GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

CCS L 80

GB 40050-2021

Critical network devices security common requirements

网络关键设备安全通用要求

Issued on: February 20, 2021 **Implemented on: August 01, 2021**

Issued by: State Administration for Market Regulation;
Standardization Administration of PRC.

Table of Contents

Critical network devices security common requirements

1 Scope

This document specifies the general security function requirements and security assurance requirements for critical network device.

This document applies to critical network device; provides a basis for network operators to purchase critical network device; is also suitable for guiding the research and development, testing, and service of critical network device.

2 Normative references

The provisions in following documents become the provisions of this Standard through reference in this Standard. For the dated references, the subsequent amendments (excluding corrections) or revisions do not apply to this Standard; however, parties who reach an agreement based on this Standard are encouraged to study if the latest versions of these documents are applicable. For undated references, the latest edition of the referenced document applies.

GB/T 25069 Information security technology - Glossary

3 Terms and definitions

The terms and definitions as defined in GB/T 25069, as well as the following terms and definitions, apply to this document.

3.1

Component

A module or component, that is composed of several parts, which are assembled together AND can realize a specific function.

3.2

Malicious program

A program, which is specifically designed to attack the system, damage or destroy the confidentiality, integrity, or availability of the system.

5 Security function requirements

5.1 Device identification security

The identification of critical network device shall meet the following security requirements.

a) The whole hardware and main components shall have unique identification.

Note 1: Common main components of routers and switches: main control board, business board, switching network board, fan module, power supply, storage system software board, hard disk or flash memory card, etc. Common main components of servers: central processing unit, hard disk, memory, fan module, power supply, etc.

Note 2: Common unique identification methods: serial number, etc.

b) Different versions of pre-installed software, patch packages/upgrade packages shall be uniquely identified.

Note 3: Common unique identification method of version: version number, etc.

5.2 Redundancy, backup recovery and anomaly detection

The redundancy, backup recovery and anomaly detection functions of critical network device shall meet the following security requirements.

a) The whole device shall support the main-standby switching function. OR the key components shall support the redundancy function; provide the automatic switching function. When the device or the key components are abnormal, switch to the redundant device or redundant components, to reduce the security risk.

Note: Common key components of routers and switches, that support redundant functions: main control board, switching network board, power supply module, fan module, etc. Common key components of servers, that support redundant functions: hard disks, power modules, fan modules, etc.

b) It shall support the backup and recovery function of pre-installed software and configuration files. When using the recovery function, it shall support the integrity check of pre-installed software and configuration files.

c) It shall support abnormal state detection; generate relevant error message.

5.5 User identification and authentication

The user identification and authentication functions of critical network device shall meet the following security requirements.

a) The user shall be identified and authenticated. The identification shall be unique.

Note 1: Common methods of identity authentication: passwords, shared keys, digital certificates or biometrics, etc.

b) When using the password authentication method, it shall support the mandatory modification of the default password OR the setting of the password, when the device is managed for the first time. OR it shall support the random initial password; support the setting of the password life cycle; support the password complexity check function. When the user inputs password, there shall be no echo password, in plaintext.

c) Support password complexity checking function. Password complexity checking includes at least one of password length checking, password character type checking, password and account independence checking.

Note 2: Different types of critical network device have different password complexity requirements and implementation methods. Examples of common password length requirements: the password length is not less than 8 digits; examples of common password character types: it contains at least two types of numbers, lowercase letters, uppercase letters, punctuation marks, special symbols; examples of common password requirements that are irrelevant to the account: The password does not include account numbers, etc.

d) It shall support the activation of security policies or have security functions, to prevent user authentication information guessing attacks.

Note 3: Common security policies or security functions to prevent user authentication information guessing attacks include enabling password complexity checking by default, limiting the number of consecutive illegal login attempts, or supporting limiting the number of management access connections, two-factor authentication (such as password + certificate, password + biometric authentication, etc.). When authentication fails, the device provides undifferentiated feedback, to avoid prompting specific information such as "user name error" and "password error".

e) It shall support the activation of security policies OR have security functions, to prevent the user's session from being idle for too long, after login.

that affect the security of device operation.

Note 1: Common key user operations include adding/deleting accounts, modifying authentication information, modifying key configuration, file uploading/downloading, user logging in/logging out, modifying user permissions, restarting/closing the device, downloading programming logic, modifying operating parameters, etc.

b) It shall provide the local storage function of log information, support the log information output.

c) The log audit function shall record the necessary log elements AND provide sufficient information for review and analysis.

Note 2: Common log elements include the date and time, subject, type, result, source IP address, etc. of the event.

d) It shall have the security function to protect the log in the local storage and output process; prevent the log content from being viewed, output or deleted, without authorization.

Note 3: Common log protection security functions include user authorization access control and so on.

e) It shall provide the function of dealing with the exhaustion of local log storage space.

Note 4: The common processing functions, when the local log storage space is exhausted, include alarming when the remaining storage space is below the threshold, cyclic coverage, etc.

f) It shall not record the sensitive data, in plaintext or weakly encrypted manner, in the log.

Note 5: Common weak encryption methods include message digest algorithm (MD5), Base64, etc.

5.8 Communication security

The critical network device shall meet the following communication security requirements.

a) It shall support the establishment of a secure communication channel/path with the management system (management user), to ensure the confidentiality and integrity of communication data.

b) It shall meet the robustness requirements of the communication protocol,

a) It shall identify the security risks during device design and development; formulate the security strategies.

Note: Common security risks in device design and development include security risks in the development environment, security risks introduced by third-party components, security risks caused by developers.

b) It shall establish the device security design and development operating procedures, to ensure that the security strategy is implemented in the entire process of design and development.

c) It shall establish a configuration management program and a list of corresponding configuration items. The configuration management system shall be able to track content changes; authorize and control the changes.

d) Measures shall be taken to prevent devices from being implanted with malicious programs.

e) Measures shall be taken to prevent the device from being set up with hidden interfaces or functional modules.

f) Measures shall be taken to prevent security risks, that may be introduced by third-party key components, firmware or software.

g) The security test of the device shall be carried out, by means of vulnerability scanning, virus scanning, code audit, robustness test, penetration test, security function verification.

h) It shall remedy OR provide remedial measures, for the discovered security flaws, vulnerabilities and other security issues.

6.2 Production and delivery

Providers of critical network device shall meet the following requirements, in the production and delivery of critical network device.

a) It shall identify the security risks, during device production and delivery; formulate security strategies.

Note 1: Common security risks in production and delivery include risks, such as tampering and forgery of self-made or purchased components, security risks in the production environment, security risks in device implantation, security risks in device vulnerabilities, logistics and transportation risks, etc.

b) It shall establish and implement a standardized device production process;

alternative plans; notify the user in time according to relevant requirements AND report to the relevant competent authority.

d) When performing remote maintenance on the device, it shall clearly state the maintenance content, risks and countermeasures; keep an unchangeable remote maintenance log record. The record content shall at least include maintenance time, maintenance content, maintenance personnel, remote maintenance methods and tools.

Note 1: Common remote maintenance includes operations such as remote upgrade of device, configuration modification, data reading, remote diagnosis.

e) When performing remote maintenance on device, it shall obtain the user authorization; support the users to suspend remote maintenance. It shall keep the authorization records.

Note 2: Common ways to obtain user authorization include authentication information authorization, written authorization, etc.

f) Users shall be provided with methods, to verify the integrity and source authenticity of the patch/upgrade package.

g) Users shall be provided with methods, for irreversible destruction of key components or data in discarded (or decommissioned) device.

h) Users shall be provided with precautions for data leakage and other security risk control, before the recycling or reuse of discarded (or decommissioned) device.

i) For device or parts that are re-sold or provided after maintenance, the user data in the device or parts shall be irreversibly destroyed.

j) The device shall be provided with continuous security maintenance, within the agreed time limit; the security maintenance shall not be unilaterally interrupted or terminated, due to business changes, property rights changes and other reasons.

k) The user shall be informed of the end time of the device life cycle.

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

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