南明离火
移动应用检测平台

ANDROID 静态分析报告

iVMS-5060 • v4.1.020171214

分析日期: 2025-05-10 23:23:55

应用概览

文件名称:	com.ivms.daoluyunshu.base_18.apk
文件大小:	16.5MB
应用名称:	iVMS-5060
软件包名:	com.ivms.daoluyunshu.base
主活动:	com.ivms.login.LoadingActivity
版本号:	4.1.020171214
最小SDK:	9
目标SDK:	9
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	36/100 (高风险)
跟踪器检测:	2/432
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	8b3da27884d52b8520e1af0d6c04dc18
SHA1:	d4065c5c94ca46e8ff8e68a41ee7ed96f85ce7fb
SHA256:	c20f1d81249bf5e24318a9812f75ba210adfdc1243e8cb8c0feedc6c4cd2574f

分析结果严重性分布

高危	中危	信息	安全	关注
6	10	1	1	2

四大组件导出状态统计

Activity组件：47个，其中export的有： 0个
Service组件：1个，其中export的有： 0个
Receiver组件：1个，其中export的有： 0个
Provider组件：0个，其中export的有： 0个

应用签名证书信息

二进制文件已签名
v1 签名: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: O=hikvision, CN=chen
签名算法: rsassa_pkcs1v15
有效期自: 2015-03-25 01:39:20+00:00
有效期至: 3013-07-26 01:39:20+00:00
发行人: O=hikvision, CN=chen
序列号: 0x57915f97
哈希算法: sha256
证书MD5: 262b0b274b4226a90615e377531864a4
证书SHA1: e12e80ef0e708bd6d0a1db89b40fdcbf14ec49f2
证书SHA256: 3a143cb8a98e06f43a22250ff55ba4290ac3de30154b3fb6a5f2526d9df3e55b
证书SHA512:
833e781bd6bf0b963352b2019eff252a2cd30fb08cbb90b10f98d3d49fb20eddd327ea55539ae761feaf9ec0905ed424bdb2d82ba11903f6cd1af69b67223dc0

公钥算法: rsa
密钥长度: 2048
指纹: 9aecf43e0d390b856327d331dce4002c7c3145da76c6e10ce6a7e2663332124b
找到 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.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.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.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.WRITE_OWNER_DATA	未知	未知权限	来自 android 引用的未知权限。
android.permission.CHANGE_CONFIGURATION	危险	改变UI设置	允许应用程序 允许应用程序更改当前配置，例如语言区域或整体的字体大小。
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.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户粗略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。

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.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.WRITE_SECURE_SETTINGS	签名(系统)	修改安全系统设置	允许应用程序修改系统的安全设置数据。普通应用程序不能使用此权限。
android.permission.ACCES_MOCK_LOCATION	未知	未知权限	来自 android 引用的未知权限。
com.android.launcher.permission.READ_SETTINGS	危险	读取桌面快捷方式	这种权限的作用是允许应用读取桌面快捷方式的设置。
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。
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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.BROADCAST_STICKY	普通	发送置顶广播	允许应用程序发送顽固广播，这些广播在结束后仍会保留。恶意应用程序可能会借此使手机耗用太多内存，从而降低其速度或稳定性。
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置方面的数据。恶意应用程序可借此破坏您的系统配置。
android.permission.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。

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	应用程序使用代码签名证书进行签名

Manifest 配置安全分析

高危: **2** | 警告: **0** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	Activity (com.ivms.imageManager.ImageDetailActivity) 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。
2	Activity（com.ivms.imageManager.ImageDetailActivity）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（9） 升级至 28 及以上以获得平台级防护。

代码安全漏洞检测

高危: **4** | 警告: **8** | 信息: **1** | 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 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
2	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
3	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
4	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

5	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
6	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
7	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
8	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
9	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
10	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
11	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

12	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 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	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	默认情况下，调用Cipher.getInstance("AES")将返回AES ECB模式。众所周知，ECB模式很弱，因为它导致相同明文块的密文相同	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

应用行为分析

编号	行为	标签	文件
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
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
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
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
00091	从广播中检索数据	信息收集	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
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
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
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

