Evaluation Warning: The document was created with Spire.Doc for Python.

**BOE新鲜人（ 1.1.2版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | BOE新鲜人 |
| 版本 | 1.1.2 |
| 包名 | cn.mymax.manmanapp.jdf |
| 域名线索 | 19条 |
| URL线索 | 8条 |
| APP图标 |  |
| 分析日期 | 2025年6月17日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | cn.mymax.manmanapp.jdf\_19.apk |
| 文件大小 | 51.47MB |
| MD5值 | ab4d6ff7cb6b8e19c423db5455d85bdc |
| SHA1值 | a4f81c16dc52016bb1ac9be3ffe5b5d3ced5bdeb |
| SHA256值 | 944881ad4a41e6e0e542ce5a0dee9a0255870df8fe827fd27c49d7b2b462139c |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | BOE新鲜人 |
| 包名 | cn.mymax.manmanapp.jdf |
| 主活动Activity | cn.mymax.manman.FirstActivity |
| 安卓版本名称 | 1.1.2 |
| 安卓版本 | 19 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| newvector.map.baidu.com | IP: 111.206.209.177 所属国家: China 地区: Beijing 城市: Beijing  |
| client.map.baidu.com | IP: 111.206.209.119 所属国家: China 地区: Beijing 城市: Beijing  |
| rs.easemob.com | IP: 39.97.193.187 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| 60.205.13.54 | IP: 60.205.13.54 所属国家: China 地区: Beijing 城市: Beijing  |
| www.openssl.org | IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.ietf.org | IP: 104.16.45.99 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.apple.com | IP: 222.138.3.126 所属国家: China 地区: Henan 城市: Zhumadian  |
| sv0.map.bdimg.com | IP: 111.206.209.186 所属国家: China 地区: Beijing 城市: Beijing  |
| sv.map.baidu.com | IP: 111.206.209.186 所属国家: China 地区: Beijing 城市: Beijing  |
| www.webrtc.org | IP: 173.194.203.138 所属国家: United States of America 地区: California 城市: Mountain View  |
| wp.map.baidu.com | IP: 111.206.209.185 所属国家: China 地区: Beijing 城市: Beijing  |
| lame.sf.net | IP: 104.18.21.237 所属国家: United States of America 地区: California 城市: San Francisco  |
| its.map.baidu.com | IP: 153.3.237.86 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| api.map.baidu.com | IP: 111.206.208.72 所属国家: China 地区: Beijing 城市: Beijing  |
| v.map.baidu.com | IP: 111.206.209.185 所属国家: China 地区: Beijing 城市: Beijing  |
| d1.client.map.bdimg.com | IP: 101.72.203.35 所属国家: China 地区: Hebei 城市: Langfang  |
| vector0.map.bdimg.com | IP: 101.72.203.38 所属国家: China 地区: Hebei 城市: Langfang  |
| ns.adobe.com | 没有服务器地理信息.  |
| www.mob.com | IP: 180.188.26.28 所属国家: China 地区: Zhejiang 城市: Taizhou  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://www.mob.com  | 摸瓜V1引擎  |
| http://client.map.baidu.com/  | lib/armeabi/libBaiduMapSDK\_base\_v4\_0\_0.so  |
| http://api.map.baidu.com/s  | lib/armeabi/libBaiduMapSDK\_base\_v4\_0\_0.so  |
| http://api.map.baidu.com/  | lib/armeabi/libBaiduMapSDK\_base\_v4\_0\_0.so  |
| http://client.map.baidu.com/phpui2/  | lib/armeabi/libBaiduMapSDK\_base\_v4\_0\_0.so  |
| http://client.map.baidu.com/?qt=rg&mmproxyver=1&url=  | lib/armeabi/libBaiduMapSDK\_base\_v4\_0\_0.so  |
| http://client.map.baidu.com/imap/sdk/tj?qt=vmap  | lib/armeabi/libBaiduMapSDK\_map\_v4\_0\_0.so  |
| http://v.map.baidu.com/low/  | lib/armeabi/libBaiduMapSDK\_map\_v4\_0\_0.so  |
| http://v.map.baidu.com/indoorinside/  | lib/armeabi/libBaiduMapSDK\_map\_v4\_0\_0.so  |
| http://v.map.baidu.com/high/  | lib/armeabi/libBaiduMapSDK\_map\_v4\_0\_0.so  |
| http://newvector.map.baidu.com/grid\_vc/  | lib/armeabi/libBaiduMapSDK\_map\_v4\_0\_0.so  |
| http://vector0.map.bdimg.com/vecdata/  | lib/armeabi/libBaiduMapSDK\_map\_v4\_0\_0.so  |
| http://its.map.baidu.com:8003/its.php  | lib/armeabi/libBaiduMapSDK\_map\_v4\_0\_0.so  |
| http://wp.map.baidu.com/  | lib/armeabi/libBaiduMapSDK\_map\_v4\_0\_0.so  |
| http://api.map.baidu.com/sdkws/heatmap?  | lib/armeabi/libBaiduMapSDK\_map\_v4\_0\_0.so  |
| http://client.map.baidu.com/footmap/image.php?  | lib/armeabi/libBaiduMapSDK\_map\_v4\_0\_0.so  |
| http://sv.map.baidu.com/  | lib/armeabi/libBaiduMapSDK\_map\_v4\_0\_0.so  |
| http://sv0.map.bdimg.com/  | lib/armeabi/libBaiduMapSDK\_map\_v4\_0\_0.so  |
| http://client.map.baidu.com/phpui2/?  | lib/armeabi/libBaiduMapSDK\_map\_v4\_0\_0.so  |
| http://client.map.baidu.com/offline-search/?  | lib/armeabi/libBaiduMapSDK\_map\_v4\_0\_0.so  |
| http://d1.client.map.bdimg.com/offline-search/?  | lib/armeabi/libBaiduMapSDK\_map\_v4\_0\_0.so  |
| http://client.map.baidu.com/?qt=rg&mmproxyver=1&url=  | lib/armeabi/libBaiduMapSDK\_map\_v4\_0\_0.so  |
| http://www.apple.com/DTDs/PropertyList-1.0.dtd  | lib/armeabi/libcocos2dlua.so  |
| http://www.openssl.org/support/faq.html  | lib/armeabi/libcocos2dlua.so  |
| http://rs.easemob.com/easemob/server.json  | lib/armeabi/libhyphenate.so  |
| http://60.205.13.54/easemob/server.json  | lib/armeabi/libhyphenate.so  |
| https://rs.easemob.com/easemob/server.json  | lib/armeabi/libhyphenate.so  |
| http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01  | lib/armeabi/libhyphenate\_av.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time  | lib/armeabi/libhyphenate\_av.so  |
| http://lame.sf.net  | lib/armeabi/libhyphenate\_av\_recorder.so  |
| http://ns.adobe.com/xap/1.0/  | lib/armeabi/libimagepipeline.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| ftp@example.com  | lib/armeabi/libcocos2dlua.so  |
| ffmpeg-devel@ffmpeg.org  | lib/armeabi/libijkplayer.so  |

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: False v3 签名: False 找到 1 个唯一证书 主题: C=BJ, ST=BJ, L=BJ, O=MAX, OU=MAX, CN=HS 签名算法: rsassa\_pkcs1v15 有效期自: 2015-11-12 07:31:25+00:00 有效期至: 2040-11-05 07:31:25+00:00 发行人: C=BJ, ST=BJ, L=BJ, O=MAX, OU=MAX, CN=HS 序列号: 0x7120c263 哈希算法: sha256 md5值: 630926702436a0ddae2d842f55c5a779 sha1值: 0fe5d161b01b5fe69cb6900992533ce6383fe9b3 sha256值: 65861347c3129c92ad2b42a8ed83032963d9e979c80c8386cc959c525cd5cd9e sha512值: 67816874db1345e5a4e87f72754b6768cbc33b4b56018dc96a52e3199b2cb55283cba2ef1d5ee070e29a85317d87e45e23179e9b996af3a97daa7bbca19ea24d**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "Please\_enter\_a\_username" : "Please enter a username"  |
| "Two\_input\_password" : "Inconsistent password, please enter again!"  |
| "check\_result\_get\_token\_fail" : "Get token from server failed%1$s%2$s"  |
| "check\_result\_get\_token\_success" : "Get token from server success"  |
| "illegal\_user\_name" : "Illegal user name"  |
| "password" : "Password"  |
| "session" : "Conversation"  |
| "set\_custom\_appkey" : "Set custom App key"  |
| "ssdk\_instapaper\_pwd" : "密码"  |
| "ssdk\_weibo\_oauth\_regiseter" : "应用授权"  |
| "user\_name" : "User name"  |
| "ssdk\_instapaper\_pwd" : "Password"  |
| "ssdk\_weibo\_oauth\_regiseter" : "Authorization"  |
| "Please\_enter\_a\_username" : "请输入用户名"  |
| "Two\_input\_password" : "两次输入的密码不一致，请重新输入!"  |
| "check\_result\_get\_token\_fail" : "Token获取失败%1$s%2$s"  |
| "check\_result\_get\_token\_success" : "Token获取成功"  |
| "illegal\_user\_name" : "用户名不合法"  |
| "password" : "密码"  |
| "session" : "会话"  |
| "set\_custom\_appkey" : "自定义App key"  |
| "user\_name" : "用户名"  |
