ICS 11.040.99
C 30

团　　体　　标　　准

T/CSBME 007—2019

医疗器械网络安全质量评价方法

Quality Evaluation Method of Cybersecurity in Medical Devices

2019-11-15发布　　2019-12-15实施

中国生物医学工程学会　发布

目　　次

前　　言

本标准按GB/T 1.1-2009《标准化工作导则 第1部分：标准的结构和编写》给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国生物医学工程学会提出。

本标准由中国生物医学工程学会医疗器械标准工作委员会归口。

本标准起草单位：中国食品药品检定研究院、上海市医疗器械检测所、河南驼人医疗器械集团有限公司、秦皇岛市惠斯安普医学系统股份有限公司

本标准主要起草人：王晨希、黄嘉华、张冲、王佳名

引　言

随着互联网技术在医疗领域的广泛应用，越来越多的医疗器械具备网络连接功能以进行电子数据交换或远程控制，这在提高医疗服务质量与效率的同时也面临着网络攻击的威胁。医疗器械网络安全出现问题不仅可能会侵犯患者隐私，而且可能会产生医疗器械非预期运行的风险，导致患者或使用者受到伤害甚或死亡。因此，医疗器械网络安全是医疗器械安全性和有效性的重要组成部分。

网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可得性的能力。

本标准的目的是对处于网络环境中的医疗器械产品（包含软件和硬件）从网络安全的角度如何进行评估和考量。

医疗器械网络安全质量评价方法

1 范围

本标准规定了医疗器械产品进行网络安全评价时的技术要求和试验方法。

本标准适用于同外部有数据交换功能的有源医疗器械产品，此类产品一般是指独立医疗器械软件和包含医疗器械软件组件的医疗器械。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25000.10-2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE）第10部分：系统与软件质量模型

GB/T 25000.51-2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE）第51部分：就绪用软件产品（RUSP）的质量要求和测试细则

GB/T 29246-2012 信息安全技术 信息安全管理体系概述和词汇

YY/T 0316-2016 医疗器械 风险管理对医疗器械的应用

3 术语和定义

3.1 制造商 manufacturer

在上市和/或投入服务前。对医疗器械的设计、制造、包装或作标记、系统的装配或者改装医疗器械负有责任地自然人或法人，不管上述工作是由他自己或由第三方代其完成。

[YY/T 0316-2016，定义2.8]

3.2 随附文件 accompanying documents

随同医疗器械的，为医疗器械安装、使用和维护的责任方提供信息以及为操作者或使用者提供信息，特别是关于安全信息的文件

[YY/T 0316-2016，定义2.1随附文件]

3.3 外部接口 EXTERNAL INTERFACE

预期设计成允许医疗器械本身之外的实体访问的接口，举例来说，用户接口、远程接口、本地接口、无线接口和文件导入

[UL2900-1,定义3.17]

3.4 访问控制 access control

确保对医疗器械产品的访问是基于业务和安全要求进行授权和限制的手段

[GB/T 29246—2017，定义2.1，做了修改，范围限定]

3.5 可核查性 Accountability

确保可从一个实体的行为唯一地追溯到该实体的特性。

[ISO/IEC 21827:2008，定义 3.1]

3.6 鉴别 authentication

为一个实体声称的特征是正确的而提供的保障措施。

[GB/T 29246—2017，定义 2.7]

3.7 授权 authorization

根据预先认可的安全策略，赋与主体可实施相应行为权限的过程。

[GB/T 25069—2010，定义 2.1.33，做了修改]

3.8 保密性 confidentiality

信息不能对未授权的个人、实体或过程可用或泄露的特性。

[GB/T 29246—2017，定义 2.12]

3.9 数据交换 data interchange

为满足不同平台或应用间数据资源的传送和处理需要，依据一定的原则，采取相应的技术，实现不同平台和应用间数据资源的流动过程。

[GB/T 35274—2017，定义 3.11]

3.10 加密 encryption

通过一种密码算法产生密文的（可逆的）数据转换，即隐藏数据的信息内容。

[ISO/IEC 10116:2017，定义 3.6]

3.11 防火墙 firewall

设置在网络环境之间的一种安全屏障。它由一台专用设备或若干组件和技术的组合组成。从一个网络环境到另一个网络环境的，以及反向的，所有通信流均通过此安全屏障，只有按照本地安全策略定义的、已授权的通信流才允许通过。

[ISO/IEC 27033-1:2015，定义 3.12]

3.12 运行环境 operational environment

由操作系统和硬件平台组成的、模块安全运行所需的所有软硬件的集合。

[ISO/IEC 19790:2015，定义 3.83]

3.13 口令 password

用于实体鉴别的秘密的字、短语、数字或字符序列，是一个被默记的弱秘密。

[ISO/IEC 11770-4:2017，定义 3.27]

3.14 权限 permission

对一个主体访问某一资源的授权。

[ISO/IEC 29146:2016，定义 3.8]

4 技术要求

4.1 随附文件应包含以下要求：

a) 随附文件应包含产品所有功能描述，尤其是与安全相关管理功能的描述；

b) 随附文件应明确所有与数据交换相关的物理接口和逻辑接口（远程接口、串口、无线接口和文件传输协议）；

c) 随附文件应明确数据的存储格式；

d) 若适用，随附文件应明确产品安装以及运行过程中与安全相关的运行环境配置的要求（杀毒软件、防火墙、操作系统更新补丁）；

e) 若适用，随附文件应明确产品应明确所有软件组件的名称

f) 随附文件应明确软件版本；

g) 随附文件应明确与安全相关的并被产品的日志功能记录的事件；

h) 若适用，随附文件应明确产品的版权控制或认证方法；

i) 随附文件应对用户管理的每一项数据所对应的软件信息安全级别给出的必要的信息。

4.2 产品设计要求

4.2.1 配置管理应包含以下要求：

a）制造商在产品的生存周期过程中，需求文档、设计文档、测试文档、用户文档等应置于配置管理之下，产品开发工具应在配置管理范围内；

b)产品的生存周期过程中，制造商应有一个配置管理系统保持对改变代码安全和变更的控制。

4.2.2 产品开发应包含以下要求：

a) 制造商在产品设计研发过程中，应保证数据的完整性。例如，检查数据更新的规则、多重输入的正确处理、返回状态的检查、中间结果的检查、异常值输入检查、处理更新的正确性检查等；

b) 内部代码检查时，应解决潜在的安全缺陷，关闭和取消所有后门；

c) 产品的数据如口令和秘钥不应以明文形式存储。

4.3 产品功能要求

4.3.1 访问控制应包含以下要求：

a) 当产品的操作或管理服务会影响到产品安全时，需要做用户身份验证和授权；

b) 产品的用户身份验证服务应当有会话机制或其他机制来阻止持续的验证，并且会话应当是可配置的；

c) 通过外部接口或无线进行服务访问时，访问之前需要进行身份验证；

d) 产品应该支持用户名和口令的长度、复杂度和更新频率的等设置；

e) 产品基于角色访问控制机制，产品应具备管理员权限的角色，此类权限不能赋予其他用户；

f) 产品应具备管理用户功能：通过对用户的增删改查，赋予和修改权限；

g) 软件应能防止对程序和数据的未授权访问（不管是无意的还是有意的）；

h) 软件应能识别出对结构数据库或文件完整性产生损害的事件，且能阻止该事件，并通报给授权用户；

i) 软件应能对保密数据进行保护，只允许授权用户访问。

4.3.2 可核查性应包含以下要求：

a) 产品应具备安全事件的日志功能，如登录成功与失败、用户认证的改变、有效用户的改变和软件更新成功与否等；

b) 产品的安全相关日志应存储在本地磁盘，并且非授权用户不能删除和更改。

4.3.3 产品升级应包含以下要求：

a)产品在设计和实施过程中应能保证软件可以正常升级，如果软件升级失败，应能回滚到之前的版本；

b)产品在安装软件更新之前，应能确认任何软件加密更新的可靠性和完整性，产品更新应该离线环境下进行，离线产品更新模式也应能支持可靠性和完整性的确认；

c)产品初始化过程中，产品应提示用户对系统默认设置的修改，比如初始密码的更改。

4.3.4 接口可靠性

产品应保证经接口传输数据的保密性和完整性。

5 符合性评价细则

5.1 随附文件符合性评价

实际检查随附文件，明确相关内容，验证其符合性。

5.2 产品设计要求符合性评价

5.2.1 配置管理

检查配置管理相关文件，验证其符合性。

5.2.2 产品开发

检查产品研发相关文件，验证其符合性。

5.3 产品功能要求符合性评价

5.3.1 访问控制

实际操作产品功能，验证其符合性。

5.3.2 可核查性

实际操作查看产品日志，验证其符合性。

5.3.3 产品升级

进行产品升级和更新安装，验证其符合性。

5.3.4 接口可靠性

使用漏洞扫描工具，验证接口的可靠性。

参 考 文 献

[1]《医疗器械软件注册技术审查指导原则》（原国家食品药品监督管理总局2015年第50号通告）

[2]《医疗器械网络安全注册技术审查指导原则》（原国家食品药品监督管理总局2017年第13号通告）

[3]《中华人民共和国计算机信息系统安全保护条例》（中华人民共和国国务院令第147号）

[4] 中华人民共和国互联网信息办公室《国家网络安全事件应急预案》（中网办发文〔2017〕4号）

[5]《医疗器械网络安全审查指导原则实施指南》 （北京市药品监督管理局）