ICS 35.030
CCS L 80

# 中华人民共和国国家标准

GB/T 20278—2022
代替 GB/T 20278—2013，GB/T 20280—2006

# 信息安全技术　网络脆弱性扫描产品安全技术要求和测试评价方法

**Information security technology—Security technical requirements and testing assessment approaches for network vulnerability scanners**

2022-03-09 发布　　2022-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

# 目　　次

前言 …… Ⅰ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 1
5　网络脆弱性扫描产品描述 …… 2
6　安全技术要求 …… 2
6.1　概述 …… 2
6.2　基本级安全要求 …… 5
6.3　增强级安全要求 …… 11
7　测试评价方法 …… 20
7.1　测试环境 …… 20
7.2　测试工具 …… 20
7.3　基本级测试评价方法 …… 21
7.4　增强级测试评价方法 …… 36
参考文献 …… 59

# 前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替GB/T 20278—2013《信息安全技术　网络脆弱性扫描产品安全技术要求》和GB/T 20280—2006《信息安全技术　网络脆弱性扫描产品测试评价方法》，与GB/T 20278—2013相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了“网络脆弱性扫描产品描述”的内容（见第5章）；
b) 增加了“扫描报文标识”的要求（见6.2.1.5.3和6.3.1.5.3）；
c) 增加了“并发扫描”的要求（见6.2.1.7和6.3.1.7）；
d) 增加了“支撑系统安全”的要求（见6.2.2.4和6.3.2.5）；
e) 增加了“通信保密性”的要求（见6.3.2.4）；
f) 增加了“环境适应性要求（有则适用）”的内容，其中主要是明确了产品对IPv6的支持能力，包括支持纯IPv6网络环境的扫描能力、IPv6网络环境下的自身管理能力以及双协议栈的要求（见6.2.3和6.3.3）；
g) 增加了“测试评价方法”的内容（见第7章）；
h) 删除了“扫描IP地址限制”的要求（见2013年版的8.1.8）；
i) 删除了“易用性”的要求（见2013年版的8.2.2.2）；
j) 修改了“脆弱性扫描内容”，将原标准中要求的15项扫描要求重新整理分为5类扫描要求（见6.2.1.2和6.3.1.2，2013年版的7.1.2），在增强级中还提出了对云环境和工控设备目标对象的扫描要求（见6.3.1.2.6和6.3.1.2.7）；
k) 修改了各级的“安全保证要求”为“安全保障要求”（见6.2.4和6.3.4，2013年版的7.3和8.3）。

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专利的责任。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：公安部第三研究所、北京神州绿盟科技有限公司、网神信息技术（北京）股份有限公司、北京天融信网络安全技术有限公司、启明星辰信息技术集团股份有限公司、上海国际技贸联合有限公司、中国网络安全审查技术与认证中心、西安交大捷普网络科技有限公司、北京中科网威信息技术有限公司、上海市信息安全测评认证中心、工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）、新华三技术有限公司、中国电子科技集团公司第十五研究所（信息产业信息安全测评中心）、国家工业信息安全发展研究中心、陕西省网络与信息安全测评中心、国网新疆电力有限公司电力科学研究院、中国科学院信息工程研究所、中国电力科学研究院有限公司信息通信研究所、中国信息通信研究院、远江盛邦（北京）网络安全科技股份有限公司、北京通和实益电信科学技术研究所有限公司、上海斗象信息科技有限公司、深圳市联软科技股份有限公司、北京知道创宇信息技术股份有限公司。

本文件主要起草人：顾建新、宋好好、陆臻、顾健、沈亮、尹航、陈昕宇、熊毅、秦兰、曹宁、申永波、何建锋、宋伟、徐佟海、郭永振、杨洪起、刘健、刘志尧、巨腾飞、李明轩、陈佳、闫兆腾、严敏辉、许子先、于忠臣、闻蕾、谢忱、侯俊、崔兆。

本文件及其所替代文件的历次版本发布情况为：

——2006年首次发布为GB/T 20278—2006，2013年第一次修订；
——本次为第二次修订，并入了GB/T 20280—2006《信息安全技术　网络脆弱性扫描产品测试评价方法》的内容。

# 信息安全技术　网络脆弱性扫描产品安全技术要求和测试评价方法

## 1　范围

本文件规定了网络脆弱性扫描产品的安全技术要求和测试评价方法。

本文件适用于脆弱性扫描产品的设计、开发与测试。

## 2　规范性引用文件

下列文件中的内容通过文中的规范化引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 25069　信息安全技术　术语

## 3　术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

**扫描　scan**

使用技术工具对目标系统进行探测，查找目标系统中存在安全弱点的过程。

3.2

**网络脆弱性扫描　network vulnerability scan**

通过网络对目标系统安全弱点进行远程探测，检查和分析其安全脆弱性，从而发现可能被入侵者利用的安全弱点，并提出一定的防范和补救措施建议。

3.3

**旗标　banner**

应用程序发送的一段信息。

注：通常包括欢迎语、应用程序名称和版本等信息。

3.4

**支撑系统　supporting system**

支撑网络脆弱性扫描设备运行的操作系统。

## 4　缩略语

下列缩略语适用于本文件。

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

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

FTP：文件传输协议(File Transfer Protocol)