiv1 • http://api.s6pgls9ya8.com/tiv1 • http://api.cssohi4n0w.com/tiv1 • http://api.fl2fk7un3fn.com/tiv1 • http://api.i6g4br95vc.com/tiv1 • http://api.l0ygc07re.com/tiv1	h5/l.java
• https://greenrobot.org/greendao/documentation/database-encryption/	org/greenrobot/greendao/database/b.java
• https://tianmei.tw	自研引擎-S

☞ 第三方 SDK 组件分析

SDK名称	开发者	描述信息
-------	-----	------

Conscript	Google	Conscript 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。
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。
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。
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。
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。
Jetpack App Startup	Google	App Startup 库提供了一种直接、高效的方法为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。
AndroidAutoSize	JessYanCoding	今日头条屏幕适配方案终极版，一个极低成本 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 MediaRouter	Google	Enable media display and playback on remote receiver devices using a common user interface.
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Google Cast	Google	使用 Google Cast SDK，您可以扩展 Android，iOS 或 Chrome 应用，以将其流式视频和音频定向到电视或声音系统。您的应用程序成为播放，暂停，搜索，倒带，停止和控制媒体的遥控器。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).
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，获得更强健的数据库访问机制。

✉ 邮箱地址敏感信息提取

EMAIL	源码文件
-------	------

this@appstoreactivity.lifecycl	com/jbzd/media/blackliaos/ui/appstore/AppStoreActivity.java
this@aichangefaceactivity.lifecycl	com/jbzd/media/blackliaos/ui/post/topic/AiChangeFaceActivity.java
this@purchaseactivity.lifecycl	com/jbzd/media/blackliaos/ui/purchase/PurchaseActivity.java
org@gmail.com	自研引擎-S

 敏感凭证泄露检测

可能的密钥
1234567890qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
cd271bb945844572818ba0bda1b59e85

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，深入扫描软件中潜在的漏洞和安全隐

© 2025 南明离火 - 移动安全分析平台自动生成