南明离火
移动应用检测平台

# ANDROID 静态分析报告


中特视频 • v2.2.32

分析日期: 2025-05-16 16:21:03

# 应用概览

| | |
|---|---|
| 文件名称: | 中特视频_2.2.32.apk |
| 文件大小: | 27.13MB |
| 应用名称: | 中特视频 |
| 软件包名: | com.legendsoft.cm_patch_2_2_32 |
| 主活动: | com.legendsoft.ui_cm.ui.SplashActivity |
| 版本号: | 2.2.32 |
| 最小SDK: | 19 |
| 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: | 43/100 (中风险) |
| 跟踪器检测: | 3/432 |
| 杀软检测: | AI评估：可能有安全隐患 |
| MD5: | f4eca3ca1ebe73e64b306ee000e79bb0 |
| SHA1: | dad05d105e2ff0b409c8838ca300a43264157633 |
| SHA256: | c4fab8170c97c40dd6ffe55d2266a267ed61a4b628ba90cb2e22d1dabb71fab |

# 分析结果严重性分布

| 高危 | 中危 | 信息 | 安全 | 关注 |
|---|---|---|---|---|
| 5 | 21 | 2 | 1 | 0 |

# 四大组件导出状态统计

| |
|---|
| Activity组件：34个，其中export的有： 0个 |
| Service组件：10个，其中export的有： 6个 |
| Receiver组件：7个，其中export的有： 3个 |
| Provider组件：4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: C=IHAP10, ST=AYO70R, L=OL7C5E, O=0KCJRH, OU=O5DRM1, CN=CK4Y9A
签名算法: rsassa_pkcs1v15
有效期自: 2025-01-15 09:33:34+00:00
有效期至: 2050-01-09 09:33:34+00:00
发行人: C=IHAP10, ST=AYO70R, L=OL7C5E, O=0KCJRH, OU=O5DRM1, CN=CK4Y9A
序列号: 0x56610b74
哈希算法: sha512
证书MD5: 4c580278164098ddb4b1ec050b409454
证书SHA1: 56d0ad9ff96ac8c7be118a083ae79288c53f5e53
证书SHA256: ae8250798009d0ad8243bbbd3f4af707d05a17860ca1e6d845cf6b2e26fc9058
证书SHA512:
aab2b1a395ab63ce1935910436cc0780c67ef20dd82167412face659d4257277d5e87d647527c87ad9265ff4bd4ce2400a07db20d9944ccefc8a95b0d2cfa316

公钥算法: rsa
密钥长度: 2048
指纹: a0f270f0598de5e08714fd37bfd2fab709fe9cdb055c3d851751acd59c738c12
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 | 完全互用网访问 | 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.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.BLUETOOTH | 危险 | 创建蓝牙连接 | 允许应用程序查看或创建蓝牙连接。 |
| 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.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.BROADCAST_PACKAGE_ADDED | 签名 | 接收新增APP的通知 | 它允许一个应用程序接收到其他应用程序添加新包（即新安装的可执行文件）的广播消息。 |
| android.permission.BROADCAST_PACKAGE_CHANGED | 签名 | 接收APP变化的通知 | 它允许一个应用程序接收到其他应用程序变化（安装、卸载、修改）的广播消息。 |

| | | | |
|---|---|---|---|
| android.permission.BROADCAST_PACKAGE_INSTALL | 签名 | 接收APP安装的通知 | 它允许一个应用程序接收到其他应用程序安装新包（即新安装的可执行文件）的广播消息。 |
| android.permission.BROADCAST_PACKAGE_REPLACED | 签名 | 接收APP替换的通知 | 它允许一个应用程序接收到其他应用程序被覆盖安装的广播消息。 |
| android.permission.RESTART_PACKAGES | 普通 | 重启进程 | 允许程序自己重启或重启其他程序 |
| 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.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。 |

## 网络通信安全风险分析

高危: **1** | 警告: **0** | 信息: **0** | 安全: **0**

| 序号 | 范围 | 严重级别 | 描述 |
|---|---|---|---|
| 1 | * | 高危 | 基本配置不安全地配置为允许到所有域的明文流量。 |

