南明离火
移动应用检测平台

ANDROID 静态分析报告

移动护士站 • v1.69

分析日期: 2024-02-29 17:36:09

应用概览

文件名称:	移动护士站.apk
文件大小:	5.28MB
应用名称:	移动护士站
软件包名:	com.kyee.mobilenursestation
主活动:	com.kyee.nursestation.controller.WelcomeActivity
版本号:	1.69
最小SDK:	8
目标SDK:	19
加固信息:	未加壳
应用程序安全分数:	45/100 (中风险)
杀软检测:	AI评估：可能有安全隐患
MD5:	30025a4c88cb1b71e1c0db087a062464
SHA1:	df799d5e5a3a13dc25c858e8cf4897b5e95a1155
SHA256:	e888a6773937ea8f1733c5e9[illegible]0ad9b555dbf91790[illegible]70dee2b4d484

分析结果严重性分布

高危	中危	信息	安全	关注
3	15	11	1	0

四大组件导出状态统计

Activity组件：6个，其中export的有：3个
Service组件：4个，其中export的有：0个
Receiver组件：2个，其中export的有：2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: ST=shanghai, L=shanghai, O=kingyee, CN=kyee
签名算法: rsassa_pkcs1v15
有效期自: 2014-01-20 07:35:38+00:00
有效期至: 2039-01-14 07:35:38+00:00
发行人: ST=shanghai, L=shanghai, O=kingyee, CN=kyee
序列号: 0x1fce3096
哈希算法: sha256
证书MD5: 218b1cee22d4e84f04ceebbd6c6f339f
证书SHA1: 3c12af57c8885ed4ebc82e105ce5e0bfcdf10905
证书SHA256: c1e85ee7c5204f0ecfa85025189f77453a4c10d83ea78047f19a194ca4e9c7ee
证书SHA512:
500c267f92a429abebbc3413591972b31457c7783bb971bd14ebcc2731f811a12039a99025724c51eac650df062750e93f240cf0a91e4d8245e8f9c263d7dfd

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.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.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.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.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.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.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.MOUNT_FORMAT_FILESYSTEMS	危险	格式化外部存储设备	允许应用程序格式化可移除的存储设备。
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.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.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.READ_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。
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。
com.honeywell.decode.permission.DECODE	未知	未知权限	来自 android 引用的未知权限。

android.permission.BCREADER	未知	未知权限	来自 android 引用的未知权限。
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.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。

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: **1** | 警告: **9** | 信息: **0** | 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 2.2-2.2.3, [minSdk=8]	警告	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。
3	Activity (com.kyee.nursestation.controller.UserLoginActivity) 未被保护。存在一个 intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
4	Activity (com.kyee.nursestation.controller.NurseStationActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (19) 更新到 29 或更高版本以在平台级别修复此问题。
5	Activity (com.kyee.nursestation.controller.NurseStationActivity) 未被保护。[android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。

6	Activity (com.kyee.nursestation.views.menu.checkout.CheckoutDetailActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
7	Broadcast Receiver (com.kyee.nursestation.utils.scancontrol.BNBroadCastReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
8	Broadcast Receiver (com.kyee.nursestation.utils.scancontrol.EMHBroadCastReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
9	高优先级的Intent (1000) [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。
10	高优先级的Intent (1000) [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。

代码安全漏洞检测

高危: **1** | 警告: **5** | 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
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	启用了调试配置。生产版本不能是可调试的	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
4	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限

5	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
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	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	6/30	android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.SYSTEM_ALERT_WINDOW android.permission.RECEIVE_BOOT_COMPLETED android.permission.CAMERA android.permission.GET_TASKS
其它常用权限	7/46	android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.WRITE_EXTERNAL_STORAGE android.permission.MOUNT_FORMAT_FILESYSTEMS android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE

常用: 已知恶意软件广泛使用的权限。

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
api.wamp.ws	安全	否	**IP地址:** 89.31.143.90 **国家:** Germany **地区:** Bayern **城市:** Starnberg **纬度:** 48.001930 **经度:** 11.344160 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• http://132.147.160.62/CisServer/	com/kyee/nursestation/controller/UserLoginActivity.java
• http://202.120.40.105:8001/CisServer/	com/kyee/nursestation/global/CustomApplication.java
• http://api.wamp.ws/ • http://api.wamp.ws/error# • http://api.wamp.ws/error#generic • http://api.wamp.ws/error#internal • http://api.wamp.ws/procedure# • http://api.wamp.ws/topic#	de/tavendo/autobahn/Wamp.java
• http://api.wamp.ws/procedure#auth • http://api.wamp.ws/procedure#authreq	de/tavendo/autobahn/WampCraConnection.java
• https://git-wip-us.apache.org/repos/asf?p=incubator-cordova-android.git;a=blob;f=framework/res/xml/plugins.xml • javascript:try{cordova.fireDocumentEvent('pause');}catch(e){console.log('exception • http://api.wamp.ws/error#generic • javascript:cordova.fireDocumentEvent('searchbutton'); • http://logging.apache.org/log4j/1.2/faq.html#noconfig • http://api.wamp.ws/topic# • javascript:try{ • http://132.147.160.62/CisServer/ • http://api.wamp.ws/procedure# • file:/// • javascript:cordova.fireDocumentEvent('menubutton'); • http://202.120.40.105:8001/CisServer/ • http://api.wamp.ws/procedure#authreq • http://logging.apache.org/log4j/1.2/faq.html#unknown • javascript:try{cordova.require('cordova/channel').onDestroy.fire();}catch(e){console.log('exception • http://api.wamp.ws/error# • http://api.wamp.ws/procedure#auth • javascript:try{cordova.fireDocumentEvent('resume');}catch(e){console.log('exception • javascript:cordova.fireDocumentEvent('backbutton'); • http://api.wamp.ws/ • http://api.wamp.ws/error#internal	自研引擎分析结果

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。

敏感凭证泄露检测

可能的密钥
"elder_nusing_username" : "姓名"

"medicine_first_patlookuser" : "日常照顾者"
"user_name" : "请输入用户名"
"user_password" : "请输入密码"

免责声明及风险提示: