

ICS 35.240
CCS A 90

GA

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

GA/T 1558-2019

**Information security technology - Security technical
requirements for IPv6-based high-performance network
vulnerability scanners**

信息安全技术 基于IPv6的高性能网络脆弱性扫描产品安全技术要求
(English Translation)

Issued on: January 1, 1970

Implemented on: April 19, 2019

Issued by: Ministry of Public Security

Table of Contents

Foreword	
1 Scope	
2 Normative references	
3 Terms and definitions	
4 Acronyms	
5 Product description of high-performance network vulnerability scanning based on IPv6	
6 General description	
6.1 Classification of safety technical requirements	
6.2 Security Level Classification	
7 Safety function requirements	
7.1 Information Acquisition	
7.2 Vulnerability scan content	
7.3 Scanning result analysis and processing	
7.4 Scan configuration	
7.5 Security of scanned objects	
7.6 Scan speed adjustment	
7.7 Concurrent scanning	
7.8 Upgrade capability	
7.9 Interaction requirements	
8 Requirements for own safety functions	
8.1 Identification and authentication	
8.2 Security management	
8.3 Audit logs	
9 Environmental adaptability requirements	
9.1 Supporting Pure IPv6 Network Environment	
9.2 Self-management in IPv6 network environment	
10 Security requirements	
10.1 Development	
10.2 Guiding documents	
10.3 Life cycle support	
10.4 Testing	
10.5 Vulnerability assessment	

11 Different security level requirements

11.1 Safety function requirements

11.2 Self-safety function requirements

11.3 Security requirements

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This standard was proposed by the Cyber Security Bureau of the Ministry of Public Security.

This standard is under the jurisdiction of the Information System Security Standardization Technical Committee of the Ministry of Public Security.

This standard was drafted. Computer Information System Security Product Quality Supervision and Inspection Center of the Ministry of Public Security.

1 Scope

This standard specifies the security function requirements, own security function requirements, and environmental protection requirements of high-performance network vulnerability scanning products based on IPv6.

Responsiveness requirements, security assurance requirements, and different security level requirements this standard applies to the design, development, and testing of IPv6 based network vulnerability scanning products.

2 Normative references

The following documents are essential for the application of this document. For dated references, only the dated version applies to this document.

For undated references, the latest version (including all amendments) applies to this document.

GB/T 18336.3-2015 Information technology security technology Information technology security assessment guidelines Part 3. Security assurance components GB/T 20278-2013 Information security technology Network security scanning product security technical requirements GB/T 25069-2010 Information Security Technology Terminology

3 Terms and definitions

The terms and definitions defined in GB/T 18336.3-2015, GB/T 20278-2013 and GB/T 25069-2010 and the following apply to this document Pieces.

Scan

Use technical tools to detect the target system and find the process of potential security risks in the target system.

Vulnerability

Vulnerabilities in network systems that can be exploited and cause harm.

Network vulnerability scan Remotely detect the hidden dangers of the target system through the network, check and analyze its security vulnerability, and find out that it may be used by intruders.

Potential safety hazards, and put forward certain precautions and remedial measures.

Flag banner

A piece of information sent by an application, usually including a welcome message, application name, and version.

4 Acronyms

The following abbreviations apply to this document.

CVE. Common Vulnerabilities and Exposures NETBIOS. NETwork Basic Input/Output System NFS. Network File System RPC. Remote Procedure Call SMB. Server Message Block

5 Product description of high-performance network vulnerability scanning based on IPv6

This standard proposes security function requirements and security assurance requirements for high-performance network vulnerability scanning products based on IPv6. Fragile network Sexual scanning products refer to software or software and hardware combinations that use scanning methods to detect potential security risks in the target network system this product can perform port scanning and inspection on specified devices in the target network system according to pre-defined policies or other requirements.

Check its open services, and further detect the configuration information of each service program and the existing security problems, so as to achieve the target network system System vulnerability scan. In addition, high-performance network vulnerability scanning products for next-generation Internet network environments also require support for IPv6,

IPv4/IPv6 transition technology network environment, with high processing performance, can achieve the simultaneous scanning of multiple targets.

The application environment of network vulnerability scanning products requires that the product and each network device or host of the scanned system should be in a connected state.

No other network security equipment is on the way.

6.1 Classification of safety technical requirements

This standard divides the security technical requirements of IPv6-based high-performance network vulnerability scanning products into security function requirements and self-security functions Requirements, environmental adaptability requirements, and security requirements. Among them, the security function requirement is to scan the vulnerability of high-performance network based on IPv6.

Specific requirements for the security functions that the product should have, including information acquisition, vulnerability scan content, scan result analysis and processing, scan configuration, Scanned object security, etc .; own security function requirements include identification and authentication, security management, and audit logs; security assurance requirements Specific requirements for the life cycle process of high-performance network vulnerability scanning products for IPv6, such as development, guidance documents, life cycle Support and testing.

6.2 Classification of security levels

The security level of a high-performance IPv6 based vulnerability scanning product is based on its security function requirements, its own security function requirements, and security the strength of the security requirements is divided into basic and enhanced levels. Among them, security requirements refer to GB/T 18336.3-2015.

7.1.1.1 TCP port

The product should be able to scan all TCP ports of the target device and check if they are open.

7.1.1.2 UDP port

The product should be able to scan all UDP ports of the target device and check if they are open.