

ICS 35.030
CCS L80



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

GB/T 43848-2024

**Cybersecurity technology - Evaluation method for open source
code security of software products**

网络安全技术 软件产品开源代码安全评价方法

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

1 Scope	1
2 Normative references	1
3 Terms and Definitions	1
4 Overview	1
5 Open Source Code Generation	5
10 Reference	11

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 Academy of Information and Communications Technology, Ant Group Co., Ltd., Huawei Technologies Co., Ltd., ZTE Corporation Co., Ltd., Shandong Inspur Science Research Institute Co., Ltd., Alibaba Cloud Computing Co., Ltd., Sangfor Technologies Co., Ltd., Tencent Cloud Computing (Beijing) Co., Ltd., Hangzhou Moan Technology Co., Ltd., Shenzhen Open Source Internet Security Technology Co., Ltd., Beijing Baidu Netcom Technology Co., Ltd., Shenzhen Tencent Computer Systems Co., Ltd., Beijing Topsec Network Security Technology Co., Ltd., Qi'anxin Wangshen Information Technology (Beijing) Co., Ltd., Inspur Electronic Information Industry Co., Ltd., Beijing Xiaomi Mobile Software Co., Ltd., Beijing Jingdong Shang Information Technology Co., Ltd., Beijing Kingsoft Cloud Network Technology Co., Ltd., Beijing Volcano Engine Technology Co., Ltd., Hengan Jiaxin (Beijing) Technology Technology Co., Ltd., Venusstar Information Technology Group Co., Ltd., UFIDA Network Technology Co., Ltd., Hangzhou Anheng Information Technology Co., Ltd. Co., Ltd., Beijing Knowsec Information Technology Co., Ltd., Changyang Technology (Beijing) Co., Ltd., Transwarp Information Technology (Shanghai) Co., Ltd., Zhejiang Dahua Technology Co., Ltd., Super Fusion Digital Technology Co., Ltd., Midea Group Co., Ltd., Mashang Consumer Finance Co., Ltd., Taikang Insurance Group Co., Ltd., Dopu Information Technology Co., Ltd., China Electronics Technology Group Corporation Network Security Science and Technology Co., Ltd. Technology Co., Ltd., State Grid Blockchain Technology (Beijing) Co., Ltd., Beijing Ampno Information Technology Co., Ltd., China Information Security Evaluation Center, China Software Testing Center, China Electronics Technology Group Corporation Mimic Security Technology Co., Ltd., Hangzhou

