ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 43848—2024

网络安全技术　软件产品开源代码安全评价方法

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

2024-04-25 发布　　2024-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国信息通信研究院、蚂蚁科技集团股份有限公司、华为技术有限公司、中兴通讯股份有限公司、山东浪潮科学研究院有限公司、阿里云计算有限公司、深信服科技股份有限公司、腾讯云计算(北京)有限责任公司、杭州默安科技有限公司、深圳开源互联网安全技术有限公司、北京百度网讯科技有限公司、深圳市腾讯计算机系统有限公司、北京天融信网络安全技术有限公司、奇安信网神信息技术(北京)股份有限公司、浪潮电子信息产业股份有限公司、北京小米移动软件有限公司、北京京东尚科信息技术有限公司、北京金山云网络技术有限公司、北京火山引擎科技有限公司、恒安嘉新(北京)科技股份公司、启明星辰信息技术集团股份有限公司、用友网络科技股份有限公司、杭州安恒信息技术股份有限公司、北京知道创宇信息技术股份有限公司、长扬科技(北京)股份有限公司、星环信息科技(上海)股份有限公司、浙江大华技术股份有限公司、超聚变数字技术有限公司、美的集团股份有限公司、马上消费金融股份有限公司、泰康保险集团股份有限公司、道普信息技术有限公司、中电科网络安全科技股份有限公司、国网区块链科技(北京)有限公司、北京安普诺信息技术有限公司、中国信息安全测评中心、中国软件评测中心、中电科拟态安全技术有限公司、杭州孝道科技有限公司、北京珞安科技有限责任公司、深圳华大生命科学研究院、兴唐通信科技有限公司、墨菲未来科技(北京)有限公司、北京酷德啄木鸟信息技术有限公司、中国科学院软件研究所、中国网络空间研究院、国家计算机网络应急技术处理协调中心、国家信息技术安全研究中心、中国科学院信息工程研究所、浙江省电子信息产品检验研究院、中国电子信息产业集团有限公司第六研究所、博鼎实华(北京)技术有限公司、ABB(中国)有限公司、三六零科技集团有限公司、北京神州绿盟科技有限公司、西安交大捷普网络科技有限公司、深圳市能信安科技股份有限公司、联想(北京)有限公司、北京长亭未来科技有限公司、北京山石网科信息技术有限公司、广东云百科技有限公司、武汉安天信息技术有限责任公司、北京智游网安科技有限公司、北京九章云极科技有限公司、麒麟软件有限公司、新华三技术有限公司、天翼云科技有限公司、OPPO广东移动通信有限公司。

本文件主要起草人：栗蔚、郭雪、李晓明、吴江伟、程岩、白晓媛、崔锦国、高琨、张锐刚、项曙明、李响、魏子重、方强、曾林青、赵振阳、叶润国、郑剑锋、沈锡镛、孟瑾、聂万泉、王颉、郭建领、代威、杨剑、董国伟、曹柱、钱佳煜、李欣博、李晓川、张志文、李鹏超、赵军凯、季晟宇、袁明坤、周景平、范雷、刘汪根、张剑青、惠静、张亮亮、刘志强、安丙春、韩明军、王会波、杨珂、张涛、王晓萌、袁薇、侯大鹏、谢国苗、延鹏、蔡国瑜、郝高健、欧阳强斌、史明超、晏敏、姜伟、吴巍、吴倩、刘楠、许丽丽、尹肖栋、王绍杰、董霁、王缀、张杰、张帆、何建锋、李德庆、刘俊、翟羽佳、荣钰、刘超、余丽娜、韩云、方磊、刘敏、万晓兰、洪钧煌、朱丽亚。

网络安全技术　软件产品开源代码安全评价方法

1　范围

本文件规定了软件产品中的开源代码成分安全评价要素和评价流程。

本文件适用于对软件产品包含的开源代码成分进行静态安全评价，为各单位对于软件产品中的开源代码成分进行安全性自评价提供依据，为第三方机构开展此类工作提供参考。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2022　信息安全技术　术语

3　术语和定义

GB/T 25069—2022 界定的以及下列术语和定义适用于本文件。

3.1

软件产品　software product

计算机软件、信息系统或设备中嵌入的软件，或在提供计算机信息系统集成、应用等技术服务时提供的计算机软件，表现形式为一组计算机代码、规程以及可能的相关文档和数据。

[来源：GB/T 36475—2018，3.1，有修改]

3.2

开源代码　open source code

公众可以获取源代码的计算机代码。

注：其著作权人通过开源许可证将代码的复制、修改、再发布的权利向公众开放。

3.3

开源许可证　open source license

允许公众用户根据协议内容使用、修改、复制和分发开源代码的授权协议。

3.4

开源社区　open source community

以开源代码的贡献者为主体，在开源代码贡献过程中形成的具有特定文化、组织结构、运行机制的共同体。

4　概述

当前开源代码被广泛应用在软件产品时，存在开源代码网络安全风险、知识产权风险和持续性风险（见附录 A）。