

# 中国移动互联网安全信用认证中心

## APP安全检测报告



APP来源	浙江盘石信息技术股份有限公司
应用名称	火眼金睛
版本号	Android v2.5.7 iOS v2.6.1
应用类别	工具类
生成时间	2017-11-23
认证有效期	2017-01-24 至 2019-01-24
检测机构	中国移动互联网安全信用认证中心
技术支持机构	北京盘石信用管理有限公司

版权所有，侵权必究

## 目录

一、敏感权限.....	1
二、代码加密.....	1
三、动态防护.....	1
四、盗版检测.....	2
五、漏洞分析.....	2
六、实名认证.....	3
七、用户信息安全保护.....	3
八、信息内容审核管理.....	3
九、用户行为日志记录.....	3
十、杀毒引擎.....	4

## 一、敏感权限

项目	检测说明	检测结果	检测是否自带权限
访问相机	是否需要使用相机	通过	否
访问相册	是否需要访问相册	通过	否
访问麦克风	是否需要访问麦克风	通过	否
访问通讯录	是否需要访问通讯录	通过	是
获取定位	是否需要获取当前定位	通过	是
改变Wi-Fi	是否未经允许就自动改变Wi-Fi状态	通过	是

## 二、代码加密

项目	检测说明	检测结果
本地数据加密	本地数据加密	通过
URL编码加密	URL编码加密	通过
网络传输数据加密	网络传输数据加密	通过
方法体, 方法名高级混淆	方法体, 方法名高级混淆	通过
程序结构混排加密	程序结构混排加密	通过

## 三、动态防护

项目	检测说明	检测结果
SQL调试检测	SQL调试检测	通过
进程注入检测	进程注入检测	通过
解压检测	解压检测	通过
系统加速检测	系统加速检测	通过
java调试检测	java调试检测	通过

#### 四、 盗版检测

项目	检测说明	检测结果
签名校验检测	签名校验检测	通过
原始包检测	原始包检测	通过
重打包检测	重打包检测	通过

#### 五、 漏洞分析

项目	检测说明	检测结果
代码执行检测	代码执行检测	通过
高权限代码执行	高权限代码执行	通过
<b>Fragment</b> 漏洞检测	Fragment漏洞检测	通过
<b>Base64</b> 字符串加密检测	Base64字符串加密检测	通过
<b>Key Store</b> 保护检测	Key Store保护检测	通过
应用沙箱权限检测	应用沙箱权限检测	通过
隐式服务检测	隐式服务检测	通过
<b>AndroidManifest</b> “intent-filter”配置检测	AndroidManifest“intent-filter”配置检测	通过
<b>SSL</b> 证书检测	SSL证书检测	通过
<b>SSL</b> 证书相关漏洞检测	SSL证书相关漏洞检测	通过
<b>Android Manifest</b> 高危用户权限检测	Android Manifest 高危用户权限检测	通过
<远程代码执行> <b>Web View RCE</b> 漏洞检测	<远程代码执行>Web View RCE漏洞检测	通过

## 六、实名认证

项目	检测说明	检测结果
个人	对注册用户进行基于手机号码、短信认证和真实身份信息的认证(必须上传身份证正反面.)	信息填写正确, 个人用户实名认证成功
企业	对内容供给端进行严格的真实身份信息认证(必须上传营业执照.)	信息填写正确, 企业用户实名认证成功

## 七、用户信息安全保护

项目	检测说明	检测结果
个人信息	未经用户允许, 不可以读取通讯录、短信、通话记录	通过
方式	不能在软件未打开的情况下, 后台读取用户手机信息	通过
合法	不能在后台读取用户手机里其他软件的信息	通过
范围	APP有良好的保护机制, 不会被其他恶意软件读取信息	通过

## 八、信息内容审核管理

项目	检测说明	检测结果
文字内容方面	1.使用文字敏感词过滤系统	通过
	2.建立反垃圾信息机制	通过
	3. 用户举报	通过

## 九、用户行为日志记录

项目	检测说明	检测结果
记录	用户行为日志记录保留日期60天	通过

## 十、 杀毒引擎

供应商	是否存在病毒	位置
<b>Bkav</b>	否	Clean
<b>TotalDefense</b>	否	Clean
<b>MicroWorld-eScan</b>	否	Clean
<b>nProtect</b>	否	Clean
<b>CMC</b>	否	Clean
<b>CAT-QuickHeal</b>	否	Clean
<b>McAfee</b>	否	Clean
<b>Malwarebytes</b>	否	Clean
<b>Zillya</b>	否	Clean
<b>SUPERAntiSpyware</b>	否	Clean
<b>TheHacker</b>	否	Clean
<b>BitDefender</b>	否	Clean
<b>K7GW</b>	否	Clean
<b>K7AntiVirus</b>	否	Clean
<b>Baidu</b>	否	Clean
<b>Cyren</b>	否	Clean
<b>SymantecMobileInsight</b>	否	Clean
<b>Symantec</b>	否	Clean
<b>ESET-NOD32</b>	否	Clean
<b>TrendMicro-HouseCall</b>	否	Clean
<b>Avast</b>	否	Clean
<b>ClamAV</b>	否	Clean
<b>Kaspersky</b>	否	Clean
<b>Alibaba</b>	否	Clean
<b>NANO-Antivirus</b>	否	Clean
<b>ViRobot</b>	否	Clean
<b>Tencent</b>	否	Clean

<b>Ad-Aware</b>	否	Clean
<b>Trustlook</b>	否	Clean
<b>Emsisoft</b>	否	Clean
<b>Comodo</b>	否	Clean
<b>F-Secure</b>	否	Clean
<b>DrWeb</b>	否	Clean
<b>VIPRE</b>	否	Clean
<b>TrendMicro</b>	否	Clean
<b>McAfee-GW-Edition</b>	否	Clean
<b>Sophos</b>	否	Clean
<b>F-Prot</b>	否	Clean
<b>Jiangmin</b>	否	Clean
<b>Webroot</b>	否	Clean
<b>Avira</b>	否	Clean
<b>Fortinet</b>	否	Clean
<b>Antiy-AVL</b>	否	Clean
<b>Kingsoft</b>	否	Clean
<b>Arcabit</b>	否	Clean
<b>AegisLab</b>	否	Clean
<b>ZoneAlarm</b>	否	Clean
<b>Avast-Mobile</b>	否	Clean
<b>Microsoft</b>	否	Clean
<b>AhnLab-V3</b>	否	Clean
<b>ALYac</b>	否	Clean
<b>AVware</b>	否	Clean
<b>MAX</b>	否	Clean
<b>VBA32</b>	否	Clean
<b>WhiteArmor</b>	否	Clean
<b>Zoner</b>	否	Clean

<b>Rising</b>	否	Clean
<b>Yandex</b>	否	Clean
<b>Ikarus</b>	否	Clean
<b>GData</b>	否	Clean
<b>AVG</b>	否	Clean
<b>Panda</b>	否	Clean
<b>Qihoo-360</b>	否	Clean



报告生成时间：2017年11月23日