



## ANDROID 静态分析报告



📱 AO网球最新版 · 17496

本报告由南明离火移动安全分析平台生成  
本报告由南明离火移动安全分析平台生成

分析日期: 2024-07-28 14:42:12

## i应用概览

文件名称:	493201.apk
文件大小:	1.53MB
应用名称:	AO网球最新版
软件包名:	com.aocudq4342.bqu4342dco
主活动:	com.example.administrator.myapplication.MainActivity
版本号:	1.496
最小SDK:	19
目标SDK:	26
加固信息:	未加壳
应用程序安全分数:	56/100 (中风险)
杀软检测:	29 个杀毒软件报毒
MD5:	4d0d6e333e8beb49dfec8af5ab16fe00
SHA1:	1111c8ad8404a895e77700e55b73fd7d8970e6f2
SHA256:	dcbf249ae54425c6e3598938c6bcb0163b4ac421fd153e31f19c1e02196cdf9b

## 📊 分析结果严重性分布

<b>🚨 高危</b>	<b>⚠️ 中危</b>	<b>i 信息</b>	<b>✓ 安全</b>	<b>🔍 关注</b>
1	1	0	1	1

## 📦 四大组件导出状态统计

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

v3 签名: False  
 v4 签名: False  
 主题: C=z, ST=zz, L=z, O=z, OU=zz, CN=lz  
 签名算法: rsassa\_pkcs1v15  
 有效期自: 2016-12-05 07:13:43+00:00  
 有效期至: 2116-11-11 07:13:43+00:00  
 发行人: C=z, ST=zz, L=z, O=z, OU=zz, CN=lz  
 序列号: 0x1f1ce198  
 哈希算法: sha256  
 证书MD5: 4cbb9b04a39193321c1c449974dbf868  
 证书SHA1: 887ce6b725b8f4a20e9c173bda9e7367fd2ed32d  
 证书SHA256: a825d92bee96c6d778f52354134b14403031209239f435d435ae1742a71fa495  
 证书SHA512:  
 6a04fe4e572a1b87dde0c8fe007df616e7de44eb8e72df1753e588a447e0f1520b25470cae8535d832a5f2ac07ecc0884c2e03b4e88faf195aa96d3199a8a7

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.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。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。

## 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: 1 | 警告: 0 | 信息: 1

标题	严重程度	描述信息
已签名应用	信息	应用程序已使用代码签名证书进行签名
应用程序存在Janus漏洞	高危	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

## Manifest配置安全分析

高危: 0 | 警告: 1 | 信息: 1 | 屏蔽: 0

序号	问题	严重程度	描述信息
----	----	------	------

1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 4.4-4.4.4, [minSdk=19]	信息	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。

## 代码安全漏洞检测

序号	问题	等级	参考标准	文件位置
----	----	----	------	------

## 敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	1/30	android.permission.WAKE_LOCK
其它常用权限	3/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE com.google.android.c2dm.permission.RECEIVE

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
m.96u.com	安全	是	<b>IP地址:</b> 43.135.34.219 <b>国家:</b> 中国 <b>地区:</b> 香港 <b>城市:</b> 香港 <b>纬度:</b> 22.285521 <b>经度:</b> 114.157692 <b>查看:</b> <a href="#">高德地图</a>

## URL 链接安全分析

URL 信息	源码文件
<ul style="list-style-type: none"> <li>https://m.96u.com</li> </ul>	com/example/administrator/myapplication/MainActivity.java
<ul style="list-style-type: none"> <li>https://m.96u.com</li> </ul>	自研引擎-S

## 第三方 SDK 组件分析

SDK名称	开发者	描述信息
-------	-----	------

File Provider	<a href="#">Android</a>	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。
---------------	-------------------------	---

## 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患。

© 2025 南明离火 - 移动安全分析平台自动生成

本报告由南明离火移动安全分析平台生成  
本报告由南明离火移动安全分析平台生成