《软件供应链安全能力评估规范》
标准编制说明

软件开发标准起草组

2023 年 7 月 10 日

1、 标准范围。

本文件规定了的软件供应链安全能力评估要求。适用于组织机构对软件供应链安全的评估和改进，适用于第三方开展软件供应链安全检测评估认证。

2、 工作简况。

软件供应链是一个全球分布的、具有供应商多样性、产品服务复杂性、全流程覆盖等诸多特点的复杂系统，在软件供应链各个供应活动中均可能引入安全隐患，导致软件漏洞、软件后门、恶意篡改、假冒伪劣、知识产权风险、供应中断、信息泄露等安全风险，本规范给出了软件供应链安全保护目标，规定了软件供应链组织管理和供应活动管理的安全要求。

3、标准编制原则和确定标准主要内容的依据：

原则：软件供应链是一个全球分布的、具有供应商多样性、产品服务复杂性、全流程覆盖等诸多特点的复杂系统，在软件供应链各个供应活动中均可能引入安全隐患，导致软件漏洞、软件后门、恶意篡改、假冒伪劣、知识产权风险、供应中断、信息泄露等安全风险，本规范给出了软件供应链安全保护目标，规定了软件供应链组织管理和供应活动管理的安全要求。

内容依据：软件供应链安全已成为信息安全领域关注重点。以下是国内外软件供应链安全情况的简要介绍。美国国家安全局发布过《安全技术指导：安全增强供应链风险管理》和《要求和考虑因素为了保证代码可信可审查》，致力于提升软件供应链安全。欧洲委员会提出了一项软件供应链安全倡议，鼓励欧盟内各企业采取主动措

施，提高其与供应商间合作的安全性。国内 2016 年，国家互联网应急中心发布了《软件供应链安全防范指南》，提出了在软件开发、采购、测试等环节中应注意的安全问题;2018 年，国家信息安全标准化技术委员会在发布《信息技术-安全技术-软件供应链安全管理指南》;2020 年，全国人大常委会通过《网络安全法》，将软件供应链安全纳入到法定要求中。

总的来说，国内外均在不断加强软件供应链安全的工作，并不断制定和完善相关法规、规范和指南，以提升软件安全性和可信度。但同时，也需要各行业和企业加强对软件供应链的管理和风险识别，共同保障信息安全。

4、主要试验（或验证）的分析、综述报告。

无

5、标准在起草过程中遇到的问题及解决办法：重大分歧意见的处理经过和依据：有无重要技术问题需要说明。

无。

6、与国外标准的关系：包括：采用国际标准和国外先进标准的程度，与国外标准主要技术内容的差异（可引用标准前言的内容）：

无

7、修订标准时，说明与标准前一版本的重大技术变化，并列出所涉及的新、旧版本的有关章条（可引用标准前言的内容）：废止/代替现行有关标准的建议：

无

8、说明标准与其他标准或文件的关系（可引用标准前言的内容），特别是与有关的现行法律、法规和强制性国家标准的关系：

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。

9、标准作为强制性标准或推荐性标准的建议：

建议：软件供应链安全风险越来越大，面临的威胁与日俱增：1）国家层面：数字化转型，使国内应用生态规模急速膨胀，形成软件应用大爆发趋势，也极大的刺激了国内IT基础设施的发展，暴露出供应链更多的安全问题。2）技术趋势：随着容器、微服务等新技术的演进，软件行业快速发展。功能快速实现，软件快速交付成为第一优先级，使软件在设计与开发过程产生许多安全漏洞，为软件供应链安全埋下隐患。3）随着开源供应持续加速，开源需求呈爆炸式增长，开源漏洞普遍存在。而代码开源成为当前主流开发模式之一，针对开源的攻击成倍增长，加剧了软件供应链安全风险。综上所述：软件供应链面临的安全风险至关重要，包括：软件代码本身安全、开发环境安全以及开发人员自身安全等等，都是软件供应链安全需要去考虑的问题，结合我国当下的实际情况，希望通过此规范发展软件供应链安全，帮助我国完善网络安全体系。

10、贯彻国家标准的要求和措施建议（包括组织措施、技术措施、过渡办法等内容）：

无

11、标准是否涉及知识产权的情况说明；如标准中含有自主知识产权，说明产品研发程度、产业化基础及进程。

无

12、其他应予说明的事项。