人工智能医疗器械创新合作平台

医疗器械网络安全漏洞识别与评估方法

人工智能医疗器械创新合作平台

2023-09-10

目次

前言

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。

本文件由人工智能医疗器械创新合作平台提出并归口。

本文件起草单位：中国信息通信研究院、推想医疗科技股份有限公司、上海西门子医疗器械有限公司、北京谊安医疗系统股份有限公司、北京天智航医疗科技股份有限公司。

本文件主要起草人：崔日宏、赵阳光、李曼、郭金凤、于湍、汪志鹏、苗宇、陈媛。

引言

具备网络连接功能的医疗器械，其运行的网络环境通常信息流比较复杂，存在着许多安全方面的风险，网络安全漏洞便是其中典型的风险之一。通过网络安全漏洞渗透到医疗器械中的恶意攻击，不仅会造成医疗器械运行出现故障，同时也可能造成医疗数据的泄露。实施漏洞管理可帮助医疗器械降低其网络安全所面临的威胁，而定期进行漏洞评估、漏洞维护等工作，则是减轻医疗器械网络安全风险的有效方法。

本文件的编制，旨在提供一种对医疗器械网络安全漏洞识别与评估的方法。

医疗器械网络安全漏洞识别与评估方法

1 范围

本文件描述了医疗器械网络安全漏洞识别与评估的过程，为医疗器械注册申请人和第三方评估机构提供了医疗器械网络安全漏洞评估的方法指南。

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 20984-2022 信息安全技术信息安全风险评估规范

GB/T 25069-2022 信息安全技术 术语

GB/T 28458-2020 信息安全技术 网络安全漏洞标识与描述规范

3 术语和定义、缩略语

3.1 术语和定义

3.1.1

端口 port

连接的端点。

注：在互联网协议的语境下，端口是传输控制协议（TCP）连接或用户数据报协议（UDP）消息的逻辑信道端点。基于 TCP 或 UDP 的应用协议，通常已分配默认端口号，如为超文本传输协议（HTTP）的端口号是 80。

［来源：GB/T 25069-2022,3.130］

3.1.2

访问控制 access control

一种确保数据处理系统的资源只能由经授权实体以授权方式进行访问的手段。

［来源：GB/T 25069-2022,3.147］

3.1.3

固件 firmware

功能上独立于主存储器，通常存储在只读存储器（ROM）中的指令和相关数据的有序集。

［来源：GB/T 25069-2022,3.225］

3.1.4

过滤 filtering

依照所规定的准则，接受或拒绝数据流通过某一网络的过程。

［来源：GB/T 25069-2022,3.235］

3.1.5

基于角色的访问控制 role-based access control

一种对某一角色授权，许可其访问相应对象的访问控制方法。

［来源：GB/T 25069-2022,3.263］

3.1.6

威胁 threat

可能对系统或组织造成危害的不期望事件的潜在因素。

［来源：GB/T 25069-2022,3.628］

3.1.7

主机 host

在基于传输控制协议/互联网协议（TCP/IP）的网络(如互联网)中，可设定地址的系统或计算机。

［来源：GB/T 25069-2022,3.803］

3.2 缩略语

CVSS:通用漏洞评分系统(Common Vulnerability Scoring System)

CVE:通用漏洞披露（Common Vulnerabilities and Exposure）

CNVD:中国国家信息安全漏洞共享平台（China National Vulnerability Database）

CNNVD: 中国国家信息安全漏洞库（China National Vulnerability Database of Information

Security）

4 漏洞扫描评估过程

医疗器械网络安全漏洞评估是对医疗器械网络安全的系统性审查，用于发现存在于医疗器械网络中的现有漏洞，确定漏洞的等级和危害程度。

网络安全漏洞评估主要有三个目的：

1. 评估产品是否存在网络安全方面的漏洞。

2. 为每个漏洞确定风险等级。

3. 根据漏洞的分布情况与风险等级，采取相应的措施以提升产品的网络安全性能。

在漏洞评估的过程中，漏洞扫描是确认医疗器械及其网络环境中是否存在潜在漏洞的实用方法，扫描结果能够帮助医疗器械注册申请人了解其产品网络安全所存在的问题，并做出有依据性的评估。

漏洞风险等级的确定参考 CVSS 评分规则，即“通用漏洞评分系统”。 CVSS 是用于评估系统安全漏洞严重程度的一个行业公开标准。漏洞风险等级评分为 10 分—0 分，漏洞评分越高，表明漏洞被攻击的复杂度越低，漏洞被利用所需要的技术能力越低，漏洞被利用后对系统的影响程度越高。

漏洞评估主要包括下列几个过程：

1. 评估范围分析
2. 确定漏洞扫描策略
3. 执行漏洞扫描
4. 漏洞扫描检测结果评估
5. 已知剩余漏洞的维护

4.1 评估范围分析

对于医疗器械网络安全漏洞的评估，不仅针对医疗器械产品本身，还应综合考虑产品实际使用时所处的环境，产品技术要求中所描述的必备软硬件、运行环境也应在评估的范围之内。

在进行医疗器械网络安全漏洞扫描评估时，注册申请人根据产品技术要求的内容，确保产品运行所必需的其他医疗器械软件、医用中间件及医疗器械硬件产品处在正常的配置和运

行条件下。

同时注册申请人在进行网络安全漏洞扫描评估时，应确保医疗器械运行在产品技术要求所规定的典型运行环境中，包括硬件配置、外部软件环境、必备软件、网络条件等。

4.2 漏洞扫描策略

在进行网络安全漏洞扫描之前，首先应确定产品的结构和组成，根据不同的产品结构和组成类型，从而确定相应的扫描检测评估方法。

如果产品运行在通用计算平台上，使用 Windows 或 Linux 等通用操作系统，且是基于网络的部署方式（包括局域网和广域网），漏洞扫描时使用基于网络的扫描方式。基于网络的扫描通过网络探测医疗器械，扫描的范围包括医疗器械产品及其所使用的网络环境。

如果产品是单机部署，而非基于网络的方式，则在漏洞扫描时使用基于主机的扫描方式。基于主机的扫描针对医疗器械产品自身，主要是对产品内置系统和应用程序的漏洞扫描。

如果产品属于嵌入式软件，系统软件和应用软件运行在嵌入式平台上，此类软件设计时需要在通用计算机平台上搭建专门的开发环境，使用专门的开发工具来开发应用程序，通过交叉编译，将程序烧录到目标平台上，这种情形通过对固件文件进行检测评估。

4.2.1 基于网络部署扫描策略

基于网络的漏洞扫描是从外部攻击者的角度对目标网络和产品进行扫描，应探测目标设备、操作系统、数据库及应用服务中存在的漏洞，以及目标系统使用的某些协议或开放的某些服务是否存在相应的漏洞。

基于广域网或局域网的扫描，漏洞扫描工具通过获取可访问的 IP 地址，接入其对应的网络中进行扫描。对于混合部署方式，漏洞扫描工具应分别接入其相应的使用网络中进行扫描。

医疗器械注册申请人或第三方评估机构在进行漏洞扫描前，需要了解被扫描对象所在网络部署情况，对于基于网络的漏洞扫描，需要获得被测试方的授权。

由于很多基于网络的漏洞扫描工具只支持进行某种协议的漏洞扫描，在进行基于网络的漏洞扫描时，医疗器械注册申请人或第三方评估机构需结合被扫描对象的应用特点及使用环境，恰当地选择扫描工具。

4.2.2 基于主机扫描策略

基于主机的漏洞扫描主要是从医疗器械系统用户的角度进行漏洞检测。这类医疗器械通常内置操作系统并安装医疗器械软件，通过使用者访问的方式进行使用，基于主机的扫描可以发现系统软件、中间件、注册表、用户配置、端口及开放服务等方面存在的漏洞。

对于部分不含有网络连接或远程访问与控制的医疗器械（常见如体外诊断类医疗器械），但存在非网络接口的其他电子接口（如串口、并口、USB 口、视频接口、音频接口等）或通过存储媒介（如光盘、移动硬盘、U 盘）进行数据交换，这种情况不对传输协议进行扫描，而是对相应电子接口的调用过程进行扫描。

基于主机的漏洞扫描，应根据不同的检测目标，如 Windows、Linux 的区别等，使用恰当的扫描工具，或在扫描工具上进行不同的配置。

4.2.3 嵌入式软件扫描策略

基于嵌入式软件的扫描，可以在不执行程序代码的情况下，通过静态分析程序特征以发现漏洞。

由于固件程序涉及知识产权，很少公开源代码，在这种情况下需要通过对固件文件进行逆向工程，再通过程序静态分析技术进行分析。

基于嵌入式软件的漏洞检测，除了应用程序外，还应包含引导加载程序、系统内核、文件系统等必备环境。

4.3 执行扫描

4.3.1 网络部署扫描和主机扫描

应按照产品技术要求描述的内容，使被测产品运行在典型使用环境中。

在进行漏洞扫描之前，医疗器械注册申请人应开放所有使用的端口，开放相应的安全策略（如关闭防火墙等），使扫描工具与被测对象之间处于一种无过滤的通信状态，以扫描到完整的目标。

对于基于 B/S（Brower/Server，浏览器/服务器）架构的产品，对服务器端主机进行扫描；对于基于 C/S（Client/Server，客户机/服务器) 架构的产品，应对客户端和服务器端主机分别进行扫描。

漏洞扫描通常分为以下三个阶段：

第一阶段：发现扫描目标

对于基于网络部署的情形，通过将漏洞扫描工具接入产品使用的网络环境中探测到目标主机。

对于基于单机部署的情形，通过将漏洞扫描工具与医疗器械产品直连或内置于医疗器械中，从而探测到扫描目标。

第二阶段：搜寻目标信息

当扫描工具发现目标后进一步搜集目标信息，包括操作系统类型、开放的端口、运行的服务、使用的协议类型等。

对于基于 B/S 架构的产品，扫描的对象还应包括服务器端 Web 应用程序，并且进行扫描过程中登录系统的测试账户应保证能够遍历到系统的所有功能。

第三阶段：扫描测试

根据搜集到的信息，由漏洞扫描工具向搜寻到的目标发送请求信息、返回分析信息，从而最终确定是否存在安全漏洞。

4.3.2 嵌入式软件扫描

基于嵌入式软件的扫描，应使用相应的工具对嵌入式软件固件文件进行扫描分析，整个分析流程主要分为三个阶段：

第一阶段：识别固件结构体系，提取出待分析的目标程序；

第二阶段：识别固件中存在的成分，如操作系统、第三方库文件、应用程序等；

第三阶段：通过静态分析技术对固件成分进行分析，并与分析工具中内置的漏洞库进行匹配，找出待测软件中存在的漏洞。

对于移动医疗设备，使用移动计算机终端，漏洞评估时对其应用软件的安装包文件进行扫描检测。如果应用软件可以运行在不同的终端环境，如 iOS 系统、Android 系统等，需对不同环境下的安装包文件进行扫描检测。如果移动医疗设备使用通用计算机终端，则采用基于主机或网络部署的方式进行扫描检测。

5 漏洞扫描结果评估

医疗器械注册申请人或第三方评估机构在对医疗器械产品完成扫描检测后，应对该次扫描检测的结果进行描述，记录检测过程中的信息，说明漏洞分布情况，并输出漏洞信息和评估结果。

5.1 概况说明

医疗器械注册申请人或第三方评估机构在漏洞扫描结束后，应记录被测产品的基本信息（产品名称、规格型号、软件版本、生产日期等），输出被测产品已知剩余漏洞的数量及其危险等级。

5.2 漏洞分布

对于经扫描后发现的已知漏洞，医疗器械注册申请人或第三方评估机构应描述在哪些端口、协议、服务下出现了漏洞，并说明漏洞名称、相应漏洞危险等级等信息。

5.3 漏洞详情

对于经扫描后发现已知的剩余漏洞，医疗器械注册申请人或第三方评估机构应描述剩余漏洞的详情，包括漏洞名称、漏洞的详细描述、基于漏洞库的漏洞编号（如 CVE、CNNVD、CNVD）、CVSS 评分等。对于未被分配编号的漏洞，可基于漏洞分级规则判断漏洞详情。

5.4 被测产品信息

医疗器械注册申请人或第三方评估机构进行漏洞评估时应记录被测产品所使用的的操作系统及版本，在扫描过程中被识别到的端口信息（端口号、协议类型、服务类型、状态），以及被识别到安装的软件的信息（软件名称、版本号）等。

对于嵌入式软件，应记录被测产品的操作系统、CPU 架构、固件大小、文件系统等内容。

5.5 CVSS 评分标准

医疗器械注册申请人或第三方评估机构进行漏洞评估时应明确漏洞风险等级的评定标准，根据 CVSS 的评分标准以确定发现漏洞的风险值以及被测医疗器械产品的网络安全风险。

5.6 扫描工具信息

医疗器械注册申请人或第三方评估机构进行漏洞评估时应明确漏洞扫描软件工具信息、漏洞库信息（基于国家信息安全漏洞库或互认的国际信息安全漏洞库）的基本信息。

6 已知剩余漏洞的维护方案

根据扫描后的已知剩余漏洞及其分布情况，医疗器械注册申请人应针对剩余漏洞的具体信息、漏洞的风险等级、漏洞出现的位置、漏洞修复的难易程度、漏洞修复的紧迫性等方面，并结合风险管理综合分析剩余漏洞对产品安全性方面的影响，确定补偿剩余漏洞的网络安全策略，制定剩余漏洞维护方案。

参考文献

[1] GB/T 30276-2020 信息安全技术网络安全漏洞管理规范[S]

[2] GB/T 28458-2020 信息安全技术—网络安全漏洞标识与描述规范[S]

[3] GB/T 30279-2020 信息安全技术网络安全漏洞分类分级指南[S]

[4] ISO/IEC 29147:2018, Information Technology-Security Techniques - Vulnerability Disclosure [S]

[5] ISO/IEC 30111:2013, Information Technology - Security Techniques - Vulnerability Handling Processes [S]