GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

CCS L 80

GB 42250-2022

Information security technology - Security technical requirements of specialized cybersecurity products

信息安全技术 网络安全专用产品安全技术要求

Issued on: December 29, 2022 **Implemented on: July 01, 2023**

Issued by: State Administration for Market Regulation;
Standardization Administration of the People's Republic of China.

Table of Contents

Information security technology - Security technical requirements of specialized cybersecurity products

1 Scope

This document stipulates the security function requirements, own security requirements and security assurance requirements of specialized cybersecurity products.

This document is applicable to the research and development, production, service, and testing of specialized cybersecurity products sold or provided.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GB/T 25069, *Information security techniques -- Terminology*

3 Terms and definitions

For the purposes of this document, the terms and definitions defined in GB/T 25069 as well as the followings apply.

3.1 specialized cybersecurity products

Specialized hardware and software products used to secure networks.

NOTE: Including products that provide security protection capabilities in the form of services.

3.2 specialized cybersecurity products provider

Developers, producers or maintenance service providers of specialized cybersecurity products。

3.3 security domain

A collection of assets and resources subject to a common security policy.

[Source: GB/T 25069-2022, 3.36]

3.4 personal information

Various information related to identified or identifiable natural persons recorded electronically, excluding anonymized information.

3.5 user information

Electronically recorded information generated, collected, stored, transmitted, and processed by individuals, legal persons, or other organizations during the installation and use of specialized cybersecurity products.

NOTE: User information includes network traffic information, security status information, security configuration data, operation process logs and other information, as well as personal information.

3.6 malicious program

Programs with network attack functions such as destroying networks and information systems, interfering with the normal use of networks and information systems, stealing or maliciously encrypting network and system data.

NOTE: Malicious programs mainly include viruses, worms, Trojans, and other programs that affect the security and stable operation of the host, network, or system.

3.7 security flaw

Weaknesses that may affect the security of specialized cybersecurity products are introduced by errors in the design, development, configuration, production, operation and maintenance stages.

3.8 vulnerability

Weaknesses in specialized cybersecurity products that can be exploited by threats.

4 Security functional requirements

4.1 Access control

Specialized cybersecurity products with access control functions should have the following functions:

a) Support configuring access control policies;

NOTE: Different types of specialized cybersecurity products have different access control strategies. For example: network firewalls set access control policies based on source address, destination address, source port, destination port and network communication protocol. Virtual private network products set access control policies based on user security attributes. Security isolation and information exchange products set access control policies based on application layer protocols.

5 Own security requirements

5.1 Identification and authentication

Specialized cybersecurity products should have the following functions:

a) Identify and authenticate the user's identity, and the identity identifier is unique;

b) Ensure the confidentiality and integrity of identification information during transmission and storage;

c) When using the password authentication method, the identity authentication information complexity verification function and the regular replacement setting function are provided. Support forced modification of the default password or setting of a password when managing the product for the first time.

5.2 Own access control

Specialized cybersecurity products should have the following functions:

a) Assign accounts and permissions to users, distinguish administrator roles, and realize mutual constraints on management permissions;

b) Access control policies are configured by authorized subjects. Access control policies specify the rules for subjects to access objects.

5.3 Own security audit

Specialized cybersecurity products should have the following functions:

a) Monitor and record the operating status and important operations of the product itself;

b) Protect audit logs from unexpected deletion, modification, overwriting or loss;

c) Store audit logs in non-volatile storage media. Logs shall be kept for no less than six months.

5.4 Communication security

Specialized cybersecurity products should provide security measures to ensure the confidentiality and integrity of product remote management network communication data.

5.5 Support system security

Specialized cybersecurity products should not contain disclosed medium- and high-risk vulnerabilities.

NOTE: The vulnerability risk level refers to the national network security vulnerability classification and grading guidelines (such as GB/T 30279 and other standards) and other relevant national regulations.

5.6 Product upgrade

Specialized cybersecurity products should have the following functions:

a) Provide the function of upgrading product components, including but not limited to the main program, feature library, and strategy library;

b) Ensure upgrade security. Avoid getting false, fake upgrades and patches.

5.7 User information security

Specialized cybersecurity products should have the following functions:

a) Only collect user information necessary to implement product functions;

b) Provide relevant authorization functions when processing personal information. Personal information can be processed only after obtaining authorization;

NOTE 1: Personal information processing includes the collection, storage, use, processing, transmission, provision, disclosure, deletion, etc. of personal information. Authorization functions include but are not limited to authorization consent before collection of personal information, authorization withdrawal of personal information collection, etc.

c) Provide security functions unrelated to personal information without obtaining or revoking authorization to collect personal information;

d) Ensure the confidentiality and integrity of personal information during the process involving the transmission and storage of personal information;

e) When it comes to the storage of personal information, provide processing functions for personal information that has exceeded the retention period.

NOTE 2: The processing method of personal information that has exceeded the retention period should be consistent with the processing method authorized by the user, such as deletion or anonymization.

b) Develop design documents for the security functions of specialized cybersecurity products and their own security functions. The description in this document is consistent with the safety function and its own security function;

c) Determine unique version numbers for specialized cybersecurity products. Determine unique identifiers for configuration items. Establish and maintain a list of configuration items;

NOTE 2: Configuration items include but are not limited to source code, tools, documents, components, configuration information, etc.

d) Do not install malicious programs, hidden interfaces or unspecified function modules in the product. Inform users of all functional modules, interfaces, etc. through user agreements, product manuals, etc.;

e) Conduct security testing of specialized cybersecurity products.

NOTE 3: Security testing includes but is not limited to vulnerability scanning, virus scanning, code auditing, penetration testing and security function verification, etc.

6.3 Production and delivery

Specialized cybersecurity products provider should meet the following security requirements:

a) Establish and implement standardized product integrity testing processes. Take measures to prevent risks such as tampering and counterfeiting of homemade or purchased components;

b) Establish control procedures for internal and external delivery. Ensure that specialized cybersecurity products are not destroyed or tampered with during delivery;

c) Clearly indicate to users all functional modules, external interfaces and private protocols included in the product. Inform users of all accounts and default passwords that are provisioned in the product.

6.4 Operation and maintenance service guarantee

Specialized cybersecurity products provider should meet the following security assurance requirements:

a) Provide continuous safety maintenance for products within the period stipulated by laws and regulations or agreed with users, and will not unilaterally interrupt or terminate safety maintenance;

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------