**《...》**

**漏洞评估及网络安全验证方案**

**...有限公司**

目录

**漏洞评估及网络安全验证方案 1**

**...有限公司 1**

**1 简介 1**

1.1 目的 1

1.2 背景 1

1.3 参考文档 1

**2测试资源要求 1**

**3测试项目 1**

3.1漏洞评估 1

3.2网络安全能力测试 1

**4 测试结果输出 4**

# 1 简介

##  目的

该验证方案用于...软件网络安全的验证，本文适用于该项目开发人员和测试人员。

##  背景

针对...软件网络安全需求，进行测试计划编写。

##  参考文档

《医疗器械网络安全注册审查指导原则（2022年修订版）》

《医疗器械软件注册审查指导原则（2022年修订版）》

《人工智能医疗器械注册审查指导原则》

《...技术要求》

# 2测试资源要求

网络安全测试资源以实际为准。

软件正常运行所需的典型运行环境见下表：

...

# 3测试项目

## 3.1漏洞评估

3.1.1静态检测

使用卡巴斯基杀毒软件扫描软件安装文件以及相关文件。

3.1.2漏洞扫描

使用漏洞扫描软件工具(绿盟RSAS)的WEB应用扫描功能，对...软件进行漏洞扫描。按照CVSS漏洞等级对...软件扫描出的已知漏洞总数和已知剩余漏洞数进行评估。

## 3.2网络安全能力测试

| **序号** | **网络安全能力** | **网络安全能力描述** | **测试用例名称** | **测试步骤** | **预期结果** |
| --- | --- | --- | --- | --- | --- |
|  | ALOF自动注销 | 产品在无人值守期间阻止非授权用户访问和使用的能力。 |  |  |  |
|  | AUDT审核 | 产品提供用户活动可被审核的能力。 |  |  |  |
|  | AUTH授权 | 产品确定用户已获授权的能力。 |  |  |  |
|  | NAUT节点鉴别 | 产品鉴别网络节点的能力。 |  |  |  |
|  | PAUT人员鉴别 | 产品鉴别授权用户的能力。 |  |  |  |
|  | CONN连通性 | 产品保证连通网络安全可控的能力。 |  |  |  |
|  | PLOK物理防护 | 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。 |  |  |  |
|  | SAHD系统加固 | 产品通过固化措施对网络攻击和恶意软件的抵御能力。 |  |  |  |
|  | DIDT数据去标识化与匿名化 | 产品直接去除、匿名化数据所含个人信息的能力。 |  |  |  |
|  | IGAU数据完整性与真实性 | 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。 |  |  |  |
|  | DTBK数据备份与灾难恢复 | 产品的数据、硬件或软件受到损坏或破坏后恢复的能力。 |  |  |  |
|  | STCF数据存储保密性与完整性 | 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。 |  |  |  |
|  | TXCF数据传输保密性 | 产品确保数据传输保密性的能力。 |  |  |  |
|  | TXIG数据传输完整性 | 产品确保数据传输完整性的能力。 |  |  |  |
|  | CSUP网络安全补丁升级 | 授权用户安装/升级产品网络安全补丁的能力。 |  |  |  |
|  | SBOM现成软件清单 | 产品为用户提供全部现成软件清单的能力。 |  |  |  |
|  | RDMP现成软件维护 | 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。 |  |  |  |
|  | SGUD网络安全使用指导 | 产品为用户提供网络安全使用指导的能力。 |  |  |  |
|  | CNFS安全特性配置 | 产品根据用户需求配置网络安全特征的能力。 |  |  |  |
|  | EMRG紧急访问 | 产品在预期紧急情况下允许用户访问和使用的能力。 |  |  |  |
|  | RMOT远程访问与控制 | 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。 |  |  |  |
|  | MLDP恶意软件探测与防护 | 产品有效探测、阻止恶意软件的能力。 |  |  |  |

# 4 测试结果输出

根据漏洞扫描结果及网络安全能力测试结果输出验证报告。