**康复机监控软件**

**网络安全研究报告**

编 制**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

审 核**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

批 准

发布日期

**目 录**

[1 基本信息 1](#_Toc12076)

[1.1 软件信息 1](#_Toc6570)

[1.2 数据架构 1](#_Toc31231)

[1.4网络安全补丁 5](#_Toc28099)

[1.5安全软件 5](#_Toc14240)

[2 实现过程 5](#_Toc59)

[3漏洞评估 5](#_Toc12995)

[4其他 6](#_Toc14677)

[5结论 6](#_Toc16784)

# 1 基本信息

## 1.1 软件信息

软件名称：康复机监控软件

型号规格：/

软件类型：Android软件

软件发布版本：V1

软件完整版本：V1.0.0

软件安全性级别：《医疗器械软件注册技术审查指导原则》所定义的轻微级别

## 1.2 数据架构

1.2.1产品预期使用的地点及其网络环境和数据流图

使用场景：在医疗机构和康复机构。

网络环境：蓝牙4.0。

数据流图如下：

康复机设备

康复机蓝牙数据交互APP

实时运动数据（如速度、阻力等）

运动参数（如设置阻力、痉挛等级、运动时间等）

数据流向为：

1、康复机监控软件将设置好的运动参数通过蓝牙传输至康复机设备；

2、康复机设备将患者的实时运动数据信息通过蓝牙传输给康复机监控软件软件。

注：康复机设备可以与本司设计开发的康复机监控软件软件（版本号：V1）进行双向数据传输，康复机监控软件软件不属于康复机设备的组成部分，但可与康复机设备配合使用。康复机监控软件软件须具备用户授权访问控制功能。

1.2.2可能影响其安全性和有效性的环境条件

使用时环境温度应保持稳定，应避免强电磁干扰（如手机电磁干扰等），使用时请与其他设备保持有效距离，在使用本设备时，不要使用其它电子设备，以免设备之间相互干扰，影响正常工作。