Xiaodao Technology Co., Ltd., Beijing Luoan Technology Co., Ltd: Shenzhen Huada Life Sciences Institute, Xingtang Communication Technology Co., Ltd., Murphy Future Technology (Beijing) Co., Ltd., Beijing Kudezhu Mu Niao Information Technology Co., Ltd., Institute of Software, Chinese Academy of Sciences, China Cyberspace Research Institute, National Computer Network Emergency Response Technology Processing Co., Ltd: Coordination Center, National Information Technology Security Research Center, Institute of Information Engineering, Chinese Academy of Sciences, Zhejiang Electronic Information Product Inspection Institute, The Sixth Research Institute of China Electronics Information Industry Group Co., Ltd., Boding Shihua (Beijing) Technology Co., Ltd., ABB (China) Co., Ltd., Six Zero Technology Group Co., Ltd., Beijing Shenzhou Green Alliance Technology Co., Ltd., Xi'an Jiaotong University Jabil Network Technology Co., Ltd., Shenzhen Nengxinan Technology Co., Ltd., Lenovo (Beijing) Co., Ltd., Beijing Changting Future Technology Co., Ltd., Beijing Hillstone Network Technology Co., Ltd: Guangdong Yunbai Technology Co., Ltd., Wuhan Antiy Information Technology Co., Ltd., Beijing Zhiyou Network Security Technology Co., Ltd., Beijing Jiuzhang Cloud Ji Technology Co., Ltd., Kylin Software Co., Ltd., H3C Technologies Co., Ltd., Tianyi Cloud Technology Co., Ltd., OPPO Guangdong Mobile LICENSING LIMITED: The main drafters of this document are: Li Wei, Guo Xue, Li Xiaoming, Wu Jiangwei, Cheng Yan, Bai Xiaoyuan, Cui Jinguo, Gao Kun, Zhang Ruigang, Xiang Shuming, Li Xiang, Wei Zizhong, Fang Qiang, Zeng Linqing, Zhao Zhenyang, Ye Runguo, Zheng Jianfeng, Shen Xiyong, Meng Jin, Nie Wanquan, Wang Jie, Guo Jianling, Dai Wei, Yang Jian, Dong Guowei, Cao Zhu, Qian Jiayu, Li Xinbo, Li Xiaochuan, Zhang Zhiwen, Li Pengchao, Zhao Junkai, Ji Shengyu, Yuan Mingkun, Zhou Jingping, Fan Lei, Liu Wanggen, Zhang Jianqing, Hui Jing, Zhang Liangliang, Liu Zhiqiang, An Bingchun, Han Mingjun, Wang Huibo, Yang Ke, Zhang Tao, Wang Xiaomeng, Yuan Wei, Hou Dapeng, Xie Guomiao, Yan Peng, Cai Guoyu, Hao Gaojian, Ouyang Qiangbin, Shi Mingchao, Yan Min, Jiang Wei, Wu Wei, Wu Qian, Liu Nan, Xu Lili, Yin Xiaodong, Wang Shaojie, Dong Ji, Wang Zhui, Zhang Jie, Zhang Fan, He Jianfeng, Li Deqing, Liu Jun, Zhai Yujia, Rong Yu, Liu Chao, Yu Lina, Han Yun, Fang Lei, Liu Min, Wan Xiaolan, Hong Junhuang, and Julia: Network security technology software products open source code security Evaluation Method

1 Scope

GB/T 43848-2024 gives the method for evaluating the security of the open source code in a software product. Most of a modern product is code the vendor did not write, pulled transitively from repositories nobody audits, and the risk is not only the known vulnerability in a component but the health of what stands behind it: who owns the copyright, who is still committing, which platform hosts it, and whether a single unpaid maintainer is the whole supply chain. The standard sets the evaluation factors: the evaluation parameters, and then the open source code sources, covering the scale and proportion of open source in the product, the languages, the copyright holders, the pattern of contributions, the richness of

the code, the security management of the community, and the hosting and download platforms, together with the code's own security properties and licence compliance, and then the evaluation process, scoring and conclusions. It took effect on 1 November 2024.

This document specifies the security evaluation elements and evaluation process for open source code components in software products: This document is applicable to the static security evaluation of the open source code components contained in software products, and provides a reference for each unit to evaluate the open source code components in software products: It provides a basis for self-assessment of the security of source code components and a reference for third-party organizations to carry out such work:

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

3 Terms and definitions

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

1 Software Productsoftwareproduct Computer software, software embedded in information systems or equipment, or provided when providing technical services such as computer information system integration and application Computer software provided by the Company is in the form of a set of computer codes, procedures and possibly related documentation and data: [Source: GB/T 36475-2018, 3:1, modified] 3:

2 Open source codeopensourcecode Source code is available to the public:

Note: The copyright owner has made the rights to copy, modify and redistribute the code available to the public through an open source license: 3:

3 Open source licenseopensourcelicense An authorization agreement that allows public users to use, modify, copy and distribute open source code according to the content of the agreement: 3:4 open source community The open source code contributors are the main body, and the specific culture, organizational structure, and operating mechanism are formed in the process of open source code contribution: community:

4 Overview

Currently, when open source code is widely used in software products, there are open

source code network security risks, intellectual property risks and sustainability risks: (See Appendix A):

chinastandards.org - PREVIEW