ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20278—2013
代替 GB/T 20278—2006

信息安全技术
网络脆弱性扫描产品安全技术要求

Information security technology—
Security technical requirements for network vulnerability scanners

2013-12-31 发布　　2014-07-15 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 20278—2006《信息安全技术　网络脆弱性扫描产品技术要求》，本标准与 GB/T 20278—2006 的主要差异如下：

——标准名称修改为《信息安全技术　网络脆弱性扫描产品安全技术要求》；

——修改了“网络脆弱性扫描”的定义（见 3.3）；

——删除了“NIS 服务的脆弱性”（见 2006 版的 7.3.1.8）；

——删除了“数据库脆弱性”（见 2006 版的 7.3.1.18）；

——删除了“RPC 端口”（见 2006 版的 7.3.4.1）；

——删除了“NT 服务”（见 2006 版的 7.3.4.5）；

——删除了“报警功能”（见 2006 版的 7.4.4.1）；

——删除了“安装与操作控制”（见 2006 版的 7.5）；

——删除了“与 IDS 产品的互动”“与防火墙产品的互动”“与其他应用程序之间的互动”（见 2006 版的 7.7.4.2、7.7.4.3、7.7.4.4 和 8）；

——删除了“性能要求”；

——新增了在产品升级过程中升级安全措施要求；

——新增了扫描结果的比对分析功能；

——在产品自身安全要求中新增了鉴别数据保护、鉴别失败处理、超时锁定或注销、远程管理等功能；

——调整了标准的整体结构，按照产品安全功能要求、自身安全要求和安全保证要求三部分描述，同时，细化了产品自身安全的要求项，明确了审计功能要求的内容。

本标准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。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心、启明星辰信息技术有限公司、北京中科网威信息技术有限公司。

本标准主要起草人：顾建新、陆臻、俞优、顾健、赵婷、王志佳、王红虹、明旭。

信息安全技术
网络脆弱性扫描产品安全技术要求

1 范围

本标准规定了网络脆弱性扫描产品的安全功能要求、自身安全要求和安全保证要求，并根据安全技术要求的不同对网络脆弱性扫描产品进行了分级。

本标准适用于网络脆弱性扫描产品的研制、生产和检测。

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 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 18336.3—2008 信息技术 信息技术安全性评估准则 第3部分：安全保证要求

GB/T 25069—2010 信息安全技术 术语

3 术语和定义

GB 17859—1999 和 GB/T 25069—2010 中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的安全隐患的过程。

3.2

脆弱性 vulnerability

网络系统中可能被利用并造成危害的弱点。

3.3

网络脆弱性扫描 network vulnerability scan

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

3.4

旗标 banner

由应用程序发送的一段信息，通常包括欢迎语、应用程序名称和版本等信息。

4 缩略语

下列缩略语适用于本文件。

CGI：公共网关接口(Common Gateway Interface)

CVE：通用脆弱性知识库(Common Vulnerabilities and Exposures)