ICS 33.040.01
CCS C71

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

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 1, 2021**

Issued by: State Administration for Market Regulation;
Standardization Administration of China

Table of Contents

Foreword

This document was drafted in accordance with GB/T 1.1-2020 "Directives for standardization - Part

1.Rules for the structure and drafting of standardizing documents". Please note that some of the contents of this document may involve patents. The issuing agency of this document is not responsible for identifying these patents. This document was proposed by AND shall be under the jurisdiction of the Ministry of Industry and Information Technology of the People's Republic of China. Critical network devices security common requirements

1 Scope

GB 40050-2021 is the Chinese national standard on critical network devices security

common requirements, in the field of telecommunications and audio-video engineering. It carries no /T suffix, which in the Chinese system means compliance is mandatory: a product or a practice within its scope has to meet it to be lawfully made, sold or carried out in China. It was issued on 20 February 2021 by the State Administration for Market Regulation; Standardization Administration of China, and has been in force since 1 August 2021. Classification: ICS 33.040.01, CCS C71. This page is published from the official record of the standard held by the Chinese standards administration: the identification, the dates, the classification and the issuing body are taken from there. The clause text, the tables and the numeric limits are in the document itself, which is delivered complete in English translation.

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.

Note. Common malicious programs include viruses, worms, Trojan horses, spyware, etc.

3.3 Vulnerability Weaknesses in assets or controls, that may be exploited.

3.4 Sensitive data The data which, once leaked, illegally provided or misused, may endanger network security.

3.5 Robustness The extent to which the functions of critical network device or components

can maintain correct operation, under invalid data input OR high-intensity input environment.

3.6 Private protocol Dedicated, non-universal protocol.

4 Abbreviations

The following abbreviations apply to this document. HTTP. Hypertext Transfer Protocol IP. Internet Protocol MAC. Media Access Control SNMP. Simple Network Management Protocol SSH. Secure Shell TCP. Transmission Control Protocol UDP. User Datagram Protocol

5 Security function requirements

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

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.

5.3 Prevention of vulnerabilities and malicious programs The critical network device shall meet the following requirements for preventing vulnerabilities and malicious programs.

5.4 Security of startup and update of pre-installed software The pre-installed software startup and update functions of critical network device shall meet the following security requirements.

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

5.6 Access control security The access control function of critical network device shall meet the following security requirements.

5.7 Log audit security The log audit function of critical network device shall meet the following security requirements.

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

5.9 Data security Critical network device shall meet the following data security requirements.

5.10 Password requirements The relevant content of this document, which involves cryptographic algorithms, shall be implemented in accordance with relevant national provisions.

6 Security guarantee requirements

6.1 Design and development Providers of critical network device shall meet the following requirements in the design and development of critical network device.

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

6.3 Operation and maintenance Providers of critical network device shall meet the following requirements, in the operation and maintenance of critical network device.

a) It shall identify the device's own security risks (not including the network environment security risks) existing in the operation link, as well as the security risks introduced when the device is maintained; formulate a security strategy.

b) It shall establish and implement the emergency response mechanisms and procedures for device security incidents; allocate corresponding resources for emergency response.

c) When the device is found to have security risks such as security defects, loopholes, etc., it shall take remedial measures such as repair or 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.