## 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: **2** | 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=@xml/network_security_config] | 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 | 应用可被调试 [android:debuggable=true] | 高危 | 应用开启了可调试标志，攻击者可轻易附加调试器进行逆向分析，导出堆栈信息或访问调试相关类，极大提升被攻击风险。 |
| 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 | Activity (com.legendsoft.ui_com.ui.MainActivity) 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 | Service (com.taobao.accs.ChannelService) 未受保护。 [android:exported=true] | 警告 | 检测到 Service 已导出，未受任何权限保护，任意应用均可访问。 |

| | | | |
|---|---|---|---|
| 6 | Service (com.taobao.accs.data.MsgDistributeService) 未受保护。<br>[android:exported=true] | 警告 | 检测到 Service 已导出，未受任何权限保护，任意应用均可访问。 |
| 7 | Broadcast Receiver (com.taobao.accs.EventReceiver) 未受保护。<br>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。 |
| 8 | Broadcast Receiver (com.taobao.accs.ServiceReceiver) 未受保护。<br>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。 |
| 9 | Service (org.android.agoo.accs.AgooService) 未受保护。<br>[android:exported=true] | 警告 | 检测到 Service 已导出，未受任何权限保护，任意应用均可访问。 |
| 10 | Service (com.umeng.message.UmengIntentService) 未受保护。<br>[android:exported=true] | 警告 | 检测到 Service 已导出，未受任何权限保护，任意应用均可访问。 |
| 11 | Service (com.umeng.message.XiaomiIntentService) 未受保护。<br>[android:exported=true] | 警告 | 检测到 Service 已导出，未受任何权限保护，任意应用均可访问。 |
| 12 | Broadcast Receiver (com.taobao.agoo.AgooCommondReceiver) 未受保护。<br>[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。 |
| 13 | Service (com.umeng.message.UmengMessageIntentReceiverService) 未受保护。<br>[android:exported=true] | 警告 | 检测到 Service 已导出，未受任何权限保护，任意应用均可访问。 |

## 代码安全漏洞检测

高危: **2** | 警告: **9** | 信息: **2** | 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<br>OWASP MASVS: MSTG-STORAGE-3 | 升级会员：解锁高级权限 |
| 2 | 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<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | 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<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | 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'）<br>OWASP Top 10: M7: Client Code Quality | 升级会员：解锁高级权限 |
| 5 | 已启用远程WebView调试 | 高危 | CWE: CWE-919: 移动应用程序中的弱点<br>OWASP Top 10: M1: Improper Platform Usage<br>OWASP MASVS: MSTG-RESILIENCE-2 | 升级会员：解锁高级权限 |
| 6 | 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<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | 升级会员：解锁高级权限 |
| 7 | 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 |
| 8 | 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<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-6 | 升级会员：解锁高级权限 |
| 9 | IP地址泄露 | 信息 | CWE: CWE-200: 信息泄露<br>OWASP MASVS: MSTG-CODE-2 | 升级会员：解锁高级权限 |
| 10 | 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<br>OWASP Top 10: M9: Reverse Engineering<br>OWASP MASVS: MSTG-STORAGE-14 | 升级会员：解锁高级权限 |
| 11 | 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<br>OWASP Top 10: M1: Improper Platform Usage<br>OWASP MASVS: MSTG-PLATFORM-7 | 升级会员：解锁高级权限 |

| | | | | |
|---|---|---|---|---|
| 12 | 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'）<br>OWASP Top 10: M1: Improper Platform Usage<br>OWASP MASVS: MSTG-PLATFORM-6 | 升级会员：解锁高级权限 |
| 13 | 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<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | 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 |

## 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/libtnet-3.1.14.so | True<br>info<br>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)<br>info<br>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<br>info<br>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<br>info<br>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<br>info<br>二进制文件没有设置运行时搜索路径或RPATH | None<br>info<br>二进制文件没有设置RUNPATH | True<br>info<br>二进制文件有以下加固函数: ['__strrchr_chk', '__strlen_chk', '__sprintf_chk', '__strchr_chk', '__strcpy_chk'] | True<br>info<br>符号被剥离 |

## 应用行为分析

| 编号 | 行为 | 标签 | 文件 |
|---|---|---|---|
| 00096 | 连接到 URL 并设置请求方法 | 命令<br>网络 | 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<br>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<br>命令 | 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 |
| 00013 | 读取文件并将其放入流中 | 文件 | 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 |
| 00192 | 获取短信收件箱中的消息 | 短信 | 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 |
| 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 |
| 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 |
| 00029 | 动态初始化类对象 | 反射 | 升级会员：解锁高级权限 |
| 00026 | 方法反射 | 反射 | 升级会员：解锁高级权限 |

| | | | |
|---|---|---|---|
| 00039 | 启动网络服务器 | 控制<br>网络 | 升级会员：解锁高级权限 |
| 00024 | Base64解码后写入文件 | 反射<br>文件 | 升级会员：解锁高级权限 |
| 00177 | 检查是否授予权限并请求 | 权限 | 升级会员：解锁高级权限 |
| 00072 | 将 HTTP 输入流写入文件 | 命令<br>网络<br>文件 | 升级会员：解锁高级权限 |
| 00094 | 连接到 URL 并从中读取数据 | 命令<br>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<br>命令 | 升级会员：解锁高级权限 |
| 00056 | 修改语音音量 | 控制 | 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 |
| 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 |
| 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 |

## 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.REQUEST_INSTALL_PACKAGES<br>android.permission.READ_PHONE_STATE<br>android.permission.ACCESS_FINE_LOCATION<br>android.permission.GET_TASKS<br>android.permission.WAKE_LOCK<br>android.permission.RECEIVE_BOOT_COMPLETED |
| 其它常用权限 | 8/46 | android.permission.INTERNET<br>android.permission.READ_EXTERNAL_STORAGE<br>android.permission.WRITE_EXTERNAL_STORAGE<br>android.permission.ACCESS_NETWORK_STATE<br>android.permission.ACCESS_WIFI_STATE<br>android.permission.BLUETOOTH<br>android.permission.CHANGE_NETWORK_STATE<br>android.permission.CHANGE_WIFI_STATE |

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://%s:%d/%s<br>• 127.0.0.1 | com/danikula/videocache/HttpProxyCacheServer.java |
| • http://127.0.0.1:%d%s | jaygoo/local/server/M3U8HttpServer.java |
| • 127.0.0.1 | jaygoo/local/server/NanoHTTPD.java |
| • 8.8.8.8<br>• 8.8.4.4 | io/netty/resolver/dns/DefaultDnsServerAddressStreamProvider.java |
| • http://%s:%d/%s | com/danikula/videocache/Pinger.java |
| • https://github.com/vinc3m1<br>• https://github.com/vinc3m1/roundedimageview<br>• https://github.com/vinc3m1/roundedimageview.git | 自研引擎-S |

## 第三方 SDK 组件分析

| SDK名称 | 开发者 | 描述信息 |
|---|---|---|
| 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线上监控平台，为多家知名企业提供服务。 |
| AgentWeb | Justson | AgentWeb 是一个基于的 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。 |
| 友盟推送 | Umeng | 基于友盟+全域数据建立精准的消息推送平台，为开发者提供更灵活、更智能、更有效的消息推送方案，有效提升用户粘性，提高 App 活跃度。 |
| EasyPermissions | Google | EasyPermissions 是一个包装器库，用于简化针对 Android M 或更高版本的基本系统权限逻辑。 |
| 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 | 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 |
|---|---|---|
| Baidu Mobile Stat | Analytics | https://reports.exodus-privacy.eu.org/trackers/101 |
| Umeng Analytics | | https://reports.exodus-privacy.eu.org/trackers/119 |
| Yueying Crash SDK | Analytics, Crash reporting | https://reports.exodus-privacy.eu.org/trackers/448 |

## 敏感凭证泄露检测

| 可能的密钥 |
|---|
| 百度统计的=> "BaiduMobAd_STAT_ID" : "4d0309bb6d" |
| 百度统计的=> "BaiduMobAd_CHANNEL" : "Baidu Market" |
| 友盟统计的=> "UMENG_APPKEY" : "5e439a2acb23d2dbec000210" |

| |
|---|
| 友盟统计的=> "UMENG_CHANNEL" : "cm_short_video" |
| "library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1" |
| 0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78 |
| EhMLxwqi3KFK4qzJlZG5ktmUVbTzT |

## 免责声明及风险提示: