

ICS 35.040
CCS L 80



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 20278-2013

**Information security technology -- Security technical
requirements for network vulnerability scanners**

信息安全技术 网络脆弱性扫描产品安全技术要求

(English Translation)

Issued on: December 31, 2013

Implemented on: July 15, 2014

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine of the People's Republic of China**

Table of Contents

1 Scope...	5
2 Normative References...	5
3 Terms and Definitions...	5
4 Abbreviations...	6
5 Level Classification of Network Vulnerability Scanners...	7
5.1 Description of Level Classification...	7
5.2 Level Classification...	7
6 Service Environment...	10
7 Security Technical Requirements for Basic-level...	11
7.1 Security Function Requirements...	11
7.2 Self-security Requirements...	17
7.3 Security Assurance Requirements...	19
8 Security Technical Requirements for Enhanced-level...	23
8.1 Security Function Requirements...	23
8.2 Self-security Requirements...	31
8.3 Security Assurance Requirements...	34

Foreword

This Standard was drafted according to the rules in GB/T 1.1-2009.

This Standard replaces GB/T 20278-2006 "Information Security Technology Technique Requirement for Network Vulnerability Scanners". The main differences in this Standard over GB/T 20278-2006 are as follows.

- The name of the standard was changed to "Information Security Technology - Security Technical Requirements for Network Vulnerability Scanners";
- The definition of "network vulnerability scan" was modified (see 3.3);
- "vulnerability of NIS service" (see 7.3.1.8 of 2006-edition) was deleted;
- "vulnerability of database" was deleted (see 7.3.1.18 of 2006-edition);
- "RPC port" was deleted (see 7.3.4.1 of 2006-edition);
- "NI service" was deleted (see 7.3.4.5 of 2006-edition);

- "alarm function" was deleted (see 7.4.4.1 of 2006-edition);
- "installation and operation control" was deleted (see 7.5 of 2006-edition);
- "interaction with IDS product", "interaction with fire wall product", "interaction with other application programs" were deleted (see 7.7.4.2, 7.7.4.3, 7.7.7.4 and 8 of 2006-edition);
- "performance requirements" was deleted;
- The requirement of upgrading security measures during product upgrading was added;
- The function of comparison and analysis between scanning results was added;
- Authentication data protection, authentication failure handling, timeout locking or logout, remote management and other functions were added in the self-security requirements of product;
- The integral structure of this Standard was adjusted; it is described according to the product security function requirements, self-security requirements and security assurance requirements; in addition, the requirement items of product self-security were detailed, and the contents of audit function requirements were defined.

This Standard was proposed by and shall be under the jurisdiction of National Technical Committee on Information Technology Security of Standardization Administration of China (SAC/TC 260).

Certain content of this document may involve patent. The issuing organization of this Standard shall not undertake the responsibility of identifying these patents.

Drafting organizations of this Standard. Quality Supervision Testing Center of Ministry of Public Security for Computer information system security product, Venustech Information & Technology Co., Ltd. AND Netpower Information & Technology Co., Ltd. Chief drafters of this Standard. Gu Jianxin, Lu Zhen, Yu You, Gu Jian, Zhao Ting, Wang Zhijia, Wang Honghong and Ming Xu.

Information Security Technology - Security Technical
Requirements for Network Vulnerability Scanners

1 Scope

This Standard specifies the security function requirements, self-security requirements and security assurance requirements of network vulnerability scanners, and classifies their levels according to different security technical requirements for network vulnerability scanners.

This Standard is applicable to the development, production and detection of network vulnerability scanners.

2 Normative References

The following documents are essential for the application of this document. For the dated references, only the dated editions apply to this document. For undated references, the latest editions (including amendments) apply to this document.

GB 17859-1999 Classified Criteria for Security Protection of Computer Information System

GB/T 18336.3-2008 Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 3.Security Assurance Requirements

GB/T 25069-2010 Information Security Technology - Glossary

3 Terms and Definitions

For the purpose of this Standard, the terms and definitions specified in GB/T 17859-

1999 and GB/T 25069-2010 as well as the following ones apply.

3.1

Scan

The process of using technical tools to detect the security risks that are existed in target system.

3.2

Vulnerability

The weakness in network system that may be made use of and cause hazard.

3.3

Network vulnerability scan

Remotely detect target system for security risk through network, inspect and analyze its security vulnerability thereby to find out the security loophole that may be utilized by intruder, and recommend some preventative and remedial measures.

3.4

Banner

A piece of information sent by application program, generally including words of welcome, application name and version, etc.

4 Abbreviations

For the purpose of this Standard, the following abbreviations apply.

CGI. Common Gateway Interface

CVE. Common Vulnerabilities and Exposures

DNS. Domain Name System

DoS. Denial of Service

FTP. File Transfer Protocol

IP. Internet Protocol

NETBIOS. NETwork Basic Input Output System

NFS. Network File System

POP3. Post Office Protocol 3

RPC. Remote Procedure Call

SMB. Server Message Block

SMTP. Simple Mail Transfer Protocol

SNMP. Simple Network Management Protocol

TCP. Transmission Control Protocol

UDP. User Datagram Protocol