南明离火
移动应用检测平台

ANDROID 静态分析报告

□□□□□ • v1.2.3

分析日期: 2025-07-05 07:00:29

应用概览

文件名称:	ds.apk
文件大小:	30.18MB
应用名称:	□□□□□
软件包名:	com.qsruvmx.jcdhxu
主活动:	not_found_main_activity!!
版本号:	1.2.3
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:	54/100 (中风险)
杀软检测:	18 个杀毒软件报毒
MD5:	6764fd2bddf45649efc7111bfdbf6fff
SHA1:	72af310ac55974427c9ad68893bbe52f37a4bdea
SHA256:	db6bbe55ef66b91872b7873f6718b9eb5a9ffaf00c32871db57d1e1f3288bc44

分析结果严重性分布

高危	中危	信息	安全	关注
0	15	1	1	1

四类组件导出状态统计

Activity组件：20个，其中export的有： 5个
Service组件：10个，其中export的有： 3个
Receiver组件：11个，其中export的有： 4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: CN=awjer, OU=awvwnn8, O=awgc7, L=ccs9, ST=serggp
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-15 05:09:10+00:00
有效期至: 2056-06-07 05:09:10+00:00
发行人: CN=awjer, OU=awvwnn8, O=awgc7, L=ccs9, ST=serggp
序列号: 0x1
哈希算法: sha256
证书MD5: 10ba10dc50fd541de95afabe39d2de20
证书SHA1: 605120d7fb88f8ec5bab4e4618a16e048f6923f0
证书SHA256: ccf64e6bfb34e0160cba8eccd5b145b0832ede5776a9c1b6c2a6c8d84d2d1ebd
证书SHA512:
1b433ff7284a9bfce98a9c004a55519e9df873ea6eee5fb0bdd085ca3386a29326f07cb09327e01d4477b254d732511524b6c4d8bb78be5d951068d081eb8cb

公钥算法: rsa
密钥长度: 2048
指纹: 2bd55761cc7134a187e4f03db3b74ae533b0eabfd39654380f30a091d68b33c8
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.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录
android.permission.READ_CONTACTS	危险	读取联系人信息	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.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.WRITE_CALL_LOG	危险	写入通话记录	允许应用程序写入（但不读取）用户的通话记录数据。
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.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_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_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.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.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
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.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.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.FOREGROUND_SERVICE_MEDIA_PROJECTION	普通	允许媒体投影的前台服务	允许常规应用程序使用类型为“mediaProjection”的 Service.startForeground。
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
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.READ_PHONE_NUMBERS	危险	允许读取设备的电话号码	允许读取设备的电话号码。这是READ PHONE STATE授予的功能的一个子集，但对即时应用程序公开。
android.permission.MANAGE_OWN_CALLS	普通	使呼叫应用程序能够管理自己的呼叫	允许通过自我管理的ConnectionService API管理自己的调用的调用应用程序。
android.permission.ACTION_MANAGE_OVERLAY_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
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.SET_DEFAULT_DIALER	未知	未知权限	来自 android 引用的未知权限。
android.permission.ANSWER_PHONE_CALLS	危险	允许应用程序接听来电	一个用于以编程方式应答来电的运行时权限。
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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
com.android.alarm.permission.SET_ALARM	未知	未知权限	来自 android 引用的未知权限。
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。

可浏览 Activity 组件分析

ACTIVITY	INTENT

com.qsruvmx.jcdhxu.activity.CallActivity	Schemes: tel://,
com.qsruvmx.jcdhxu.activity.ActionActivity	Schemes: ddudolctg://,
com.qsruvmx.jcdhxu.activity.UserInfoActivity	Schemes: musrinfox://,

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: **15** | 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、Media Player 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，改使用加密协议。
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	Activity (com.qsruvmx.jcdhxu.MainActivity) 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。
4	Service (com.qsruvmx.jcdhxu.service.CallService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_INCALL_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。
5	Service (com.qsruvmx.jcdhxu.service.IComService) 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	Broadcast Receiver (com.qsruvmx.jcdhxu.receiver.CallReceiver) 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。
7	Broadcast Receiver (com.qsruvmx.jcdhxu.receiver.RebootReceiver) 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。
8	Broadcast Receiver (com.qsruvmx.jcdhxu.receiver.MegReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BROADCAST_SMS [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。
9	Activity (com.qsruvmx.jcdhxu.activity.CallActivity) 未受保护。 存在 intent-filter。	警告	检测到 Activity 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 被显式导出，存在安全风险。
10	Activity (com.qsruvmx.jcdhxu.activity.ActionActivity) 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	Activity (com.qsruvmx.jcdhxu.activity.UserInfoActivity) 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。
12	Activity (com.szz.jhb.ContactActivity) 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。
13	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。
14	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。
15	高优先级 Intent（2147483647） - {2} 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: **0** | 警告: **0** | 信息: **1** | 安全: **0** | 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

