



中华人民共和国国家标准

GB/T 47020—2026

网络安全技术 软件物料清单数据格式

Cybersecurity technology—Data format of software bill of materials

2026-01-28 发布

2026-08-01 实施

国家市场监督管理总局 发布
国家标准化管理委员会

目 次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 软件物料清单组成 2

6 软件物料清单文件格式要求 3

7 软件物料清单元素 3

附录 A（资料性） 软件物料清单必选元素和字段 19

附录 B（资料性） 软件物料清单实例参考 21

参考文献 30



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：水利部信息中心、国家能源局信息中心、中国科学院信息工程研究所、南方电网数字电网集团信息通信科技有限公司、西安交通大学、中国电子技术标准化研究院、中国铁道科学研究院集团有限公司电子计算技术研究所、杭州默安科技有限公司、中国信息通信研究院、天翼安全科技有限公司、华为技术有限公司、京东科技信息技术有限公司、阿里云计算有限公司、神州网信技术有限公司、深信服科技股份有限公司、蚂蚁科技集团股份有限公司、广西电网有限责任公司、中国建设银行股份有限公司、软安科技有限公司、杭州孝道科技有限公司、深圳开源互联网安全技术有限公司、杭州安恒信息技术股份有限公司、国家计算机网络应急技术处理协调中心、浙江省水利信息宣传中心、北京天融信网络安全技术有限公司、中兴通讯股份有限公司、中国南水北调集团东线有限公司、中国软件评测中心、重庆长安汽车股份有限公司、长江水利委员会网络与信息中心、麒麟软件有限公司、奇安信网神信息技术(北京)股份有限公司、国网思极网安科技(北京)有限公司、国家信息技术安全研究中心、南方电网科学研究院有限责任公司、水利部海河水利委员会、苏州棱镜七彩信息科技有限公司。

本文件主要起草人：付静、詹全忠、沈智槟、张潮、邹希、戴逸聪、吴桐、刘玉岭、姜政伟、姚叶鹏、范子静、刘家豪、王海军、刘炆、姚相振、王惠莅、张维伦、何娟、沈锡镛、孟瑾、满弘鹏、林谦、栗蔚、郭雪、吴江伟、方宇、梁伟、陈奎强、刘海军、郑伟娜、田凯、方强、牛明珠、孔勇、白晓媛、程岩、谢铭、曾明霏、陈德锋、吴猛、朱辉、吴菊华、徐锋、范丙华、王颀、汪杰、沈蓉芽、王会博、林星辰、魏杰、骆小龙、寇增杰、张金鑫、殷玲玲、杨旭、王新雷、袁薇、孙康健、李鹏、邓烨、李歆、王震、董国伟、张春光、李祉歧、张芝军、刘鸿运、徐传懋、杜金燃、宗华丽、梁大功、黄浩东。



网络安全技术 软件物料清单数据格式

1 范围

本文件规定了软件物料清单数据格式,包括软件物料清单组成、软件物料清单文件格式要求、软件物料清单元素以及软件物料清单中各元素的属性和属性值格式。

本文件适用于指导软件供应链相关方之间进行软件物料清单信息的生成、共享和使用。

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

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

向用户提供的计算机软件、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。

[来源:GB/T 36475—2018,3.1.1]

3.2

软件物料清单 software bill of materials

软件中所包含的所有组件、文件、开源代码片段的清单,以及软件内外部依赖关系和安全信息的描述。

注:软件物料清单包括软件基本信息、软件组成信息、外部依赖信息、安全信息和签名信息。

[来源:GB/T 43698—2024,3.8,有修改]

3.3

外部网络服务 external network service

通过网络为软件运行提供必要功能的非软件自身具备的应用服务。

注:外部网络服务包括域名服务、CDN 服务、邮件发送、短信发送、消息推送、支付接口等服务。

3.4

制品 artifact

由某一种软件开发或运维过程所使用的或产生的一种信息的物理件。

注:制品的实例有模型、源文件、文本和二进制可执行文件。制品构成可部署构件的实现。

[来源:GB/T 42560—2023,3.1.1]



4 缩略语

- 下列缩略语适用于本文件。
- HTTP:超文本传输协议(Hypertext Transfer Protocol)
- JSON:JavaScript 对象标记语言(JavaScript Object Notation)
- RPC:远程过程调用协议(Remote Procedure Call Protocol)
- RTP:实时传输协议(Real-Time Transport Protocol)
- SBOMDF:软件物料清单数据格式(Software Bill of Materials Data Format)
- SMTP:简单邮件传输协议(Simple Mail Transfer Protocol)
- URL:统一资源定位符(Uniform Resource Locator)
- UUID:通用唯一识别码(Universally Unique Identifier)

5 软件物料清单组成

- 软件物料清单由基本信息、软件组成信息、外部依赖信息、安全信息、扩展信息和签名信息六大类信息组成,每类信息包括若干软件物料清单元素(简称“元素”)。图 1 给出了软件物料清单的组成,其中:
- a) 基本信息:描述软件和软件物料清单的标识、来源等基本信息,包括:软件信息和清单信息;
 - b) 软件组成信息:描述软件组成成分、成分来源及其依赖关系的信息,包括:组件信息、文件信息、代码片段信息和内部依赖信息;
 - c) 外部依赖信息:描述软件开发、部署、运行、更新所依赖的外部工具、运行环境、网络服务等必需条件及其来源的信息,包括:外部网络服务信息、基础环境信息和开发工具信息;
 - 注:外部指不包含在软件中的功能、服务、特性等。
 - d) 安全信息:描述软件自身安全和供应链安全管理相关的信息,包括网络服务接口信息、补丁信息、许可证信息、安全漏洞、配置风险和生命周期维护中断风险信息;
 - e) 扩展信息:描述本文件中未定义的其他软件物料信息;
 - f) 签名信息:描述用于验证软件物料清单完整性的数字证书和签名信息,宜使用符合国家或行业规定的机构签发的数字证书。

