ICS 35.030
CCS L80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 43698-2024

Cybersecurity technology - Security requirements for software supply chain

网络安全技术 软件供应链安全要求

Issued on: April 25, 2024 **Implemented on: November 1, 2024**

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

Table of Contents

Foreword

This document is in accordance with the provisions of GB/T 1:1-2020 "Guidelines for standardization work Part 1: Structure and drafting rules for standardization documents" Drafting: Please note that some of the contents of this document may involve patents: The issuing organization of this document does not assume the responsibility for identifying patents: This document was proposed and coordinated by the National Cybersecurity Standardization Technical Committee (SAC/TC260): This document was drafted by: China Information Security Evaluation Center, China Electronics Technology Standardization Institute, Huawei Technologies Co:, Ltd:, National Planning Commission Computer Network Emergency Technical Processing Coordination Center, China Software Evaluation Center (Software and Integrated Circuit Promotion Center of the Ministry of Industry and Information Technology), Nokia Asia Communication System Technology (Beijing) Co:, Ltd:, Qi'anxin Wangshen Information Technology (Beijing) Co:, Ltd:, Sangfor Technologies Co:, Ltd:, Ning Ge, Zhang Tao, Yuan Mingkun, Yang Tingfeng, Wang Qi, Wang Weiqi, Yang Mutian, Li Yue, Li Teng, Wan Juan, Wu Jingzheng, Wang Zhenyuan, Liu Jingqiang, Xiao Yang, Liang Dagong, Wan Xiaolan, Cai Yibing, Liang Lulu, Zhao Xiaohui, Peng Chen, Yang Yi, Zhang Yong, Feng Quanbao, Cheng Yan, Nie Wanquan, Fu Yanyan, Huo Shanshan, Liu Yang, Wong Jing, Quan Xiaowen, Zhou Haowei: Cybersecurity Technology Software Supply Chain Security Requirements

1 Scope

GB/T 43698-2024 sets the Chinese security requirements for the software supply chain. It arrives after a decade in which the most consequential compromises came not through a target's own code but through its suppliers, its build system or an open source dependency, and it treats the supply chain as the object to be secured rather than the product. The

standard sets the security objectives and then a protection framework covering the whole chain, and within it the requirements: on the supplier and the acquisition process, including the evaluation of suppliers and the terms that must be imposed on them; on the development, covering the source, the third-party and open source components and their inventory, the build environment and the integrity of the artefacts it produces; on the delivery, its signing, verification and channel; on the operation and maintenance, the vulnerability monitoring, the patching and the response when a component is found to be compromised; and on the disposal. For any organisation supplying software into China, or buying it there, this is the framework the assessment will follow. It takes effect on 1 November 2024.

This document establishes software supply chain security goals, specifies software supply chain security risk management requirements and organizational management of both supply and demand sides: and supply activities management security requirements: This document is applicable to guiding both the supply and demand sides in the software supply chain to carry out risk management, organizational management and supply activity management: It provides a basis for institutions to conduct software supply chain security testing and assessment, and is used as a reference for competent regulatory authorities:

2 Normative references

The contents of the following documents constitute the essential clauses of this document through normative references in this document: For referenced documents without a date, only the version corresponding to that date applies to this document; for referenced documents without a date, the latest version (including all amendments) applies to This document:

GB/T 25069-2022 Information Security Technical Terminology

GB/T 36637-2018 Information Security Technology ICT Supply Chain Security Risk Management Guide

3 Terms and definitions

The terms and definitions defined in GB/T 25069-2022 and GB/T 36637-2018 and the following apply to this document: 3:

1 Software Productsoftwareproduct Software embedded in computer software, information systems or equipment, or when providing technical services such as computer information system integration and application services Provided computer software:

Note 1: A software product consists of computer program code, procedures, associated data, documentation and related services:

Note 2: In this document, software products are referred to as software: [Source: GB/T

36475-2018, 3:1:1, modified] 3:2 A general term for information such as software product version, logo, source, authorization, and associated software: 3:3 acquirer An organization that acquires software products from other organizations:

Note: In this document, the purchaser refers to the purchaser and user of the software product: [Source: GB/T 36637-2018, 3:1, modified] 3:

4 Supplier An organization that carries out life cycle activities such as software product development, delivery, operation and maintenance, and retirement:

Note 1: In this document, suppliers refer to the first-tier (direct) suppliers of the purchaser; in addition, they also include software product developers, sales and agents at all levels, system integrators, It also includes software or application stores, code hosting platforms, third-party download sites, and organizations that provide software products based on open source code:

Note 2: The open source community itself is not a supplier: