|  |  |
| --- | --- |
| ；ICS  | 35.030 |
| CCS  | L80 |

中华人民共和国国家标准

GB/T XXXXX—XXXX

网络安全技术 软件物料清单数据格式

Cybersecurity technology-Software bill of materials data format

征求意见稿

2024-04-26

XXXX - XX - XX发布

XXXX - XX - XX实施

`

目次

[前言 II](#_Toc164987705)

[引言 III](#_Toc164987706)

[1 范围 4](#_Toc164987707)

[2 规范性引用文件 4](#_Toc164987708)

[3 术语和定义 4](#_Toc164987709)

[4 缩略语 5](#_Toc164987714)

[5 软件物料清单组成 5](#_Toc164987715)

[6 清单文件格式要求 6](#_Toc164987716)

[7 软件物料清单元素 6](#_Toc164987717)

[附录A （资料性） 软件物料清单必要字段 21](#_Toc164987724)

[附录B （资料性） 软件物料清单实例参考 23](#_Toc164987725)

[参考文献 32](#_Toc164987742)

1. 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。

本文件由全国网络安全标准化技术委员会（SAC/TC260）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、中国信息通信研究院、南方电网数字电网集团有限公司、西安交通大学、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。

本文件主要起草人：付静、詹全忠、张潮、沈智镔、邹希、栗蔚、郭雪、吴江伟、吴桐、刘玉岭、姜政伟、姚叶鹏、范子静、刘家豪、王定波、关声涛、王海军、刘烃、晋武侠、杨立鹏、张维伦、何娟、沈锡镛、孟瑾、满弘鹏。

1. 引言

软件物料清单描述了软件组成信息，以提升软件产品的成分透明度，为软件的供应链安全管理提供支撑。本文件提出了软件物料清单数据格式，以实现相关信息在软件生产、销售和使用各相关方之间的交换和使用。。

软件物料清单数据格式描述软件的内部组成和内外部依赖，包括构成软件的组件、文件、代码片段及其依赖关系，软件运行依赖的基础环境和外部网络服务，以及软件生产依赖的开发工具，并且提供必要的安全信息，为软件物料清单信息的生成、共享和使用提供参考。

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和软件物料清单元素，以及软件物料清单中各元素的属性和属性值格式等信息。

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。

* 1. 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 11457-2006 信息技术 软件工程术语

GB/T 25069-2022 信息安全技术 术语

GB/T 36475-2018 软件产品分类

* 1. 术语和定义

GB/T 25069－2022中界定的以及下列术语和定义适用于本文件。

* + 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。

注1：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]

* + 1.

软件物料清单 software bill of materials

描述软件产品的组成成分、内外部依赖关系、来源信息以及潜在的安全风险信息的清单。

注1：本文件中清单为软件物料清单的简称。

* + 1.

外部网络服务 external 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，例如：域名服务、CDN服务、邮件发送、短信发送、消息推送、支付接口等。

* + 1.

制品 artifact

由某一种软件开发过程所使用的或所产生的一种信息的文件。制品的实例有模型、源文件、文本和二进制可执行文件。

[来源：GB/T 11457-2006，2.76，有修改]

* 1. 缩略语

CPE：通用平台枚举（Common Platform Enumeration）

HTTP：超文本传输协议（Hypertext Transfer Protocol）

JSON：JavaScript对象标记语言（JavaScript Object Notation）

PURL：包统一资源定位符（Package Uniform Resource Locators）

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）

* 1. 软件物料清单组成

特定版本的软件应有一份对应的软件物料清单。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，每类信息包括若干清单元素（简称“元素”）。本文件对每个清单元素所涉及的字段进行了规定。图1给出了软件物料清单的组成，其中：

1. 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；
2. 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；
3. 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。

1. 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；
2. 扩展信息：描述本文件中未定义的其他软件物料信息；
3. 签名信息：描述用于验证清单完整性的数字证书和签名信息，应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，本文件规定了支持清单基本功能的最小元素集，包括软件信息、清单信息、组件信息、内部依赖信息和签名信息等元素。最小元素集的必要字段详见附录A。

* 1. 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以下要求：

1. 应支持人类容易理解和解释的格式；
2. 应支持自动化工具解析处理；
3. 应支持独立于编程语言的通用格式，包括JSON、XML等；
4. 清单文件的命名应以SBOMDF为后缀，例如：“\*.SBOMDF.json”。
	1. 软件物料清单元素
		1. 概述

本章按照软件物料清单信息类别，对每一类别所涉及的清单元素和元素字段的进行描述，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。

1. 清单信息字段描述

|  |  |
| --- | --- |
| 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）、enum（枚举）、boolean（布尔）。 |
| 字段必要性 | 字段必要性应为如下三种情况之一：1. 必选项：清单中必须包含该字段，并为该字段生成至少一个数据实体。
2. 可选项：清单中可根据实际情况选择性的包含该字段。
3. 条件必选：某些条件下必须包含该字段，包括:
* 当选用另一个字段时，此字段为必选；
* 当另一个字段选择了一个特定值时,此字段为必选。
 |

* + 1. 基本信息类别
			1. 类别概述

基本信息类别应包括如下元素：

1. 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；
2. 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。
	* + 1. 软件信息

软件信息包括如下字段：

1. 软件名称：软件的名称，用于标识和区分软件；
2. 软件版本：软件的版本编号；
3. 杂凑算法：对软件的制品进行完整性保护的杂凑算法名称；
4. 消息摘要：对软件的制品通过杂凑运算获取的摘要值；
5. 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，包括：

-integrator：集成商

-developer：开发商

-agent：代理商

-other：其他

* 1. 所属区域：软件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”；
	2. 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，本字段为必选项；
1. 获取途径：获取开源软件的渠道，包括：

-codeHostingPlatform：代码托管平台

-thirdPartyDownloadSite：第三方下载站点

-openSourceCommunity：开源社区

1. 许可证名称：列出软件的许可证名称，许可证名称（及其简称）遵循ISO/IEC 5962-2021中关于许可证名称和缩略名的规定，如果许可证未在ISO/IEC 5962-2021中定义，可以自定义名称；清单中所列出的许可证名称，可在清单安全类别信息（见7.5节）中找到对应的许可证信息（见7.5.4节）。
2. 授权期限：软件授权使用的截止日期，日期格式为“YYYY-MM-DD”，如为永久有效，取值为 “permanent” 。

软件信息的各字段描述见表2。

1. 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 |
| 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 | 可选项 |
| supplierType | 供应商类型 | enum（of string） | 可选项 |
| area | 所属区域 | string | 可选项 |
| originalSuppliers | 原始供应商 | string | 条件必选 |
| acquisitionChannels | 获取途径 | enum（of string） | 可选项 |
| licenseName | 许可证名称 | string | 可选项 |
| licensingTerm | 授权期限 | string | 可选项 |

* + - 1. 清单信息

清单信息包括如下字段：

1. 清单格式名称：清单所采用格式标准的名称，固定值“SBOMDF”；
2. 格式版本：清单遵循的数据格式的版本，本文件对应版本号为“1.0”；
3. 清单标识：每个生成 的清单都应该有一个唯一的序列号，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；
4. 生命周期：此清单生成时，软件所处生命周期的阶段，包括：

-develop：开发阶段

-commit：交付阶段

-operation：运维阶段

-decommission:废止阶段

1. 时间戳：创建清单的日期和时间，格式为“YYYY-MM-DDTHH:mm:ssZ”；
2. 创建者：创建清单的实体名称；
3. 创建工具：创建清单的工具名称和版本；
4. 下载链接：获取清单的URL地址。

清单信息的各字段描述见表3。

1. 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 | enum（of 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 |

* + 1. 软件组成信息类别
			1. 类别概述

软件组成信息类别应包括如下元素：

1. 组件信息列表：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。
2. 内部依赖信息列表：描述组件、文件、代码片段之间依赖关系的信息。

可根据实际情况选择性包括如下元素：

1. 文件信息列表：软件的第一层解压和镜像加载的制品文件列表，包含文件名称、路径、用途、完整性校验等信息；
2. 代码片段信息列表：自研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。
	* + 1. 组件信息

组件信息包括如下字段：

1. 组件标识：组件在清单范围内的唯一标识符；
2. 组件名称：组件的名称，通常是组件的一个缩略名称，例如：“commons-lang3”；
3. 组件版本：组件的版本编号；
4. 组件描述：组件基本功能的详细描述；
5. 自研比例：组件中自研代码的占比，包括：

-all：全部自研组件

-part：部分自研组件

-none：外部组件

1. 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，例如：通用平台枚举（CPE）；
2. 重要性：组件对于保证软件正常运行的重要程度，例如：可以根据组件的是否支持核心业务功能判定组件为“关键组件”；
3. 安全度：描述组件的安全测评结果或安全等级信息，例如：开源组件经过社区安全审查情况、组件经过权威机构安全认证情况等；
4. 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，包括：

-integrator：集成商

-developer：开发商

-agent：代理商

-other：其他

* 1. 所属区域：组件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”，非开源组件应填写本字段；
	2. 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，本字段为必选项，非开源组件应填写本字段；
1. 获取途径：获取开源组件的渠道，包括

-codeHostingPlatform代码托管平台

-thirdPartyDownloadSite第三方下载站点

-openSourceCommunity开源社区

1. 组件编程语言：组件使用的编程语言列表；
2. 许可证名称：列出组件相关的许可证名称列表，许可证名称（及其简称）遵循ISO/IEC 5962-2021中关于许可证名称和缩略名的规定，如果许可证未在ISO/IEC 5962-2021中定义，可以自定义名称；
3. 下载链接：下载组件的URL地址；
4. 主页链接：查看组件信息的主页URL地址；
5. 构建完备性：构建和编译过程中依赖的其他组件识别信息的完整程度，包括：

-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

1. 杂凑算法：对组件进行完整性保护的杂凑算法名称
2. 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4。

1. 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 | enum（of string） | 必选项 |
| regIdentifer | 组件注册标识符 | string | 可选项 |

表4（续）

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 字段描述 | 字段类型 | 字段必要性 |
| importance | 重要性 | string | 可选项 |
| security | 安全度 | string | 可选项 |
| supplier | supplierName | 供应商 | string | 可选项 |
| supplierType | 供应商类型 | enum（of 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 | enum（of 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 | 构建完备性 | enum（of string） | 可选项 |
| integrity | hashAlg | 杂凑算法 | string | 必选项 |
| messageDigest | 消息摘要 | string | 必选项 |

* + - 1. 文件信息

文件信息包括如下字段：

1. 文件标识：文件在清单范围内的唯一标识符；
2. 文件名称：包含扩展名的完整文件名称；
3. 文件路径：文件在制品文件目录中的完整相对路径；
4. 用途描述：文件在软件中的功能和作用的简要说明；
5. 杂凑算法：对文件进行完整性保护的杂凑算法名称；
6. 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5。

1. 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 |

* + - 1. 代码片段信息

代码片段信息包括如下字段：

1. 片段标识：代码片段的在清单范围内的唯一标识符；
2. 关联文件：包含此代码片段的自研文件的路径和文件名；
3. 起点字节数：代码片段在自研源文件中的起始位置（按字节计算）；
4. 终点字节数：代码片段在自研源文件中的结束位置（按字节计算）；
5. 起点行数：代码片段在自研源文件中的起始位置（按行数计算）；
6. 终点行数：代码片段在自研源文件中的结束位置（按行数计算）；
7. 片段来源：代码片段所属开源项目名称；
8. 片段链接：代码片段所属开源项目的URL地址；
9. 许可证名称：列出代码片段相关的许可证名称，许可证名称（及其简称）遵循ISO/IEC 5962-2021中关于许可证名称和缩略名的规定，如果许可证未在ISO/IEC 5962-2021中定义，可以自定义名称；
10. 杂凑算法：对代码片段进行完整性保护的杂凑算法名称；
11. 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6。

1. 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 |
| snippetUrl | 片段链接 | 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 |

* + - 1. 内部依赖信息

内部依赖信息包括如下字段：

1. 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清单内的标识符；
2. 关系：描述关系类型，包括：

-dependsOn：依赖

-contain：包含

-other：其他

1. 被依赖标识：描述被依赖的组件、文件或代码片段实体在本清单内的标识符。

内部依赖信息的各字段描述见表7。

1. 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 | array of string | 必选项 |
| identityBId | 被依赖标识 | string | 必选项 |

* + 1. 外部依赖信息类别
			1. 类别概述

外部依赖信息类别可根据实际情况选择性的包括如下元素：

1. 外部网络服务信息列表：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；
2. 基础环境信息列表：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；
3. 开发工具信息列表：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。
	* + 1. 外部网络服务信息

外部网络服务包括如下字段：

1. 服务标识：外部网络服务在清单范围内的唯一标识符；
2. 服务名称：外部网络服务的中英文名称；
3. 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

1. 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”，本字段为必选项；
2. 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；
3. 服务地址：服务端的URL地址，如果可替代性取值为“false”，本字段为必选项；
4. 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”，本字段为必选项，包括：

-domestic：国内计算环境

-overseas：国外计算环境

1. 服务协议：服务使用的网络应用协议的名称，例如：HTTP、SMTP、DNS等；
2. 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8。

1. 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 | enum（of string） | 条件必选 |
| serviceProtocol | 服务协议 | string | 可选项 |
| dataDescription | 数据描述 | string | 可选项 |

* + - 1. 基础环境信息

基础环境信息包括如下字段：

1. 基础环境标识：基础环境软件在清单范围内的唯一标识符；
2. 基础环境名称：可用于识别基础环境软件的名称；
3. 基础环境版本：基础环境软件的版本编号；
4. 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

1. 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”，本字段为必选项；
2. 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。

基础环境信息的各字段描述见表9。

1. 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 |
| supplierName | 供应商 | string | 条件必选 |
| area | 所属区域 | string | 条件必选 |

* + - 1. 开发工具信息

开发工具信息包括如下字段：

1. 工具标识：开发工具在清单范围内的唯一标识符；
2. 工具名称：开发工具的名称；
3. 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；
4. 工具版本：开发工具的版本编号；
5. 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10。

1. 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 |

* + 1. 安全信息类别
			1. 类别概述

安全信息类别应包括如下元素：

1. 生命周期维护中断风险列表：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。

可根据实际情况选择性包括如下元素：

1. 网络服务接口信息列表：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；
2. 补丁信息列表：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；
3. 许可证信息列表：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；
4. 安全漏洞列表：生成清单之前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；
5. 配置风险列表：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。
	* + 1. 网络服务接口信息

网络服务接口信息包括如下字段：

1. 接口标识：接口在清单范围内的唯一标识符；
2. 接口类型：接口的类型，例如：Restful、RPC等；
3. 接口描述：描述接口调用方法和具体功能的信息；
4. 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

1. 请求方式：接口的请求方式，例如：GET、POST、HEAD等，接口类型为“Restful”时，此字段为必选项；
2. 接口地址：接口访问URL地址，可以有一个或多个接口地址，接口类型为“Restful”时，此字段为必选项；
3. 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，此字段为必选项。

网络服务接口信息的各字段描述见表11。

1. 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 |

* + - 1. 补丁信息

补丁信息包括如下字段：

1. 补丁标识：补丁在清单范围内的唯一标识符；
2. 补丁名称：可用于识别补丁的名称；
3. 发布日期：公开发布补丁的日期，日期格式为“YYYY-MM-DD”；
4. 原厂标识：软件原始供应商维护的补丁唯一标识符；
5. 补丁地址：下载补丁的URL地址；
6. 用途描述：补丁更新内容等说明信息；
7. 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12。

1. 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 |
| 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 |

表12（续）

|  |  |  |  |
| --- | --- | --- | --- |
| 字段名 | 字段描述 | 字段类型 | 字段必要性 |
| purpose | 用途描述 | string | 可选项 |
| patchSbom | 补丁清单文件 | string | 可选项 |

* + - 1. 许可证信息

许可证信息包括如下字段：

1. 许可证标识：许可证在软件物料清单范围内的唯一标识符；
2. 许可证名称：软件、组件、文件使用的许可证名称，许可证名称应与软件信息、组件信息、文件信息中的licenseName字段值一一对应；
3. 下载链接：获取许可证信息的URL地址；
4. 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；
5. 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；
6. 到期日期：商用许可证有效期最后一天的日期，日期格式为“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；
7. 条款约束：使用者的权利和义务的详细描述；
8. 适用范围：许可证适用地理区域范围，例如：“全球”；
9. 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

1. 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13。

1. 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 | 可选项 |
| patent | 专利权 | boolean | 可选项 |
| riskDescription | 风险描述 | string | 可选项 |

* + - 1. 安全漏洞

安全漏洞包括如下字段：

1. 漏洞标识：漏洞在清单范围内的唯一标识符；
2. 漏洞名称：漏洞信息的概括性描述；
3. 影响对象：存在漏洞的组件在清单范围内的标识符；
4. 相关编号：漏洞发布平台提供的漏洞编号，例如：“CNVD-2023-27109”,可以有多个相关编号；
5. 修复情况：修复组件漏洞采取的措施说明，包括：

-code level：代码级修复

-patch repair:使用补丁修复

-other：其他缓解措施

安全漏洞的各字段描述见表14。

1. 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 |
| repairSituation | 修复情况 | string | 必选项 |

* + - 1. 配置风险

配置风险包括如下字段：

1. 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；
2. 配置风险名称：描述配置风险的简短的中文名称；
3. 配置项：存在安全风险的配置项及其默认取值的描述；
4. 处置建议：配置风险处置建议的描述；
5. 检测工具：推荐的配置风险检测工具名称；
6. 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15。

1. 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 |

* + - 1. 生命周期维护中断风险

生命周期维护中断风险包括如下字段：

1. 中断标识：中断风险的在清单范围内的唯一标识符；
2. 中断类型：说明引起中断的具体原因，包括：

-authorization expires：证书授权到期

-not updated：长期未更新

-stop updating：停止更新

- single source：有且只有唯一高风险供应商

-others：其他

1. 影响对象：受中断风险影响的组件、外部网络服务、基础环境在清单范围内的标识；
2. 风险描述：中断风险的详细说明；
3. 预计中断时间：可能发生中断事件的具体时间，格式为“YYYY-MM-DDTHH:mm:ssZ”；
4. 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16。

1. 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 |

* + 1. 扩展信息类别
			1. 类别概述

扩展信息类别可根据实际情况选择性的包括本文件中未定义的其他物料信息列表，包括扩展信息的属性名称和属性值。

* + - 1. 扩展信息

扩展信息包括如下字段：

1. 属性名称：自定义的属性名称；
2. 属性值：属性的具体取值。

扩展信息的各字段描述见表17。

1. 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 |

* + 1. 签名信息类别
			1. 类别概述

安全信息类别应包括软件物料清单的签名信息，对清单所有内容的进行数字签名，并提供签名文件和数字证书文件信息。

* + - 1. 签名信息

签名信息包括如下字段：

1. 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；
2. 数字证书文件：保存用于验签的数字证书的文件名称。

签名信息的各字段描述见表18。

1. 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）
软件物料清单必要字段

软件物料清单必要字段如表A.1所示。

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 |
| 清单信息document | formatName | 清单格式名称 | string |
| formatVersion | 格式版本 | string |
| serialNumber | 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 |
| selfDevelopedProportion | 自研比例 | enum（of 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 | 依赖标识引用 | string |
| relationship | 关系 | array of string |
| identityBId | 被依赖标识引用 | string |
| 生命周期维护中断风险disruptions | disruptionId | 中断标识 | string |
| disruptionType | 中断类型 | string |
| affectedObject | 影响对象 | string |

表A.1（续）

|  |  |  |  |
| --- | --- | --- | --- |
| 元素名 | 字段名 | 字段描述 | 字段类型 |
| 生命周期维护中断风险disruptions | description | 风险描述 | string |
| disposal | 处置情况 | boolean |
| estimatedTime | 预计中断时间 | 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：

1. 定制化开发或商业采购软件：

{

 "software": {

 "softwareName": "MyApp",

 "softwareVersion": "1.2.0",

 "integrity": {

 "hashAlg": "MD5",

 "messageDigest": "fc3aa394c8787e019eda27be38d65cdf"

 },

 "supplier": {

 "supplierName": "supplierA",

 "supplierType": "agent",

 "area": "China",

 "developer": "developerA",

 }

 "licenseName":"Commercial Agreement A"

 "authorizationTerm": "2024-11-11"

 }

}

1. 开源软件：

{

 "software": {

 "softwareName": "MyApp",

 "softwareVersion": "1.2.0",

 "integrity": {

 "hashAlg": "MD5",

 "messageDigest": "fc3aa394c8787e019eda27be38d65cdf"

 },

 "acquisitionChannel ": "openSourceCommunity",

 "licenseName":"Apache-2.0"

 }

}

B.2清单信息

JSON格式示例：

{

 "document": {

 "formatName": "SBOMDF",

 "formatVersion": "1.0",

 "serialNumber": "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：

1. 定制化开发或商业采购软件：

{

 "components": [

 {

 "componentId": "lib-001",

 "componentName": "Logging Library",

 "componentVersion": "v2.5",

 "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": "China",

 "developer": "developerA",

 }

 "language": "Java",

 "licenseName": " Commercial Agreement B",

 "downloadUrl": "https://logcorp.com/log-lib",

 "homePgaeUrl": "https://logcorp.com",

 "completeness": "known",

 "integrity": {

 "hashAlg": "MD5",

 "messageDigest": "d41d8cd98f00b204e9800998ecf8427e"

 }

 },

 ]

}

1. 开源软件：

{

 "components": [

 {

 "componentId": "lib-001",

 "componentName": "Logging Library",

 "componentVersion": "v2.5",

 "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",

 "acquisitionChannel ": "openSourceCommunity",

 "language": "Java",

 "licenseName": "Apache License 2.0",

 "downloadUrl": "https://logcorp.com/log-lib",

 "homePgae": "https://logcorp.com",

 "completeness": "known",

 "integrity": {

 "hashAlg": "MD5",

 "messageDigest": "d41d8cd98f00b204e9800998ecf8427e"

 }

 },

 ]

}

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": "MD5",

 "messageDigest": "03ac674216f3e15c761ee1a5e255f067"

 }

 },

 ]

}

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",

 "snippetUrl":"http://www.OpenSourceCommunity.org/projectA/homepage",

 "licenseName": "Apache License 2.0",

 "integrity": {

 "hashAlg": "MD5",

 "messageDigest": "a8a06469b6d584543e5619746e3d62d4"

 }

 },

 ]

}

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": "China",

 },

 "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": "v8.0",

"substitutability": false,

 "source": "https://java.com",

 "supplier": {

 "supplierName": "Java provider",

 "area": "China"

 },

 },

]

}

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": "v5.3",

 "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",

 "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

1. 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"

 },

 ]

}

1. 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."

 },

 ]

}

B.13安全漏洞

{

"vulnerabilities": [

 {

 "vulnerabilityId": "vul-001",

 "vulnerabilityName": "心脏滴血",

 "affectedObject": "lib-001",

 "number": [

 "CVE-2014-0160",

 "CNVD-2014-31337"

 ],

 "repairSituation": "code level",

 }

 ],

}

B.14配置风险

JSON格式示例：

{

 "configRisks": [

 {

 "configRiskId": "con-001",

 "configRiskName": "数据安全风险",

 " configRiskItem ": "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。",

 "testingTool": "ToolA",

 "relatedUrl": "https://configuration.risk.com"

 }

 ],

}

B.15生命周期维护中断风险

{

 "disruptionRisks": [

 {

 "disruptionId": "Drp-001",

 "disruptionType": "组件停止更新",

 "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",

"diposal": false,

 }

 ]

}

B.16签名信息

“signature”:{

 “signatureFile”:“Value.txt”

“digitalCertificateFile”:“certification.pem”,

}

参考文献

1. GB/T 28458—2020 信息安全技术 网络安全漏洞标识与描述规范
2. GB/T XXXX-2024 网络安全技术 软件供应链安全要求
3. ISO/IEC 5962—2021 Information technology—SPDX@ Specification V2.2.1
4. ISO/IEC 1970—2-2015 Information technology—Softwareasset management—Part 2:Software identification tag