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/liblive.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	True info 二进制文件有以下加固函数: ['__vsnprintf_chk', '__strlen_chk', '__memcpy_chk', '__memmove_chk']	True info 符号被剥离
2	arm64-v8a/libZegoExpressEngine.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	True info 二进制文件有以下加固函数: ['__FD_SET_chk', '__FD_ISSET_chk', '__memcpy_chk', '__vsnprintf_chk', '__strlen_chk', '__memset_chk', '__memmove_chk', '__strcpy_chk', '__strncpy_chk', '__read_chk', '__strchr_chk', '__vsprintf_chk', '__FD_CLR_chk']	True info 符号被剥离

3	arm64-v8a/libzmmp.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	True info 二进制文件有以下加固函数: ['__memset_chk', '__strlen_chk', '__strncpy_chk']	True info 符号被剥离
4	arm64-v8a/libzmmp.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	True info 二进制文件有以下加固函数: ['__vsnprintf_chk', '__memcpy_chk', '__memmove_chk', '__strlen_chk']	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
00013	读取文件并将其放入流中	文件	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
00121	创建目录	文件 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
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
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	12/30	android.permission.READ_CALL_LOG android.permission.READ_CONTACTS android.permission.CALL_PHONE android.permission.WRITE_CALL_LOG android.permission.RECEIVE_BOOT_COMPLETED android.permission.READ_PHONE_STATE android.permission.SYSTEM_ALERT_WINDOW android.permission.WRITE_CONTACTS android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.VIBRATE android.permission.WAKE_LOCK
其它常用权限	7/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.ACCESS_WIFI_STATE android.permission.FOREGROUND_SERVICE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE

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

opt-oms.zego.cloud	安全	否	**IP地址:** 10.1.75.82 国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看: Google 地图
www.phishingeyes.com	安全	否	**IP地址:** 52.79.202.9 国家: 大韩民国 地区: 首尔teukbyeolsi 城市: 首尔 纬度: 37.566311 经度: 126.977003 查看: Google 地图
opt-sentry-prod.zego.cloud	安全	否	**IP地址:** 10.111.32.37 国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看: Google 地图
www.videolan.org	安全	否	**IP地址:** 213.36.253.2 国家: 法国 地区: 法兰西岛 城市: 巴黎 纬度: 48.859077 经度: 2.293486 查看: Google 地图
docs.zegocloud.com	安全	是	**IP地址:** 52.79.202.9 国家: 中国 地区: 香港 城市: 香港 纬度: 22.285521 经度: 114.157692 查看: 高德地图

URL 链接安全分析

URL信息	源码文件
• http://www.videolan.org/x264.html	lib/arm64-v8a/liblive.so
• 8.8.8.8 • file://localfile • 127.0.0.1 • http://opt-oms.zego.cloud/#/log-server/sdk-log/info? • 1.4.1.61 • http://25b9a45feb1179ba0b611574dbcbad93@opt-sentry-prod.zego.cloud/20 • http://d9473d8f56814fdbde0813c5a7ca4fe0@opt-sentry-prod.zego.cloud/5 • http://[redacted]1abfc03b02b530bcfa3585f77a@opt-sentry-prod.zego.cloud/15 • http://557b864a93526be167a768d8602dcfe6@10.10.9.218:16001/34 • 1.2.0.4 • https://docs.zegocloud.com/article/5547 • http://38598faa2bd5ac6f5c5dfcec7b4a7fa4@opt-sentry-prod.zego.cloud/9	lib/arm64-v8a/libZegoExpressEngine.so

• https://www.phishingeyes.com/agreement-of-use-privacy?lang=ko • https://www.phishingeyes.com/react-to-phishing?lang=ko • https://www.phishingeyes.com/agreement-of-provide-personal-info?lang=ko • https://www.phishingeyes.com/terms?lang=ko	lib/arm64-v8a/libzmmp.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
即构极速视频 SDK	即构	极速视频（Express Video）是一款实时的音视频互动服务产品，能够为开发者提供便捷接入、高可靠、多平台互通的音视频服务。通过低至 200 ms 的端到端平均时延、业内领先的保障弱网质量的 QoS 策略，并结合强大的 3A 处理能力，完美支持一对多、多对多的实时音视频通话、直播、会议等场景。

邮箱地址敏感信息提取

EMAIL	源码文件
38598faa2bd5ac6f5c5dfcec7b4a7fa4@opt-sentry-prod.zego.cloud 648d601abfc03b02b530bcfa3585f77a@opt-sentry-prod.zego.cloud 25b9ad5feb1179ba0b611574dbcbad93@opt-sentry-prod.zego.cloud d9473d8f56814fdbde0813c5a7ca4fe0@opt-sentry-prod.zego.cloud	lib/arm64-v8a/libZegoExpressEngine.so

敏感凭证泄露检测

可能的密钥
凭证信息=> "app_id" : "dasdefvvvxx xxyy"

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。