ICS 35.080
CCS L00/09

团 体 标 准

T/ISC 0044—2024

软件供应链安全要求

Requirement for software supply chain security

发布稿

2024 年 1 月 29 日发布 2024 年 2 月 28 日实施

中 国 互 联 网 协 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。

本标准由中国互联网协会归口。

本文件起草单位：中国信息通信研究院、深圳开源互联网安全技术有限公司、扬州数安技术有限公司、北京风行网安科技有限公司、中国石油昆仑数智科技有限责任公司、中国移动通信集团设计院有限公司、中国电力科学研究院有限公司、中国民航信息网络股份有限公司、中国经济信息社、中建数字科技有限公司、OpenSDV汽车软件开源联盟、北京智精灵科技有限公司、四川赛闯检测股份有限公司、成都信息工程大学、网宿科技股份有限公司、仁寿智仁智慧科技有限公司、四川仁恒智合科技有限公司、江苏大道云隐科技有限公司。

本文件主要起草人：蒋阿芳、马英轩、樊可欣、王颉、菅志刚、王晓龙、郭治文、张志强、滕征岑、张嵩、孙忠伟、肖秀琴、易兴辉、刘玲、缪思薇、周亮、左海峰、杨京煜、王宇、翟冬梅、吴新丽、王勇、王一村、段柯欣、贾大伟、滕召智、梁尧、张坤、方建康、周琼、冯丽、袁丽、黄莎琳、吕士表、杨志伟、廖敏飞、党杜均、邓恒、黄圣超。

软件供应链安全要求

1 范围

本文件规定了的软件供应链安全要求。适用于信息技术产品研发的组织机构对自身的软件供应链安全的建设、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 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

GB/T 30279—2020 信息安全技术 网络安全漏洞分类分级指南

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

软件供应链 software supply chain

为满足软件供应关系通过资源和过程将需方、供方相互连接的网链结构，可用于将软件产品和服务提供给需方。

3.2

软件供应链安全 software supply chain security

指软件供应链生命周期中各环节、过程涉及的软件产品和服务安全、供应关系安全、人员安全及软件供应链基础设施安全的总和。

3.3

软件供应链生命周期 software supply chain life cycle

在软件供应链中，从软件的需求分析开始至软件的废止停用或者供需双方终止协议的整个时期，包括开发环节、交付环节和使用环节，划分为协商、生产、交付、获取、使用、运维、废止7个过程。

3.4

开源组件 open source component

开放源代码，遵循开源协议进行共享、开发、使用、编译和发布的软件模块，通常是由源代码程序文件构成。

4 软件供应链安全体系模型

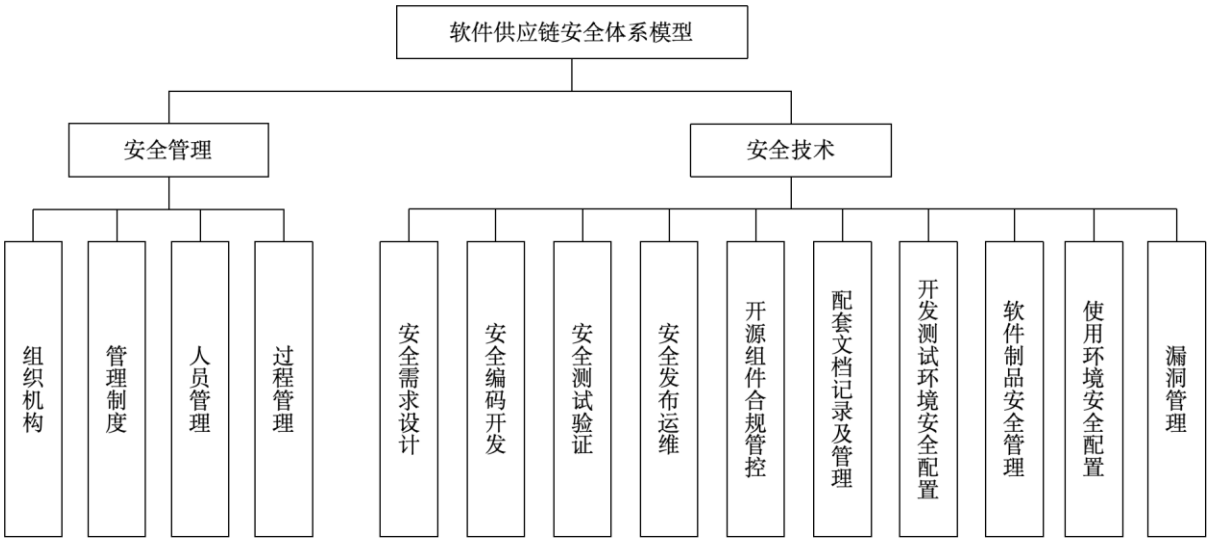

图 1 软件供应链安全体系模型

软件供应链安全体系主要包括安全管理和安全技术两部分。管理包括组织机构、管理制度、人员管理、过程管理四个部分。技术包括安全需求设计、安全编码开发、安全测试验证、安全部署运维、开源组件管控、软件制品安全检查和配套文档记录及管理、开发环境安全配置、使用环境及安全配置、软件资产及知识产权管理、漏洞管理十一个部分。建立完整的软件供应链安全体系应包括以上内容，结合实际情况持续优化。在体系建设、运行、总结、评审等情况下，应逐条对照进行实施，在体系运行范围内贯彻落实。

5 安全管理要求

5.1 组织机构

本项要求包括：

a) 应组建软件供应链安全组织机构，明确及其职责范围，对于重要或核心业务场景，应设立专职部门或岗位开展软件供应链安全管理工作；
b) 应制定年度软件供应链安全保障计划，组织实施和监督，并在年底总结；
c) 应申请保障软件供应链安全所需的资源（如有关资金、场地、人力等），并在预算中予以考虑。

5.2 管理制度

本项要求包括：

a) 应制定软件供应链安全的总体方针和制度，明确本单位软件供应链安全基本要求；
b) 应制定软件供应链安全相关的人员管理制度；
c) 应制定软件资产及知识产权的安全管理制度，包括但不限于软件授权证书、专利、软件著作权、许可协议等内容；
d) 应制定软件安全漏洞管理制度，明确安全漏洞风险的防范、响应和处理要求和流程；
e) 应制定软件全生命周期的过程管理制度。

5.3 人员管理

本项要求包括：

a) 应划分人员的权限级别，采用最小授权机制，并建立操作规范，创建操作日志；
b) 应开展人员岗前的审查，考核人员的软件供应链安全意识和相关能力；

c） 定期（至少每半年一次）开展软件供应链安全和保密培训；
d） 应建立并执行离职离岗人员账号、权限、材料的交接和清理机制和规程。

5.4 过程管理（软件全生命周期）

本项要求包括：
a） 应对软件的需求、设计、开发、测试、部署、维护、废止等各阶段进行安全过程管理；
b） 应建立安全需求流程，在软件开发过程中执行，包括安全需求的创建、确认、变更和评审流程；
c） 应建立安全设计流程，在软件开发过程中执行，在设计阶段开展安全架构设计、威胁建模等工作，形成安全设计文档，并组织评审；
d） 应建立安全开发流程，通过自动化检测工具等方式确保在开发人员执行安全开发流程，并定期进行检查；
e） 应建立安全测试流程，制定测试计划，准备测试环境，明确测试用例，并按计划完成测试工作，发现的安全问题及时记录和报告，在问题修复后进行复测，直到符合安全要求后关闭问题，并在最后进行测试总结；
f） 应建立安全部署流程，在部署阶段实行安全配置原则，要求软件部署人员严格执行安全部署工作流程规范，并逐一记录；
g） 应建立安全维护流程，制定日常安全运维计划和安全应急响应计划，明确维护工作的流程、时间、范围、方式、内容和负责人，在维护阶段对软件的安全性进行实时监测，发现安全漏洞或攻击应及时报告、响应和修复。
h） 应建立安全废止流程，对软件的废止要进行申请和审批，废止时按要求卸载和删除开发环境、测试环境以及运行环境中的软件程序包、配置文件、数据、源代码、组件和相关文档。

6 安全技术要求

6.1 安全需求设计

本项要求包括：
a） 应制定安全需求基线，结合法律法规、标准规范、业务场景等方面识别安全风险；
b） 应开展安全需求分析，提出安全需求，在软件需求规格说明等需求文档中明确记录，或者单独编制软件安全需求文档；
c） 应组织安全需求评审，并持续维护安全需求，在需求变更等情况时重新评审安全需求；
d） 应在设计阶段考虑到安全性，选型和设计符合安全需求的技术架构，形成设计文档并组织评审；
e） 应在设计阶段开展威胁建模，在概要设计文档或者详细设计文档中明确记录有关安全的内容；
f） 应组织安全设计评审，逐一确认软件设计是否符合安全需求；
g） 应持续维护安全设计，在重构、更改业务逻辑等情况时重新开展安全设计威胁建模和评审。

6.2 安全编码开发

本项要求包括：
a） 应建立安全编码规范，针对不同的编程语言，制定相对应的安全编码要求；
b） 安全编码规范应包括面向对象程序安全、并发程序安全、函数调用安全、异常处理安全、指针安全、代码生成安全、内存管理、数据库管理、文件管理、网络传输、安全的编译选项等内容；
c） 安全编码规范应对每个要求给出具体示例和说明；
d） 应在编译最终制品时关闭不必要的选项，例如调试选项。

6.3 安全测试验证

本项要求包括：
a） 应在软件开发阶段和软件开发完成后，开展安全测试验证，安全测试验证应覆盖安全需求；
b） 应针对安全需求编写测试用例并执行安全测试；
c） 应对软件的安全功能进行测试；

d） 应对软件的代码、开源组件、API接口、业务逻辑等进行安全性测试，采用白盒测试、灰盒测试、黑盒测试等方法进行测试；
e） 应开展代码评审、代码检测、代码走查，识别并修复源代码安全漏洞；
f） 应开展开源组件安全合规检查，识别并修复开源组件的安全漏洞和开源许可证冲突问题；
g） 应将发现的安全漏洞收录到内部漏洞库中，并执行后续的漏洞管理机制和流程；
h） 应具备主要安全基线的自动测试能力；
i） 应记录并跟踪软件安全测试出的问题和修复情况。