| "Please\_enter\_a\_username" : "请输入用户名"  |
| "Two\_input\_password" : "两次输入的密码不一致，请重新输入!"  |
| "illegal\_user\_name" : "用户名不合法"  |
| "password" : "密码"  |
| "session" : "会话"  |
| "user\_name" : "用户名"  |
| "Please\_enter\_a\_username" : "Пожалуйста, введите имя пользователя"  |
| "password" : "Пароль"  |
| "session" : "Диалог"  |
| "user\_name" : "Имя пользователя"  |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 此APP的危险动作**

| 向手机申请的权限 | 是否危险 | 类型  | 详细情况 |
| --- | --- | --- | --- |
| android.permission.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.ACCESS\_NETWORK\_STATE | 正常 | 查看网络状态 | 允许应用程序查看所有网络的状态 |
| android.permission.READ\_PHONE\_STATE | 危险 | 读取电话状态和身份 | 允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等 |
| android.permission.ACCESS\_WIFI\_STATE | 正常 | 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.CHANGE\_WIFI\_STATE | 正常 | 更改Wi-Fi状态 | 允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改 |
| android.permission.CHANGE\_CONFIGURATION | 系统需要 | 更改您的 UI 设置 | 允许应用程序更改当前配置,例如语言环境或整体字体大小 |
| android.permission.WAKE\_LOCK | 正常 | 防止手机睡眠  | 允许应用程序防止手机进入睡眠状态 |
| 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 | 读取外部存储器内容 | 允许应用程序从外部存储读取 |
| 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定数据。恶意应用可能会损坏你的系统的配置。 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| android.permission.ACCESS\_FINE\_LOCATION | 危险 | 精细定位（GPS） | 访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量 |
| android.permission.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| android.permission.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| android.permission.RECEIVE\_SMS | 危险 | 接收短信 | 允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示 |
| cn.mymax.manmanapp.jdf.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| android.permission.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.ACCESS\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，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.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.MODIFY\_AUDIO\_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| android.permission.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| android.permission.USE\_CREDENTIALS | 危险 | 使用帐户的身份验证凭据 | 允许应用程序请求身份验证令牌 |
| com.android.launcher.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_STICKY | 正常 | 发送粘性广播 | 允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定 |
| android.permission.REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS | 正常 |  | 应用程序必须持有的权限才能使用 Settings.ACTION\_REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS。 |
| android.permission.READ\_LOGS | 危险 | 读取敏感日志数据 | 允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息 |
| com.hyphenate.chatuidemo.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| cn.mymax.manmanapp.jdf.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| cn.mymax.manman.audiobook.AudioBookDetail\_Activity | **Schemes**: rtsp://, http://, **Mime Types:** video/\*, application/sdp, video/mp4, video/3gp, video/3gpp, video/3gpp2,  |
| cn.mymax.manman.audiobook.AudioPlayerActivity | **Schemes**: rtsp://, http://, **Mime Types:** video/\*, application/sdp, video/mp4, video/3gp, video/3gpp, video/3gpp2,  |
| cn.sharesdk.tencent.qq.ReceiveActivity | **Schemes**: tencent101470180://,  |
| com.mob.tools.MobUIShell | **Schemes**: line.1477692153://,  |

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**