**《...》**

**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**](#_Toc10615)

[**...有限公司 1**](#_Toc30570)

[**1 简介 1**](#_Toc6732)

[1.1 目的 1](#_Toc16869)

[1.2 背景 1](#_Toc14093)

[1.3 参考文档 1](#_Toc32175)

[**2测试资源要求 1**](#_Toc14761)

[**3测试项目 1**](#_Toc3980)

[3.1漏洞评估 1](#_Toc1055)

[3.2网络安全能力测试 1](#_Toc18592)

[**4 测试结果输出 4**](#_Toc17823)

# 1 简介

## 目的

用于对《...软件》网络安全的验证。

## 范围

针对《...软件》网络安全需求，进行测试计划编写与验证。主要包括以下内容：

1.网络安全能力

2.漏洞扫描

3.渗透测试

4.资产评估（若适用）

5.威胁建模（若适用）

6.脆弱性评估（若适用）

7.整体风险评估（若适用）

## 参考文件

《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》（若适用）

《...技术要求》

YY/T 1843-2022《医用电气设备网络安全基本要求》

# 2样品信息

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安全检测

使用安全软件扫描软件安装文件以及相关文件。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **软件名称** | **完整版本** | **供应商** | **运行环境** |
|  | 360杀毒软件 | 13（13.0.0.2002） | 北京奇虎科技有限公司 | Win 7/Win 10 |