00012	读取数据并放入缓冲流	文件	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
00104	检查给定路径是否是目录	文件	升级会员：解锁高级权限
00112	获取日历事件的日期	信息收集 日历	升级会员：解锁高级权限
00147	获取当前位置的时间	信息收集 位置	升级会员：解锁高级权限
00075	获取设备的位置	信息收集 位置	升级会员：解锁高级权限
00137	获取设备的最后已知位置	位置 信息收集	升级会员：解锁高级权限
00115	获取设备的最后已知位置	信息收集 位置	升级会员：解锁高级权限
00062	查询WiFi信息和WiFi Mac地址	WiFi 信息收集	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
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00066	查询ICCID号码	信息收集	升级会员：解锁高级权限
00175	获取通知管理器并取消通知	通知	升级会员：解锁高级权限
00083	查询IMEI号	信息收集 电话服务	升级会员：解锁高级权限
00082	获取当前WiFi MAC地址	信息收集 WiFi	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
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

敏感权限滥用分析

类型	匹配	权限

恶意软件常用权限	11/30	android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.GET_TASKS android.permission.READ_PHONE_STATE android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.RECEIVE_BOOT_COMPLETED android.permission.WRITE_SETTINGS android.permission.MODIFY_AUDIO_SETTINGS
其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.CHANGE_WIFI_STATE android.permission.ACCESS_WIFI_STATE android.permission.BROADCAST_STICKY

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
www.andykhan.com	安全	否	**IP地址:** 213.171.195.105 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 英格兰 **城市:** 格洛斯特 **纬度:** 51.865681 **经度:** -2.243100 **查看:** Google 地图
a.tile.openstreetmap.org	安全	否	**IP地址:** 54.148.44.189 **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
www.openstreetmap.org	安全	否	**IP地址:** 54.148.44.189 **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
etherx.jabber.org	安全	否	**IP地址:** 208.68.163.210 **国家:** 美国 **地区:** 爱荷华州 **城市:** 蒙蒂塞洛 **纬度:** 42.238514 **经度:** -91.189705 **查看:** Google 地图

webrd02.is.autonavi.com	安全	是	**IP地址:** 222.186.18.249 国家: 中国 地区: 江苏 城市: 镇江 纬度: 32.209366 经度: 119.434372 查看: 高德地图
utility.arcgis.com	安全	否	**IP地址:** 3.169.252.28 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
geocode.arcgis.com	安全	否	**IP地址:** 54.148.44.189 国家: 美国 地区: 俄勒冈 城市: 波特兰 纬度: 45.523460 经度: -122.676482 查看: Google 地图
www.me-app.net	安全	是	**IP地址:** 222.186.18.249 国家: 中国 地区: 浙江 城市: 杭州 纬度: 30.293650 经度: 120.161583 查看: 高德地图
jabber.org	安全	否	**IP地址:** 54.39.46.213 国家: 加拿大 地区: 魁北克 城市: 蒙特利尔 纬度: 45.508839 经度: -73.587807 查看: Google 地图
dev.virtualearth.net	安全	否	**IP地址:** 13.107.246.71 国家: 美国 地区: 华盛顿 城市: 雷德蒙 纬度: 47.682899 经度: -122.120903 查看: Google 地图
www.amazon.co.uk	安全	否	**IP地址:** 18.164.178.14 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