6.4 安全发布运维

本项要求包括：
a） 应按照最小化原则进行软件的安装部署，只开放软件运行所必须的端口和服务；
b） 应定期检查软件运行环境配置安全，不符合安全要求的配置应及时修改；
c） 应对软件制品进行完整性检查，防止被恶意篡改；
d） 应对重要或核心业务场景的软件实行数字签名；
e） 应通过受控的安全渠道发布软件；
f） 应持续维护软件的补丁更新，及时安装最新的补丁包；
g） 应定期检测软件是否存在安全漏洞等风险，对发现的问题及时响应和修复，并跟踪安全漏洞修复情况；
h） 应对重要或核心业务场景的软件进行安全加固，配置应用安全自我防护技术手段；
i） 应记录并跟踪软件安全测试出的问题和修复情况。

6.5 开源组件合规管控

本项要求包括：
a） 应选用不含安全漏洞（中危以上级别）的开源组件和开源代码；
b） 应选用不存在许可证授权冲突的开源组件和开源代码，避免因此导致的法律风险；
c） 应选用有替代品的开源组件和开源代码，防止停更、断供等风险；
d） 应开展软件成分分析，充分掌握软件中包含的开源组件和开源代码，以及它们之间的依赖关系；
e） 应对所有需要使用的开源组件和开源代码进行安全漏洞检测，然后收录到软件资产库集中管理；
f） 应只从内部软件资产库下载和引用开源组件和开源代码，例如Maven引用来源应配置为本地库；
g） 应检查使用、修改或发布的开源组件，对于缺少开源组件许可证信息或者使用开源许可证不规范的情况及时整改。

6.6 配套文档记录及管理

本项要求包括：
a） 应为关键供应活动编制文档，包括但不限于合同、保密协议、安全过程评审记录、软件验收单、测试报告、变更申请等；
b） 应在文档中记录时间、相关单位及负责人、主要内容，并加盖公章；
c） 应对关键文档进行管理，控制文档的流转、存储、备份和销毁；
d） 应对涉密文档设置权限，未授权人员不应获得、阅读、修改、复制、销毁。

6.7 开发测试环境安全配置

本项要求包括：
a） 应建立独立的开发环境网络和测试环境网络，网络相互隔离并与互联网隔离，并配置入侵防范等措施；
b） 应对开发环境网络和测试环境网络执行权限访问控制，未授权人员不得访问开发环境；
c） 应关闭开发环境和测试环境各软硬件系统中的常见高危端口或服务，并配置数据读写安全模式；

d） 应定期（至少半年一次）对管理开发环境中的软硬件系统、开发测试工具等进行安全检查，存在安全问题的及时响应处置；
e） 应建立软件资产库，软件资产库至少包括源代码库、开源组件库、软件制品库；
f） 应对软件资产库执行安全机制，如具备防止捆绑恶意代码、下载劫持、网络劫持、升级劫持的能力。

6.8 软件制品安全管理

本项要求包括：
a） 应对软件制品进行配置管理；
b） 应对软件制品进行恶意代码、脚本、病毒蠕虫木马等扫描；
c） 应对软件制品进行完整性检查，防止被恶意篡改；
d） 应对部署在重要或核心业务场景的软件实行数字签名；
e） 应对所有软件制品定期进行检查，将检出的漏洞收录至安全漏洞库，并组织进行整改；
f） 应对软件制品中引用的开源许可证进行检查，避免因此导致的法律风险；
j） 应对软件的发布环境进行安全管控和安全加固，防止软件发布环境被攻击而导致发布的软件被篡改或植入病毒。

6.9 使用环境安全配置

本项要求包括：
a） 应定期（至少一个月一次）对使用环境进行安全基线扫描，扫描对象包括但不限于网络设备、网络安全设备、服务器、终端、操作系统、数据库、中间件，并对发现的问题及时进行处置；
b） 应关闭使用环境各软硬件系统中的常见高危端口或服务，例如22端口、23端口、80端口等；
c） 应在重要或核心业务场景的网络中，配置软件系统的实时应用自我防护手段或产品；
d） 应对使用环境中的各软硬件系统执行一致的安全配置。

6.10 漏洞管理

本项要求包括：
a） 应建立内部安全漏洞库，并将权限开放给授权用户；
b） 应定期更新安全漏洞库，并通知组织机构中相关人员；
c） 应在发现安全漏洞时及时记录和报告，并进行跟踪和修复；
d） 应向用户通报安全漏洞并协助用户进行修复；
e） 应将安全漏洞的修复经验及相关知识转化为人员安全开发培训的素材或材料，并进行培训。