1.2.3数据类型

软件的传输数据类型为用户运动数据（运动距离、速度、时间、主被动，左右力量对比），无用户个人信息，属于非敏感医疗数据。

1.2.4电子接口

康复机设备通过无线蓝牙数据接口，与智能设备上安装的康复机监控软件连接，通过蓝牙4.0传输协议进行双向电子数据交换。

1.3网络安全能力

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 网络安全能力 | 是否  适用 | 实现方法 | 不适用理由 | 备注 |
| 1 | 自动注销（ALOF）：产品在无人值守期间阻止非授权用户访问和使用的能力。 | 不适用 | / | 产品为非无人值守设备 |  |
| 2 | 审核（AUDT）：产品提供用户活动可被审核的能力。 | 不适用 | / | 设备不保存运动数据，故不提供审核功能 |  |
| 3 | 授权（AUTH）：产品确定用户已获授权的能力。 | 适用 | 产品通过登录功能来确定用户已获授权的能力 | / |  |
| 4 | 节点鉴别（NAUT）：产品鉴别网络节点的能力。 | 适用 | 产品通过蓝牙功能对接入设备授权访问控制，利用设备蓝牙地址进行绑定，从而具备鉴别网络节点的能力。 | / |  |
| 5 | 人员鉴别（PAUT）：产品鉴别授权用户的能力。 | 适用 | 产品通过登录功能来确定用户已获授权的能力，从而拥有鉴别授权用户的能力 | / |  |
| 6 | 连通性（CONN）：产品保证连通网络安全可控的能力。 | 适用 | 产品利用设备蓝牙地址进行绑定，通过蓝牙协议进行双向数据传输，保证连通网络安全可控的能力。 | / |  |
| 7 | 物理防护（PLOK）：产品提供防止非授权用户访问和使用的物理防护措施的能力。 | 不适用 | / | 产品不保存运动数据，故不提供物理防护措施 |  |
| 8 | 系统加固（SAHD）：产品通过固化措施对网络攻击和恶意软件的抵御能力。 | 适用 | 产品通过采用自身功能和通过必备软硬件、外部软件环境等外部措施实现方式。软件严禁预留预期用途无关的配置，如某些非医疗预期用途的账号、通信端口、共享文件、服务等。通过上述措施来避免网络攻击者，实现系统加固。 | / |  |
| 9 | 数据去标识化与匿名化（DIDT）：产品直接去除、匿名化数据所含个人信息的能力。 | 不适用 | / | 产品无个人信息数据，故不提供数据去标识化与匿名化功能 |  |
| 10 | 数据完整性与真实性（IGAU）：产品确保数据未以非授权方式更改且来自创建者或提供者的能力。 | 适用 | 产品通过校验位来检查数据的完整性与真实性，不保存用户运动数据。与产品配合使用的APP软件，具备授权访问控制功能。 | / |  |
| 11 | 数据备份与灾难恢复（DTBK）：产品的数据、硬件或软件受到损坏或破坏后恢复的能力。 | 不适用 | / | 产品不保存运动数据，故不提供备份与灾难恢复功能 |  |
| 12 | 数据存储保密性与完整性（STCF）：产品确保未授权访问不会损坏存储媒介所存数据保密性和完整性的能力。 | 不适用 | / | 产品不保存运动数据，故不提供数据存储保密性与完整性功能。 |  |
| 13 | 数据传输保密性（TXCF）：产品确保数据传输保密性的能力。 | 适用 | 产品通过采用自身功能实现方式，在数据传输过程中，发送方按照传输协议进行组包和加密后传输:接收方先用过 解密后进行拆包提取实际数据信息。在传输过程中数据使用加密解密机制，具备确保数据传输保密性的能力。 | / |  |
| 14 | 数据传输完整性（TXIG）：产品确保数据传输完整性的能力。 | 适用 | 产品通过采用自身功能实现方式，在数据传输过程中，发送方按照传输协议进行组包过程中，添效加验位:接收方先用过解密后进行拆包，得到效验位后，进行数据的效验，效验通过才作为有效数据进行处理，因而具备确保数据传输完整性的能力。 | / |  |
| 15 | 网络安全补丁升级（CSUP）：授权用户安装/升级产品网络安全补丁的能力。 | 不适用 | / | 产品不提供网络安全补丁升级。 |  |
| 16 | 现成软件清单（SBOM）：产品为用户提供全部现成软件清单的能力。 | 不适用 | / | 产品未使用现成软件。 |  |
| 17 | 现成软件维护（RDMP）：产品在全生命周期中对现成软件提供网络安全维护的能力。 | 不适用 | / | 产品未使用现成软件。 |  |
| 18 | 网络安全使用指导（SGUD）：产品为用户提供网络安全使用指导的能力。 | 不适用 | / | 产品不提供网络安全使用指导。 |  |
| 19 | 网络安全特征配置（CNFS）：产品根据用户需求配置网络安全特征的能力。 | 不适用 | / | 产品不提供网络安全特征配置（CNFS） |  |
| 20 | 紧急访问（EMRG）：产品在预期紧急情况下允许用户访问和使用的能力。 | 不适用 | / | 产品不提供在紧急情况下允许用户访问和使用的能力。 |  |
| 21 | 远程访问与控制（RMOT）：产品确保用户远程访问与控制（含远程维护与升级）的网络安全的能力。 | 不适用 | / | 产品不提供远程访问与控制（RMOT） |  |
| 22 | 恶意软件探测与防护（MLDP）：产品有效探测、阻止恶意软件的能力。 | 不适用 | / | 产品不提供有效探测、阻止恶意软件的能力。 |  |

## 1.4网络安全补丁

不适用，本产品只在内网使用，没有网络安全补丁。

## 1.5安全软件

不适用。未经允许不会自动运行，不提供安全软件。

# 2 实现过程

**2.1风险管理**

见《附件4.2产品风险管理资料》。

**2.2需求规范**

见附件《4.5.1.4 软件需求文档》。

**2.3验证与确认**

本软件开发后系统测试进行了安全测试，根据网络规范要求来验证软件的网络安全需求（如保密性、完整性、可得性等特性）均已得到满足。具体见附件《4.5.1.2 系统测试计划与报告》。

**2.4可追溯性分析**

见附件《4.5.1 自研软件研究报告》。

**2.5维护计划**

见附件《4.5.1 自研软件研究报告》。

# 3漏洞评估

见附件4.5.2.1《 康复机设备网络安全漏洞自评报告》。

# 4其他

见附件4.5.2.2《标准传输协议和标准存储格式符合性声明》。

# 5结论

网络安全满足要求。软件的整个实现过程形成了相应的报告，软件的核心功能已得到有效验证，依据《产品风险管理资料》可知软件的安全有效性满足产品技术要求，受益是否大于风险。