ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 43698—2024

网络安全技术　软件供应链安全要求

Cybersecurity technology—Security requirements for software supply chain

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：中国信息安全测评中心、中国电子技术标准化研究院、华为技术有限公司、国家计算机网络应急技术处理协调中心、中国软件评测中心(工业和信息化部软件与集成电路促进中心)、诺基亚通信系统技术(北京)公司、奇安信网神信息技术(北京)股份有限公司、深信服科技股份有限公司、国网新疆电力有限公司电力科学研究院、麒麟软件有限公司、国家信息技术安全研究中心、国家计算机网络应急技术处理协调中心黑龙江分中心、深圳开源互联网安全技术有限公司、昆仑数智科技有限责任公司、联想(北京)有限公司、浪潮电子信息产业股份有限公司、中国网络安全审查技术与认证中心、杭州默安科技有限公司、北京天融信网络安全技术有限公司、三六零数字安全科技集团有限公司、长扬科技(北京)有限公司、上海观安信息技术股份有限公司、北京奇虎科技有限公司、北京快手科技有限公司、云从科技集团股份有限公司、国网区块链科技(北京)有限公司、国家计算机网络应急技术处理协调中心北京分中心、上海三零卫士信息安全有限公司、北京大学、启明星辰信息技术集团股份有限公司、瀚高基础软件股份有限公司、北京威努特技术有限公司、蚂蚁科技集团股份有限公司、中国信息通信研究院、中电长城网际安全技术研究院(北京)有限公司、北京安普诺信息技术有限公司、杭州安恒信息技术股份有限公司、北京神州绿盟科技有限公司、北京中科微澜科技有限公司、OPPO广东移动通信有限公司、公安部第一研究所、中国科学院软件研究所、阿里云计算有限公司、湖南泛联新安信息科技有限公司、北京中测安华科技有限公司、中国科学院信息工程研究所、苏州棱镜七彩信息科技有限公司、新华三技术有限公司、工业和信息化部电子第五研究所、北京源堡科技有限公司、北京人大金仓信息技术股份有限公司、上海大学、西安邮电大学、沈阳东软系统集成工程有限公司、中国电子科技集团公司第十五研究所、远江盛邦(北京)网络安全科技股份有限公司、上海文鳐信息科技有限公司。

本文件主要起草人：李守鹏、王欣、王晓萌、王惠莅、薛勇波、吴润浦、林星辰、曾晋、上官晓丽、王嘉捷、万振华、陈冬青、沈蕾、辛伟、唐福宇、董国伟、常远、崔静、叶润国、高金萍、杨慧婷、吴倩、翟艳芬、董军平、王颉、张屹、滕征岑、邱林海、邓辉、郑明、李汝鑫、谢江、张大江、刘磊、梁利、陈靓、廖毅、柴思跃、宋桂香、申永波、孟瑾、白晓媛、孔耀晖、沈锡镛、杨剑、孙世国、李娜、王聪、赵华、韩煜、落红卫、武延军、张亚京、李军、张立、王栋、温婷婷、陈亮、查海平、高庆、姚叶鹏、赵军凯、冯明冉、王春霞、刘健、李汪蔚、林飞、宁戈、张涛、袁明坤、杨廷锋、王琦、王玮琪、杨牧天、李跃、李腾、万娟、吴敬征、王振远、刘井强、肖扬、梁大功、万晓兰、蔡一兵、梁露露、赵晓晖、彭晨、杨毅、张勇、冯全宝、程岩、聂万泉、付艳艳、霍珊珊、刘洋、王晶、权晓文、周浩威。

网络安全技术　软件供应链安全要求

1　范围

本文件确立了软件供应链安全目标，规定了软件供应链安全风险管理要求和供需双方的组织管理和供应活动管理安全要求。

本文件适用于指导软件供应链中的供需双方开展风险管理、组织管理和供应活动管理，为第三方机构开展软件供应链安全检测和评估提供依据，供主管监管部门参考使用。

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

GB/T 36637—2018　信息安全技术　ICT 供应链安全风险管理指南

3　术语和定义

GB/T 25069—2022 和 GB/T 36637—2018 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、应用服务等技术服务时提供的计算机软件。

注 1：软件产品包含计算机程序代码、规程、相关数据、文档和相关服务。

注 2：本文件中软件产品简称为软件。

[来源：GB/T 36475—2018，3.1.1，有修改]

3.2

软件产品信息　software product information

软件产品版本、标识、来源、授权以及关联软件等信息的总称。

3.3

需方　acquirer

从其他组织获取软件产品的组织。

注：本文件中需方指软件产品的购买者和使用者。

[来源：GB/T 36637—2018，3.1，有修改]

3.4

供方　supplier

开展软件产品开发、交付、运维、废止等生命周期活动的组织。

注 1：本文件中供方指需方的第一级（直接）供应商；此外，还包括软件产品的开发商、各级销售和代理商、系统集成商，也包括软件或应用商店、代码托管平台、第三方下载站点以及基于开源代码提供软件产品的组织等。

注 2：开放源代码社区本身不是供方。