c.tile.openstreetmap.org	安全	否	**IP地址:** 151.101.193.91 **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
zxing.appspot.com	安全	否	**IP地址:** 13.107.246.71 **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
www.jivesoftware.com	安全	否	**IP地址:** 23.235.209.143 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 弗吉尼亚海滩 **纬度:** 36.837925 **经度:** -76.093918 **查看:** Google 地图
b.tile.openstreetmap.org	安全	否	**IP地址:** 151.101.193.91 **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
www.opengis.net	安全	否	**IP地址:** 66.244.86.70 **国家:** 美国 **地区:** 印第安纳州 **城市:** 布鲁明顿 **纬度:** 39.220310 **经度:** -86.458237 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• http://10.17.36.119:5195/Background/register.php • http://10.17.36.119:5195/Background/reportLog.php	自研引擎-A
• http://a.tile.openstreetmap.org • http://www.openstreetmap.org/ • http://c.tile.openstreetmap.org • http://b.tile.openstreetmap.org	com/esri/android/map/osm/OpenStreetMapLayer.java
• javascript:isreadyforpullup • javascript:isreadyforpulldown	com/custom/widget/pulltorefresh/library/extras/PullToRefreshWebView2.java
• http://10.64.60.3:8712/gisplatform/services/rest/mapservice/baseline/query • http://10.64.60.3:8712/gisplatform/services/rest/tokenservice	com/ivms/map/hikgis/module/ConstantMaps.java

• https://www.me-app.net/api/1.0	com/ivms/base/GlobalApplication.java
• http://www.jivesoftware.com/xmlns/xmpp/properties	org/jivesoftware/smack/util/PacketParserUtils.java
• http://etherx.jabber.org/streams	org/jivesoftware/smack/PacketWriter.java
• http://jabber.org/protocol/compress	org/jivesoftware/smack/PacketReader.java
• http://utility.arcgis.com/sharing/kml	com/esri/core/internal/a/b/a.java
• http://geocode.arcgis.com/arcgis/rest/services/world/geocodeserver	com/esri/core/tasks/ags/geocode/Locator.java
• http://10.17.48.56/gisplatform/services/rest/tiledmapservice/govmap	com/ivms/map/hikgis/control/HikGisControl.java
• http://webrd02.is.autonavi.com/appmaptile?	com/ivms/map/gaode/gis/GaodeOnLineLayer.java
• http://www.opengis.net/wms	com/esri/core/internal/tasks/b/a.java
• http://jabber.org/protocol/compress'	org/jivesoftware/smack/XMPPConnection.java
• http://zxing.appspot.com/scan • http://www.google	com/ivms/scan/CaptureActivity.java
• http://www.andykhan.com/jexcelapi/index.html	jxl/demo/ReadWrite.java
• http://www.andykhan.com/jexcelapi • http://www.amazon.co.uk/exec/obidos/asin/0571058086/qid=1099836249/sr=1-3/ref=sr_1_11_3/202-6017285-1620664 • http://www.amazon.co.uk/exec/obidos/asin/0571058086qid=1099836249/sr=1-3/ref=sr_1_11_3/202-6017285-1620664	jxl/demo/Write.java
• http://www.jivesoftware.com/xmlns/xmpp/properties	org/jivesoftware/smack/packet/Packet.java
• http://www.andykhan.com/jexcelapi/index.html	jxl/read/biff/HyperlinkRecord.java
• http://dev.virtualearth.net/rest/	com/esri/android/map/bing/BingMapsLayer.java
• http://10.196.149.9:7072 • 10.64.49.39 • http://10.196.149.9:7071 • http://10.64.60.193:9080/hzmap • http://10.64.60.237/gisplatform • http://10.64.60.193:9080/gisplatform	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息

C++ 共享库	Android	在 Android 应用中运行原生代码。
SQLCipher	Zetetic	SQLCipher 是一个 SQLite 扩展，它提供数据库文件的 256 位 AES 加密能力。
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。

第三方追踪器检测

名称	类别	网址
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97
Baidu Map		https://reports.exodus-privacy.eu.org/trackers/99

敏感凭证泄露检测

可能的密钥
凭证信息=> "BING_KEY" : "ApEqyap8rTa4WTNCNv-3pAGQc7XUsHS6595tuDI3MHR5[illegible]5bqYGYhMYJq6Ae"
凭证信息=> "CLOUDMADE_KEY" : "BC9A493B41014CAABB98F0471D759707"
"password_value" : "123456"
"pwd_not_conform" : "undesirable"
"pwd_strength_mid" : "middle"
"pwd_strength_risk" : "risk"
"pwd_strength_strong" : "strong"
"pwd_strength_weak" : "weak"
"username_value" : "admin"
"password_value" : "123456"
"username_value" : "admin"

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。