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** | **安全能力项** | **网络安全能力说明** | **网络安全能力要求** | **测试用例** | **备注** |
| --- | --- | --- | --- | --- | --- |
| 1 | 4.1.4存储保密性 | *阐述系统有关敏感数据的存储保密性。*  *对产品该方面的能力或者实现方式详细描述。如不适用，请阐明理由。* | 4.3.1保密性 | *Test CaseXXX- Test CaseXXX* |  |
| 2 | 4.1.5传输保密性 | *阐述系统有关传输保密性的陈述，尤其是对敏感数据的考量。对产品该方面的能力或者实现方式详细描述。如不适用，请阐明理由。* | 4.3.1保密性 | *Test CaseXXX* |  |
| 3 | 4.1.6健康数据中的身份信息 | *阐述系统包含的个人敏感数据的类型，以及选取的个人敏感数据类型的依从性文件。对产品该方面的能力或者实现方式详细描述。如不适用，请阐明理由。* | 4.3.2健康数据中的身份信息 | *Test CaseXXX* |  |
| 4 | 4.1.7用户访问控制 | *阐述系统的用户访问控制，包括采用的用户访问控制措施以及这种控制措施的细节，如：远程访问，其中也包括了远程控制和用于维护的远程访问。对产品该方面的能力或者实现方式详细描述。如不适用，请阐明理由。* | 4.3.3用户访问控制 | *Test CaseXXX* |  |
| 5 | 4.1.8用户授权 | *阐述产品是否提供了用户身份验证的陈述，若提供了这种手段，则应陈述所有现有用户身份及其访问权限。对产品该方面的能力或者实现方式详细描述。如不适用，请阐明理由。* | 4.3.4用户授权 | *Test CaseXXX* |  |
| 6 | 4.1.9自动注销 | *阐述有关自动注销的陈述。若产品部署于医疗服务提供组织，某些场景自动注销功能会影响可得性，制造商需要考虑这样的场景下自动注销功能所带来的风险。对产品该方面的能力或者实现方式详细描述。如不适用，请阐明理由。* | 4.3.5自动注销 | *Test CaseXXX* |  |
| 7 | 4.1.10紧急访问 | *产品是否提供了紧急访问，若提供了用于紧急访问的功能，则应陈述该功能的必要性，以及使用该功能的同时如何兼顾完整性。对产品该方面的能力或者实现方式详细描述。如不适用，请阐明理由。* | 4.3.6紧急访问 | *Test CaseXXX* |  |
| 8 | 4.1.11传输完整性 | *阐述传输过程中保证敏感数据完整性的策略。对产品该方面的能力或者实现方式详细描述。如不适用，请阐明理由。* | 4.3.7传输完整性 | *Test CaseXXX* |  |
| 9 | 4.1.12节点认证 | 1. *适用时，阐述节点认证。 2)若设备部署在HDO，身份验证策略宜灵活适应本地HDO信息技术网络的安全策略。 3)若产品包含了多个节点，且节点有可能被产品之外的其他节点接入，则应考虑这种情况的节点认证。 注：节点认证的方式一般包括了白名单、用户名/口令、证书等。*   *如不适用，请阐明理由。* | 4.3.8节点认证 | *Test CaseXXX* |  |
| 10 | 4.1.13恶意软件探测与防护 | *产品是否支持恶意软件探测与防护，包括安全产品的配置方式，探测到恶意软件时的处理和修复方式。 注：安全产品一般包括杀毒软件、辅助安全软件和防火墙等。*  *如不适用，请阐明理由。* | 4.3.9恶意软件探测与防护 | *Test CaseXXX* |  |
| 11 | 4.1.14系统与应用软件固化 | *若需要实施固化，阐述系统与应用软件固化的措施，这样的措施用于保证仅提供与预期用途相关的资源和服务，并保证尽可能少的维护活动。 注：这样的措施的举例：关闭/禁用与产品预期用途无关的访问端口；关闭/禁用与产品预期用途无关的服务；关闭/禁用与产品预期用途无关的应用软件；限制/控制资源层的访向；限制/控制任务层的访问。*  *如不适用，请阐明理由。* | 4.3.10系统与应用软件固化 | *Test CaseXXX* |  |
| 12 | 4.1.15物理防护 | *阐述数据交换端口的物理防护。 若产品部署在HDO，必须阐述产品有关物理防护，哪怕该物理设备的资产不属于制造商，若存在相关的风险，也需要进行陈述。*  *如不适用，请阐明理由。* | 4.3.11物理防护 | Test CaseXXX |  |
| 13 | 4.1.16抗抵赖性 | *阐述产品有关抗抵赖性的内容。*  *如不适用，请阐明理由。* | 4.3.12抗抵赖性 | *Test CaseXXX* |  |
| 14 | 4.1.17健康数据的完整性和真实性 | *应包含有关保证健康数据的完整性和真实性的陈述。*  *如不适用，请阐明理由。* | 4.3.13健康数据的完整性和真实性 | *Test CaseXXX* |  |
| 15 | 4.1.18可核查性 | *应包含产品有关可核查性内容及其手段的陈述。例如：成功或失败的登录尝试；健康数据的访问、修改和删除；健康数据的导入、导出；安全配置的更改(如更改用户身份验证的凭据、更改有效的用户账户列表)：远程访问(可能是用于产品维护或实现预期用途)；紧急访问。*  *如不适用，请阐明理由。* | 4.3.14可核查性 | *Test CaseXXX* |  |
| 16 | 4.1.19数据备份与灾难恢复 | *阐述产品进行数据备份与灾难恢复策略。目标是为了确保医疗业务持续进行，也可以利用第三方和操作系统的功能进行数据备份。*  *如不适用，请阐明理由。* | 4.3.15数据备份与灾难恢复 | *Test CaseXXX* |  |
| 17 | 4.1.20维护性 | 1. *描述产品维护计划中与网络安全有关的维护内容，并明确网络安全维护的责任方。 2)若产品中包含了第三方组件，应在网络安全能力说明中列出第三方组件的信息。第三方组件可能包括操作系统、第三方的动态链接库、第三方的应用程序等现成软件。第三方组件的信息可以是标识、来源及版本号等。 3)描述产品的网络安全升级。升级可能包括安全补丁文件的安装、安全产品的升级。*   *如不适用，请阐明理由。* | 4.3.16维护性 | *Test CaseXXX* |  |

# 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。