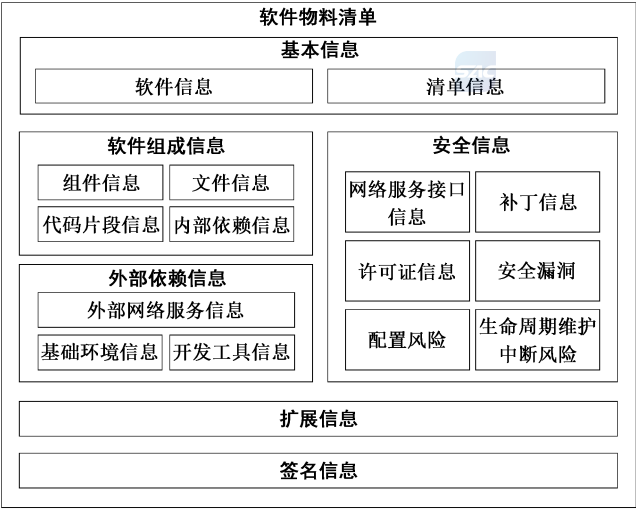


图 1 软件物料清单组成示意图

在不同的使用场景中,并非所有元素和元素字段都是必要信息,附录 A 给出了软件物料清单必选元素集和字段集。

6 软件物料清单文件格式要求

软件物料清单文件为承载软件物料清单信息的一个或一组文本文件,清单文件格式应满足下列要求:

- a) 支持层次化的数据结构,格式简单直观易于阅读;
- b) 支持自动化工具解析处理;
- c) 支持独立于编程语言的通用格式,包括 JSON、XML 等;
- d) 清单文件采用文件系统中容易识别的命名规则,文件名宜包含 SBOMDF,例如:“*.SBOMDF.json”。

附录 B 给出了软件物料清单实例参考。

7 软件物料清单元素

7.1 总则

本章按照软件物料清单信息类别,对每一类别所涉及的元素和元素字段进行描述,每一字段的描述包含字段名、字段描述、字段类型、字段必要性,具体描述规范详见表 1。本章所涉及数据格式描述以 JSON 格式为例,其他格式可参照转换。

表 1 软件物料清单元素字段描述规范

属性	属性描述
字段名	字段命名,应采用无缝连写的英文词汇或词汇组;单词汇采用小写,例如:“signature”;多词汇采用驼峰命名法,即首个词汇小写,后续词汇依次首字母大写,例如:“softwareName”
字段描述	字段的中文名称及其含义解释
字段类型	字段对应数据类型,应为如下类型中的一类:string(字符串)、object(对象)、number(数字)、array(数组)、boolean(布尔)。其中 array 包括: <ul style="list-style-type: none">a) 对象数组:array(of object);b) 字符串数组:array(of string)
字段必要性	字段必要性应为如下三种情况之一: <ul style="list-style-type: none">a) 必选项:元素应包含该字段,应为该字段生成至少一个数据实体;b) 可选项:元素可根据实际情况选择性包含该字段;c) 条件必选:另一个字段选择了一个特定值时,元素应包含该字段

7.2 基本信息类别

7.2.1 类别描述

基本信息类别应包括如下元素:

- a) 软件信息:包含软件所涉及的标识、供应商、来源、授权、完整性等信息;
- b) 清单信息:包含软件物料清单所涉及的版本、标识、创建、获取等信息。

基本信息的各元素描述详见表 2。

表 2 基本信息元素描述

元素名	元素称谓	元素类型	元素必要性
software	软件信息	object	必选项
document	清单信息	object	必选项

7.2.2 软件信息

软件信息应包括如下字段。

- a) 软件名称:软件物料清单归属软件的名称。
- b) 软件版本:软件的版本编号,应为每个版本的软件生成一份软件物料清单。
- c) 软件类型:软件的分类名称,可根据软件的功能、架构、来源或其他特征对其进行分类,如“开源软件”“人工智能软件”等。
- d) 杂凑算法:对软件的制品进行完整性保护的杂凑算法名称。
- e) 消息摘要:对软件的制品通过杂凑运算获取的摘要值。
- f) 软件产品的供应商列表,每个供应商包括如下字段。
 - 1) 供应商:软件供应商的注册名称。
 - 2) 供应商类型:软件供应商的类别,字段取值应为以下之一:
 - integrator:集成商;
 - developer:开发商;
 - agent:代理商;
 - other:其他。
 - 3) 所属区域:软件供应商注册地所属国家省市名称,格式应为“国家-[省]-市”,最小区域至城市,例如:“中国-北京”和“中国-广东-深圳”。
 - 4) 原始供应商:编写软件的人员或组织的名称,供应商类型为集成商或代理商时,本字段应为必选项。
- g) 获取途径:获取开源软件的渠道,字段取值应为以下之一:
 - codeHostingPlatform:代码托管平台;
 - thirdPartyDownloadSite:第三方下载站点;
 - openSourceCommunity:开源社区;
 - other:其他。
- h) 许可证名称:软件的许可证名称,应在许可证信息(见 7.5.4)中提供软件许可证的详细字段数据,如不存在许可证应为 NULL 值。
- i) 授权期限:软件授权使用的截止日期,日期格式应为“YYYY-MM-DD”,如为永久有效,取值应为“permanent”。

软件信息的各字段描述见表 3。

表 3 软件信息字段描述

字段名		字段描述	字段类型	字段必要性
softwareName		软件名称	string	必选项
softwareVersion		软件版本	string	必选项
softwareType		软件类型	string	可选项
integrity	hashAlg	杂凑算法	string	必选项
	messageDigest	消息摘要	string	必选项
supplier	supplierName	供应商	string	必选项
	supplierType	供应商类型	string	可选项
	area	所属区域	string	可选项
	developer	原始供应商	string	条件必选
acquisitionChannels		获取途径	string	可选项
licenseName		许可证名称	string	必选项
licensingTerm		授权期限	string	可选项
注 1：此处以及下文出现的 integrity 均是完整性校验信息，object 类型。				
注 2：此处以及下文出现的 supplier 均是软件的供应商信息，array(of object)类型。				

7.2.3 清单信息

清单信息应包括如下字段。

- a) 清单格式名称：软件物料清单所采用格式标准的名称，应为固定值“SBOMDF”。
- b) 格式版本：软件物料清单遵循的数据格式的版本，本文件对应版本号应为“1.0”。
- c) 清单标识：每个生成的软件物料清单都应有一个唯一的序列号，应采用 128 位的 UUID，匹配正则表达式：`~urn:uuid:[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}$`，示例：`urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79`。
- d) 生命周期：此软件物料清单生成时，软件所处生命周期的阶段，字段取值应为以下之一：
 - develop：开发阶段；
 - commit：交付阶段；
 - operation：运维阶段；
 - decommission：废止阶段。
- e) 时间戳：创建软件物料清单的日期和时间，格式应为“YYYY-MM-DDTHH:mm:ssZ”。
- f) 创建者：创建软件物料清单的实体名称。
- g) 创建工具：创建软件物料清单的工具名称和版本。
- h) 下载链接：获取软件物料清单的 URL 地址。

清单信息的各字段描述见表 4。

表 4 清单信息字段描述

字段名	字段描述	字段类型	字段必要性
formatName	清单格式名称	string	必选项
formatVersion	格式版本	string	必选项
listID	清单标识	string	必选项
lifecycle	生命周期	string	可选项
timestamp	时间戳	string	必选项
authors	创建者	string	必选项
createTools	创建工具	string	可选项
downloadUrl	下载链接	string	可选项

7.3 软件组成信息类别

7.3.1 类别描述

软件组成信息类别应包括如下元素,每个元素可存在多个实例:

- a) 组件信息:软件包含的所有组件列表,每个组件包含组件标识、供应商、许可协议、完整性校验等组件信息;
- b) 文件信息:软件的第一层解压和镜像加载的代码、模型、配置文件、数据集等制品文件列表,包含文件名称、路径、用途、完整性校验等信息;
- c) 代码片段信息:源代码中所包含的从社区、论坛等其他渠道获取的源代码片段列表,包含片段标识、位置、来源、许可证等信息;
- d) 内部依赖信息:描述组件、文件、代码片段之间依赖关系的信息。

软件组成信息的各元素描述详见表 5。

表 5 软件组成信息元素描述

元素名	元素称谓	元素类型	元素必要性
components	组件信息	array(of object)	必选项
files	文件信息	array(of object)	可选项
snippets	代码片段信息	array(of object)	可选项
dependencies	内部依赖信息	array(of object)	必选项

7.3.2 组件信息



组件信息应包括如下字段。

- a) 组件标识:组件在软件物料清单范围内的唯一标识符。
- b) 组件名称:组件的名称,宜使用组件的缩略名称,例如:“commons-lang3”。
- c) 组件版本:组件的版本编号。
- d) 组件描述:组件基本功能的详细描述。

- e) 自研比例:组件中自研代码的占比,字段取值应为以下之一:
 - all:全部自研组件;
 - part:部分自研组件;
 - none:外部组件。
- f) 组件注册标识符:由一定范围(如国家、行业、组织等)内的管理机构维护的唯一识别组件的标识符。
- g) 重要性:组件对于保证软件正常运行的重要程度,例如:可根据组件是否支持核心业务功能判定组件为“关键组件”。
- h) 安全度:描述组件的安全测评结果或安全等级信息,例如:开源组件经过开源社区安全审查情况、组件经过权威机构安全认证情况等。
- i) 组件的供应商列表,每个供应商包括如下字段。
 - 1) 供应商:组件供应商的注册名称,非开源组件应填写本字段。
 - 2) 供应商类型:组件供应商的类别,非开源组件应填写本字段,字段取值应为以下之一:
 - integrator:集成商;
 - developer:开发商;
 - agent:代理商;
 - other:其他。
 - 3) 所属区域:组件供应商注册地所属国家省市名称,格式应为“国家-[省]-市”,最小区域至城市,例如:“中国-北京”和“中国-广东-深圳”,非开源组件应填写本字段。
 - 4) 原始供应商:编写组件的人员或组织的名称,供应商类型为集成商或代理商时,本字段应为必选项,非开源组件应填写本字段。
- j) 获取途径:获取开源组件的渠道,字段取值应为以下之一:
 - codeHostingPlatform:代码托管平台;
 - thirdPartyDownloadSite:第三方下载站点;
 - openSourceCommunity:开源社区。
- k) 组件编程语言:组件使用的编程语言列表。
- l) 许可证名称:组件使用的许可证名称列表,应在许可证信息(见 7.5.4)中提供每个许可证的详细字段数据,如不存在许可证应为 NULL 值。
- m) 下载链接:下载组件的 URL 地址。
- n) 主页链接:查看组件信息的主页 URL 地址。
- o) 组件完备性:组件所包含的下级组件识别信息的完整程度,字段取值应为以下之一:
 - none:无下级组件;
 - known:全部列出下级组件;
 - part:部分列出下级组件;
 - unknown:未知,不知道当前组件的下级组件。
- p) 杂凑算法:对组件进行完整性保护的杂凑算法名称。
- q) 消息摘要:对组件通过杂凑运算获取的摘要值。

组件信息的各字段描述见表 6。

表 6 组件信息字段描述

字段名		字段描述	字段类型	字段必要性
componentId		组件标识	string	必选项
componentName		组件名称	string	必选项
componentVersion		组件版本	string	必选项
componentDescription		组件描述	string	可选项
selfDevelopedProportion		自研比例	string	可选项
regIdentifier		组件注册标识符	string	可选项
importance		重要性	string	可选项
security		安全度	string	可选项
supplier	supplierName	供应商	string	必选项
	supplierType	供应商类型	string	可选项
	area	所属区域	string	可选项
	developer	原始供应商	string	条件必选
acquisitionChannel		获取途径	string	可选项
progLanguage		组件语言	array(of string)	可选项
licenseName		许可证名称	array(of string)	必选项
downloadUrl		下载链接	string	可选项
homepageUrl		主页链接	string	可选项
completeness		组件完备性	string	可选项
integrity	hashAlg	杂凑算法	string	必选项
	messageDigest	消息摘要	string	必选项

7.3.3 文件信息

文件信息应包括如下字段：

- a) 文件标识：文件在软件物料清单范围内的唯一标识符；
- b) 文件名称：包含扩展名的完整文件名称；
- c) 文件路径：文件在制品文件目录中的完整相对路径；
- d) 用途描述：文件在软件中的功能和作用的简要说明；
- e) 杂凑算法：对文件进行完整性保护的杂凑算法名称；
- f) 消息摘要：对文件通过杂凑运算获取的摘要值。

文件信息的各字段描述见表 7。

表 7 文件信息字段描述

字段名		字段描述	字段类型	字段必要性
fileId		文件标识	string	必选项
fileName		文件名称	string	必选项
filePath		文件路径	string	必选项
purpose		用途描述	string	可选项
integrity	hashAlg	杂凑算法	string	可选项
	messageDigest	消息摘要	string	可选项

7.3.4 代码片段信息

代码片段信息应包括如下字段：

- a) 片段标识:代码片段在软件物料清单范围内的唯一标识符；
- b) 关联文件:包含此代码片段的文件的路径和文件名；
- c) 起点字节数:代码片段在源文件中的起始位置(按字节计算)；
- d) 终点字节数:代码片段在源文件中的结束位置(按字节计算)；
- e) 起点行数:代码片段在源文件中的起始位置(按行数计算)；
- f) 终点行数:代码片段在源文件中的结束位置(按行数计算)；
- g) 片段来源:代码片段来源的 URL 地址；
- h) 所属开源项目:代码片段所属开源项目名称；
- i) 许可证名称:列出代码片段相关的许可证名称,如不存在许可证应为 NULL 值,可在安全信息类别(见 7.5)中找到对应的代码片段许可证信息(见 7.5.4)；
- j) 杂凑算法:对代码片段进行完整性保护的杂凑算法名称；
- k) 消息摘要:对代码片段通过杂凑运算获得的摘要值。

代码片段信息的各字段描述见表 8。

表 8 代码片段信息字段描述

字段名		字段描述	字段类型	字段必要性
snippetId		片段标识	string	必选项
snippetFile		关联文件	string	必选项
byteStartPointer		起点字节数	number	必选项
byteEndPointer		终点字节数	number	必选项
lineStartPointer		起点行数	number	必选项
lineEndPointer		终点行数	number	必选项
snippetSource		片段来源	string	可选项
affiliatedProject		所属开源项目	string	可选项
licenseName		许可证名称	string	必选项
integrity	hashAlg	杂凑算法	string	可选项
	messageDigest	消息摘要	string	可选项

7.3.5 内部依赖信息

内部依赖信息应包括如下字段。

- a) 依赖标识:描述存在依赖关系的组件、文件或代码片段实体在本软件物料清单范围内的标识符。
- b) 关系:描述关系的类型,包括:
 - dependsOn:依赖;
 - contain:包含;
 - other:其他。
- c) 被依赖标识:描述被依赖的组件、文件或代码片段实体在本软件物料清单范围内的标识符。

内部依赖信息的各字段描述见表 9。

表 9 内部依赖信息字段描述

字段名	字段描述	字段类型	字段必要性
identityAId	依赖标识	string	必选项
relationship	关系	string	必选项
identityBId	被依赖标识	string	必选项



7.4 外部依赖信息类别

7.4.1 类别描述

外部依赖信息类别应包括如下元素,每个元素可存在多个实例:

- a) 外部网络服务信息:为软件运行提供必要功能的外部网络服务列表(例如:域名服务、CDN 服务、邮件发送、短信发送、支付接口等),包含服务名称、可替代性、供应商、服务环境、服务数据等信息;
- b) 基础环境信息:支撑软件运行的数据库管理系统、web 应用框架、中间件、操作系统、BIOS 等基础运行环境的列表,包含基础环境名称、版本、可替代性、供应商等信息;
- c) 开发工具信息:能够生成或影响最终软件代码的开发工具的列表,例如:编译器、构建工具、配置管理工具等,包含开发工具名称、版本、用途等信息。

外部依赖信息的各元素描述详见表 10。

表 10 外部依赖信息元素描述

元素名	元素称谓	元素类型	元素必要性
services	外部网络服务信息	array(of object)	可选项
platform	基础环境信息	array(of object)	可选项
developmentTools	开发工具信息	array(of object)	可选项

7.4.2 外部网络服务信息

外部网络服务信息应包括如下字段。

- a) 服务标识:外部网络服务在软件物料清单范围内的唯一标识符。

- b) 服务名称:外部网络服务的中英文名称。
 - c) 可替代性:是否存在其他的供应商能提供相同功能的外部网络服务,包括:
 - true:存在;
 - false:不存在。
 - d) 供应商:外部网络服务供应商的注册名称,如果可替代性取值为“false”,本字段应为必选项。
 - e) 所属区域:外部网络服务供应商注册地所属国家省市名称,格式为“国家-[省]-市”,最小区域至城市,例如:“中国-北京”和“中国-广东-深圳”,如果可替代性取值为“false”,本字段为必选项。
 - f) 服务地址:服务端的 URL 地址,如果可替代性取值为“false”,本字段应为必选项。
 - g) 服务环境:服务端所在地理位置区域,如果可替代性取值为“false”,本字段应为必选项,字段取值应为以下之一:
 - domestic:国内计算环境;
 - overseas:国外计算环境。
 - h) 服务协议:服务使用的网络应用协议的名称,例如:HTTP、SMTP、DNS 等。
 - i) 数据描述:对服务传输的敏感数据内容的描述。
- 外部网络服务信息的各字段描述见表 11。

表 11 外部网络服务信息字段描述

字段名		字段描述	字段类型	字段必要性
serviceId		服务标识	string	必选项
serviceName		服务名称	string	必选项
substitutability		可替代性	boolean	必选项
supplier	supplierName	供应商	string	条件必选
	area	所属区域	string	条件必选
serviceUrl		服务地址	string	条件必选
serviceArea		服务环境	string	条件必选
serviceProtocol		服务协议	string	可选项
dataDescription		数据描述	string	可选项

7.4.3 基础环境信息

- 基础环境信息应包括如下字段。
- a) 基础环境标识:基础环境软件在软件物料清单范围内的唯一标识符。
 - b) 基础环境名称:可用于识别基础环境软件的名称。
 - c) 基础环境版本:基础环境软件的版本编号。
 - d) 可替代性:软件是否支持其他供应商提供的相同功能的基础环境软件,包括:
 - true:支持;
 - false:不支持。
 - e) 供应商:基础环境软件供应商的注册名称,如果可替代性取值为“false”,本字段应为必选项。
 - f) 所属区域:外部网络服务供应商注册地所属国家省市名称,格式应为“国家-[省]-市”,最小区域至城市,例如:“中国-北京”和“中国-广东-深圳”,如果可替代性取值为“false”,本字段应为必选项。
- 基础环境信息的各字段描述见表 12。

表 12 基础环境信息字段描述

字段名		字段描述	字段类型	字段必要性
assetId		基础环境标识	string	必选项
assetName		基础环境名称	string	必选项
assetVersion		基础环境版本	string	必选项
substitutability		可替代性	boolean	必选项
supplier	supplierName	供应商	string	条件必选
	area	所属区域	string	条件必选

7.4.4 开发工具信息

- 开发工具信息应包括如下字段：
- a) 工具标识:开发工具在软件物料清单范围内的唯一标识符；
 - b) 工具名称:开发工具的名称；
 - c) 工具类型:开发工具的类型说明,例如:代码编辑器、配置管理工具、需求跟踪工具、代码仓库、持续集成/部署工具、包管理器、容器工具等；
 - d) 工具版本:开发工具的版本编号；
 - e) 用途描述:使用开发工具完成开发工作内容的简要说明。
- 开发工具信息的各字段描述见表 13。

表 13 开发工具信息字段描述

字段名	字段描述	字段类型	字段必要性
toolId	工具标识	string	必选项
toolName	工具名称	string	必选项
toolType	工具类型	string	可选项
toolVersion	工具版本	string	必选项
purpose	用途描述	string	可选项

7.5 安全信息类别



7.5.1 类别描述

- 安全信息类别应包括如下元素,每个元素可存在多个实例：
- a) 网络服务接口信息:软件提供的可被访问或调用的网络服务接口列表,包含接口描述、协议、地址、请求方式等信息；
 - b) 补丁信息:从软件发布到生成软件物料清单期间为了修复问题和漏洞、优化性能而发布的补丁列表,包含补丁名称、原厂标识、用途描述等信息；
 - c) 许可证信息:软件及其组件和代码片段中使用的许可证列表,包含许可证名称、内容、风险等信息；
 - d) 安全漏洞:生成软件物料清单之前可检测但已修复的组件安全漏洞信息列表,包含漏洞名称、相关编号、影响对象、修复情况等信息；

- e) 配置风险:从软件发布到生成软件物料清单期间发现的软件默认配置项可能存在的已知配置风险信息列表,包含风险名称、受影响配置项、处置建议等信息;
- f) 生命周期维护中断风险:软件生命周期中可能发生的维护服务终止的风险列表,包含中断类型、描述、预计中断时间、处置情况等信息。

安全信息的各元素描述详见表 14。

表 14 安全信息元素描述

元素名	元素称谓	元素类型	元素必要性
interfaces	网络服务接口信息	array(of object)	可选项
patches	补丁信息	array(of object)	可选项
licenses	许可证信息	array(of object)	必选项
vulnerabilities	安全漏洞	array(of object)	必选项
configRisks	配置风险	array(of object)	可选项
disruptions	生命周期维护中断风险	array(of object)	可选项

7.5.2 网络服务接口信息

网络服务接口信息应包括如下字段。

- a) 接口标识:接口在软件物料清单范围内的唯一标识符。
- b) 接口类型:接口的类型,例如:RESTful、RPC 等。
- c) 接口描述:描述接口调用方法和具体功能的信息。
- d) 接口必要性:接口对软件在当前配置状态下正常使用的必要性说明,包括:
 - true:必要;
 - false:非必要。
- e) 请求方式:接口的请求方式,例如:GET、POST、HEAD 等,接口类型为“RESTful”时,此字段应为必选项。
- f) 接口地址:接口访问 URL 地址,可有一个或多个接口地址,接口类型为“RESTful”时,此字段应为必选项。
- g) 方法签名:接口在代码中的入口点函数名和参数列表,接口类型为“RESTful”时,此字段应为必选项。

网络服务接口信息的各字段描述见表 15。

表 15 网络服务接口信息字段描述

字段名	字段描述	字段类型	字段必要性
interfaceId	接口标识	string	必选项
interfaceType	接口类型	string	必选项
description	接口描述	string	必选项
necessity	接口必要性	boolean	可选项
requestMethod	请求方式	string	条件必选
interfaceAddress	接口地址	array(of string)	条件必选
method	方法签名	string	条件必选

7.5.3 补丁信息

- 补丁信息应包括如下字段：
- a) 补丁标识:补丁在软件物料清单范围内的唯一标识符；
 - b) 补丁名称:可用于识别补丁的名称；
 - c) 补丁版本:补丁的版本编号；
 - d) 发布日期:公开发布补丁的日期,日期格式为“YYYY-MM-DD”；
 - e) 原厂标识:软件原始供应商维护的补丁唯一标识符；
 - f) 补丁地址:下载补丁的 URL 地址；
 - g) 用途描述:补丁更新内容等说明信息；
 - h) 补丁清单文件:补丁配套的软件物料清单文件名称,应为每个补丁文件建立软件物料清单。
- 补丁信息的各字段描述见表 16。

表 16 补丁信息字段描述

字段名	字段描述	字段类型	字段必要性
patchId	补丁标识	string	必选项
patchName	补丁名称	string	必选项
patchVersion	补丁版本	string	必选项
releaseDate	发布日期	string	必选项
originalId	原厂标识	string	必选项
patchAddress	补丁地址	string	可选项
purpose	用途描述	string	可选项
patchSbom	补丁清单文件	string	可选项

7.5.4 许可证信息

- 许可证信息应包括如下字段。
- a) 许可证标识:许可证在软件物料清单范围内的唯一标识符。
 - b) 许可证名称:软件、组件、代码片段使用的许可证名称,许可证名称应与软件信息、组件信息、代码片段信息中的 licenseName 字段值一一对应。
 - c) 下载链接:获取许可证信息的 URL 地址。
 - d) 许可方:授予许可证的个人或组织的名称,本字段适用于商用许可证。
 - e) 被许可方:被授予许可证的个人或组织的名称,本字段适用于商用许可证。
 - f) 到期日期:商用许可证有效期最后一天的日期,日期格式应为“YYYY-MM-DD”,如果是永久有效,本字段应填“permanent”,本字段适用于商用许可证。
 - g) 条款约束:使用者的权利和义务的详细描述。
 - h) 适用范围:许可证适用地理区域范围,例如:“全球”。
 - i) 专利权:许可证是否包含授予专利许可的声明,包括:
 - true:包含；
 - false:不包含。
 - j) 风险描述:许可证的风险信息的详细描述,例如:违规使用许可证的行为和可能造成的影响。
- 许可证信息的各字段描述见表 17。

表 17 许可证信息字段描述

字段名	字段描述	字段类型	字段必要性
licenseId	许可证标识	string	必选项
licenseName	许可证名称	string	必选项
downloadUrl	下载链接	string	可选项
licensor	许可方	string	可选项
licensee	被许可方	string	可选项
term	到期日期	string	可选项
content	条款约束	string	必选项
scope	适用范围	string	必选项
patent	专利权	boolean	必选项
riskDescription	风险描述	string	必选项

7.5.5 安全漏洞

安全漏洞应包括如下字段。

- a) 漏洞标识:漏洞在软件物料清单范围内的唯一标识符。
- b) 漏洞名称:漏洞信息的概括性描述。
- c) 影响对象:存在漏洞的组件在软件物料清单范围内的标识符。
- d) 相关编号:漏洞发布平台提供的漏洞编号,例如:“CNVD-2023-27109”,可有多个相关编号。
- e) 修复方式:修复组件漏洞采取的措施类型,包括:
 - codeLevel:代码级修复;
 - patchRepair:使用补丁修复;
 - other:其他缓解措施。
- f) 关联补丁:修复安全漏洞使用的补丁在本软件物料清单范围内的标识符,如果修复方式为“使用补丁修复”,则本字段应为必选字段。
- g) 修复方式说明:修复组件漏洞的采取措施的详细说明。

安全漏洞的各字段描述见表 18。

表 18 安全漏洞字段描述

字段名	字段描述	字段类型	字段必要性
vulnerabilityId	漏洞标识	string	必选项
vulnerabilityName	漏洞名称	string	必选项
affectedObject	影响对象	string	必选项
otherID	相关编号	array(of string)	必选项
repairMethod	修复方式	string	必选项
relatedPatch	关联补丁	string	条件必选
repairMethodDescription	修复方式说明	string	必选项

7.5.6 配置风险

配置风险应包括如下字段：

- a) 配置风险标识:配置风险在软件物料清单范围内的唯一标识符；
- b) 配置风险名称:描述配置风险的简短的名称；
- c) 配置项:存在安全风险的配置项及其默认取值的描述；
- d) 处置建议:配置风险处置建议的描述；
- e) 检测工具:推荐的配置风险检测工具名称；
- f) 相关链接:可获取配置风险详细信息的 URL 地址。

配置风险的各字段描述见表 19。

表 19 配置风险字段描述

字段名	字段描述	字段类型	字段必要性
configRiskId	配置风险标识	string	必选项
configRiskName	配置风险名称	string	必选项
configItem	配置项	string	必选项
suggestion	处置建议	string	可选项
testingTool	检测工具	string	可选项
relatedUrl	相关链接	string	可选项

7.5.7 生命周期维护中断风险

生命周期维护中断风险应包括如下字段。

- a) 中断标识:中断风险的在软件物料清单范围内的唯一标识符。
- b) 中断类型:说明引起中断的具体原因,包括：
 - authorizationExpires:证书授权到期；
 - notUpdated:长期未更新；
 - stopUpdating:停止更新；
 - singleSource:有且只有唯一高风险供应商；
 - others:其他。
- c) 影响对象:受中断风险影响的组件、外部网络服务、基础环境在软件物料清单范围内的标识。
- d) 风险描述:中断风险的详细说明。
- e) 预计中断时间:可能发生中断事件的具体时间,格式应为“YYYY-MM-DDTHH:mm:ssZ”。
- f) 处置情况:针对存在生命周期维护中断风险的外部组件,供应商是否能够在中断事件发生后继续提供运维服务的说明,包括：
 - true:能够继续提供运维服务；
 - false:不能继续提供运维服务。

生命周期维护中断风险的各字段描述见表 20。

表 20 生命周期维护中断风险字段描述

字段名	字段描述	字段类型	字段必要性
disruptionId	中断标识	string	必选项
disruptionType	中断类型	string	必选项
affectedObject	影响对象	string	必选项
description	风险描述	string	必选项
estimatedTime	预计中断时间	string	必选项
disposal	处置情况	boolean	必选项

7.6 扩展信息类别

7.6.1 类别描述

扩展信息类别应包括扩展信息,扩展信息可存在多个实例,包含本文件中未定义的其他物料信息。
扩展信息的各元素描述详见表 21。

表 21 扩展信息元素描述

元素名	元素称谓	元素类型	元素必要性
properties	扩展信息	array(of object)	可选项

7.6.2 扩展信息

扩展信息应包括如下字段：
a) 属性名称:自定义的属性名称；
b) 属性值:属性的具体取值。
扩展信息的各字段描述见表 22。

表 22 扩展信息字段描述

字段名	字段描述	字段类型	字段必要性
propertieName	属性名称	string	可选项
propertieValue	属性值	string	可选项

7.7 签名信息类别

7.7.1 类别描述

签名信息类别应包括签名信息,包含软件物料清单所有内容的数字签名。
签名信息的各元素描述详见表 23。

表 23 签名信息元素描述

元素名	元素称谓	元素类型	元素必要性
integrity	签名信息	object	必选项

7.7.2 签名信息

签名信息应包括如下字段：

- a) 签名文件：保存签名后的摘要信息的文件名称，签名文件应与软件物料清单同时交付；
- b) 数字证书文件：保存用于验签的数字证书的文件名称，数字证书文件应与软件物料清单同时交付。

签名信息的各字段描述见表 24。

表 24 签名信息字段描述

字段名	字段描述	字段类型	字段必要性
signatureFile	签名文件	string	必选项
digitalCertificateFile	数字证书文件	string	必选项



附 录 A
(资料性)

软件物料清单必选元素和字段

表 A.1 给出了本文件所规定的软件物料清单数据格式的必选元素以及必选元素的必选字段。

表 A.1 软件物料清单必要字段

元素名	字段名		字段描述	字段类型
软件信息 software	softwareName		软件名称	string
	softwareVersion		软件版本	string
	integrity	hashAlg	杂凑算法	string
		messageDigest	消息摘要	string
	supplier	supplierName	供应商	string
	licenseName		许可证名称	string
清单信息 document	formatName		清单格式名称	string
	formatVersion		格式版本	string
	listID		清单标识	string
	timestamp		时间戳	string
	authors		创建者	string
组件信息 components	componentId		组件标识	string
	componentName		组件名称	string
	componentVersion		组件版本	string
	supplier	supplierName	供应商	string
	licenseName		许可证名称	array(of string)
	integrity	hashAlg	杂凑算法	string
messageDigest		消息摘要	string	
内部依赖信息 dependencies	identityAId		依赖标识	string
	relationship		关系	string
	identityBId		被依赖标识	string
许可证信息 licenses	licenseId		许可证标识	string
	licenseName		许可证名称	string
	content		条款约束	string
	scope		适用范围	string
	patent		专利权	boolean
	riskDescription		风险描述	string

表 A.1 软件物料清单必要字段（续）

元素名	字段名	字段描述	字段类型
安全漏洞 vulnerabilities	vulnerabilityId	漏洞标识	string
	vulnerabilityName	漏洞名称	string
	affectedObject	影响对象	string
	otherID	相关编号	array(of string)
	repairMethod	修复方式	string
	repairMethodDescription	修复方式说明	string
签名信息 integrity	signatureFile	签名文件	string
	digitalCertificateFile	数字证书文件	string



附 录 B
(资料性)
软件物料清单实例参考

B.1 软件信息

JSON 格式示例如下。

a) 定制化开发或商业采购软件:

```
{
  "software": {
    "softwareName": "MyApp",
    "softwareVersion": "1.2.0",
    "softwareType": "财务软件",
    "integrity": {
      "hashAlg": "SM3",
      "messageDigest": "DGKCqI9VdT2NNDc0RuVu3jWcxhVT69R5kn2S4UfYUpQ="
    },
    "supplier": {
      "supplierName": "supplierA",
      "supplierType": "agent",
      "area": "中国-北京",
      "developer": "developerA"
    },
    "licenseName": "Commercial Agreement A",
    "licensingTerm": "2024-11-11"
  }
}
```

b) 开源软件:

```
{
  "software": {
    "softwareName": "MyApp",
    "softwareVersion": "1.2.0",
    "softwareType": "手机应用",
    "integrity": {
      "hashAlg": "SM3",
      "messageDigest": "DGKCqI9VdT2NNDc0RuVu3jWcxhVT69R5kn2S4UfYUpQ="
    },
    "supplier": {
      "supplierName": "supplierA",
      "supplierType": "agent",
      "area": "中国-北京",
      "developer": "developerA"
    }
  }
}
```

```

    },
    "acquisitionChannels": "openSourceCommunity",
    "licenseName": "Apache-2.0"
  }
}

```

B.2 清单信息

JSON 格式示例：

```

{
  "document": {
    "formatName": "SBOMDF",
    "formatVersion": "1.0",
    "listID": "urn:uuid:f47ac10b-58cc-4372-a567-0e02b2c3d479",
    "lifecycle": "commit",
    "timestamp": "2024-01-10 10:00:00",
    "authors": "SBOMDF CreatorA",
    "createTools": "Automation Tool v2.1",
    "downloadUrl": "https://myapp.com/download/sbom"
  }
}

```

B.3 组件信息

JSON 格式示例如下。

a) 定制化开发或商业采购组件：



```

{
  "components": [
    {
      "componentId": "lib-001",
      "componentName": "Logging Library",
      "componentVersion": "2.5",
      "componentDescription": "Library for application logging.",
      "selfDevelopedProportion": "none",
      "regIdentifier": "cpe:/a:microsoft:sql_server:6.5",
      "importance": "核心组件",
      "security": "经过三方机构安全检测",
      "supplier": {
        "supplierName": "supplierA",
        "supplierType": "integrator",
        "area": "中国-北京",
        "developer": "developerA"
      },
      "progLanguage": "Java",
      "licenseName": [

```

```
        " Protocol A",
        " Protocol B"
    ],
    "downloadUrl": "https://logcorp.com/log-lib",
    "homePageUrl": "https://logcorp.com",
    "completeness": "known",
    "integrity": {
        "hashAlg": "SM3",
        "messageDigest": "QCLy7eCQId565vH10JLeNiDestumsDXCSvuKDeH4hyk="
    }
}
]
}
```

b) 开源组件:

```
{
    "components": [
        {
            "componentId": "lib-001",
            "componentName": "Logging Library",
            "componentVersion": "2.5",
            "componentDescription": "Library for application logging.",
            "selfDevelopedProportion": "none",
            "regIdentifier": "cpe:/a:microsoft:sql_server:6.5",
            "importance": "核心组件",
            "security": "经过开源社区安全审查",
            "supplier": {
                "supplierName": "supplierA",
                "supplierType": "integrator",
                "area": "中国-北京",
                "developer": "developerA"
            },
            "acquisitionChannel": "openSourceCommunity",
            "progLanguage": "Java",
            "licenseName": [
                " Protocol A",
                " Protocol B"
            ],
            "downloadUrl": "https://logcorp.com/log-lib",
            "homePageUrl": "https://logcorp.com",
            "completeness": "known",
            "integrity": {
                "hashAlg": "SM3",
                "messageDigest": "QCLy7eCQId565vH10JLeNiDestumsDXCSvuKDeH4hyk="
            }
        }
    ]
}
```

```

    }
  }
]
}

```

B.4 文件信息

JSON 格式示例：

```

{
  "files": [
    {
      "fileId": "file-001",
      "fileName": "syslog.java",
      "filePath": "/src/com/myapp/syslog.java",
      "purpose": "实现软件日志信息生成的源代码文件",
      "integrity": {
        "hashAlg": "SM3",
        "messageDigest": "KngAbinsojIjJVoxBp9Q95QihvXWcX/o38FKItCjoE="
      }
    }
  ]
}

```

B.5 代码片段信息

JSON 格式示例：

```

{
  "snippets": [
    {
      "snippetId": "snippet-001",
      "snippetFile": "/src/com/myapp/Main.java",
      "byteStartPointer": 100,
      "byteEndPointer": 200,
      "lineStartPointer": 10,
      "lineEndPointer": 20,
      "snippetSource": "Open source project A",
      "affiliatedProject": "http://www.OpenSourceCommunity.org/projectA/homepage",
      "licenseName": "Apache License 2.0",
      "integrity": {
        "hashAlg": "SM3",
        "messageDigest": "uzq67gmmvlhwe15NG7BwHLeDmPYTB4oPYQX6AiZuR4w="
      }
    }
  ]
}

```



B.6 内部依赖信息

JSON 格式示例：

```
{
  "dependencies": [
    {
      "identityAId": "lib-001",
      "relationship": "dependsOn",
      "identityBId": "lib-002"
    },
    {
      "identityAId": "file-001",
      "relationship": "contains",
      "identityBId": "snippet-001"
    }
  ]
}
```

B.7 外部网络服务信息

JSON 格式示例：

```
{
  "services": [
    {
      "serviceId": "service-001",
      "serviceName": "Authentication Service",
      "substitutability": false,
      "supplier": {
        "supplierName": "payment service provider",
        "area": "中国-北京"
      },
      "serviceUrl": "https://auth.servicecorp.com/api",
      "serviceArea": "国内计算环境",
      "serviceProtocol": "http",
      "dataDescription": "包含电话、身份证、银行卡号等个人隐私信息"
    }
  ]
}
```

B.8 基础环境信息

JSON 格式示例：

```
{
  "platform": [
    {
```

```

        "assetId": "java-runtime",
        "assetName": "Java Runtime Environment",
        "assetVersion": "8.0",
        "substitutability": false,
        "supplier": {
            "supplierName": "Java provider",
            "area": "中国-北京"
        }
    }
]
}

```

B.9 开发工具信息

JSON 格式示例：

```

{
    "developmentTools": [
        {
            "toolId": "tool-001",
            "toolName": "IDE",
            "toolType": "代码编辑器",
            "toolVersion": "5.3",
            "purpose": "编辑源代码"
        }
    ]
}

```

B.10 网络服务接口信息

JSON 格式示例：

```

{
    "interfaces": [
        {
            "interfaceId": "INT-001",
            "interfaceType": "RESTful",
            "description": "这是一个对外提供远程更新服务的外部接口",
            "necessity": false,
            "requestMethod": "GET",
            "interfaceAddress": "http://192.168.1.127/api/update",
            "method": "update"
        }
    ]
}

```


B.11 补丁信息

JSON 格式示例：

```
{
  "patches": [
    {
      "patchId": "patch-001",
      "patchName": "Security Update",
      "patchVersion": "1.0.0",
      "releaseDate": "2023-03-15",
      "originalId": "software_patch_v1.0",
      "patchAddress": "http://www.company.org/patch/download",
      "perpose": "修复软件登录模块安全漏洞",
      "patchSbom": "patch.SBOMDF.json"
    }
  ]
}
```

B.12 许可证信息

JSON 格式示例如下。

a) 开源许可证：

```
{
  "licenses": [
    {
      "licenseId": " License-001",
      "licenseName": " LGPL-3.0",
      "downloadUrl": "http://www.apache.org/licenses/",
      "content": "This license text includes a warranty disclaimer.",
      "scope": "Global",
      "patent": "有专利权",
      "riskDescription": "该协议为强传染性协议"
    }
  ]
}
```

b) 商业许可证：

```
{
  "licenses": [
    {
      "licenseId": " License-002",
      "licenseName": " Commercial License A",
      "downloadUrl": "http://www.apache.org/licenses/",
      "licensor": "CompanyA",
      "licensee": "CompanyB",

```

```

        "term": "2024-05-01",
        "content": "This license text includes a warranty disclaimer.",
        "scope": "Global",
        "patent": "有专利权",
        "riskDescription": "该协议限制多用户共享单个许可证,请勿与其他用户共享。"
    }
]
}

```

B.13 安全漏洞

JSON 格式示例:

```

{
    "vulnerabilities": [
        {
            "vulnerabilityId": "vul-001",
            "vulnerabilityName": "心脏滴血",
            "affectedObject": "lib-001",
            "otherID": [
                "CVE-2014-0160",
                "CNVD-2014-31337"
            ],
            "repairMethod": "code level",
            "relatedPatch": "patch-20250615-security-uuid-validation-fix-v1.0.2",
            "repairMethodDescription": "修改代码,通过使用数据库提供的参数化查询接口,将用户输入的变量作为参数传递给 SQL 语句。"
        }
    ]
}

```

B.14 配置风险

JSON 格式示例:

```

{
    "configRisks": [
        {
            "configRiskId": "con-001",
            "configRiskName": "数据安全风险",
            "configItem": "数据库远程访问功能设置为开启",
            "suggestion": "该配置可能导致数据泄露,建议设置为关闭。",
            "testingTool": "ToolA",
            "relatedUrl": "https://configuration.risk.com"
        }
    ]
}

```



B.15 生命周期维护中断风险

JSON 格式示例：

```
{
  "disruptions": [
    {
      "disruptionId": "Drp-001",
      "disruptionType": "stop updating",
      "affectedObject": "lib-003",
      "description": "由于知识产权纠纷,该组件已停止更新",
      "estimatedTime": "2023-06-10 09:30:00",
      "disposal": false
    }
  ]
}
```

B.16 签名信息

JSON 格式示例：

```
{
  "integrity": {
    "signatureFile": "Value.txt",
    "digitalCertificateFile": "certification.pem"
  }
}
```



参 考 文 献

- [1] GB/T 36475—2018 软件产品分类
 - [2] GB/T 42560—2023 系统与软件工程 开发运维一体化 能力成熟度模型
 - [3] GB/T 43698—2024 网络安全技术 软件供应链安全要求
 - [4] ISO/IEC 5962:2021 Information technology—SPDX[®] Specification V2.2.1
 - [5] IETF RFC 8259 The JavaScript Object Notation (JSON) Data Interchange Format
-

