ICS 35.030
CCS L 80

# 中华人民共和国国家标准

GB/T XXXXX—XXXX

# 信息安全技术 软件产品开源代码安全评价方法

Information security technology -Evaluation method for open source code security of software products

(点击此处添加与国际标准一致性程度的标识)

（征求意见稿）

**在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。**

XXXX - XX - XX 发布　　XXXX - XX - XX 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 ..... III
1 范围 ..... 1
2 规范性引用文件 ..... 1
3 术语和定义 ..... 1
4 评价目标 ..... 1
5 评价指标 ..... 2
5.1 指标体系 ..... 2
5.2 开源代码来源 ..... 3
5.2.1 开源代码规模占比 ..... 3
5.2.2 开源代码编码语言 ..... 3
5.2.3 开源代码著作权人 ..... 3
5.2.4 开源代码贡献量 ..... 3
5.2.5 开源代码丰富度 ..... 3
5.2.6 开源社区安全管理 ..... 3
5.2.7 开源代码托管平台 ..... 3
5.2.8 开源代码下载平台 ..... 3
5.3 开源代码质量 ..... 3
5.3.1 开源代码漏洞率 ..... 3
5.3.2 开源代码漏洞严重性 ..... 3
5.3.3 开源代码漏洞影响程度 ..... 4
5.3.4 开源代码漏洞利用复杂度 ..... 4
5.3.5 开源代码漏洞修复率 ..... 4
5.3.6 开源代码版本更新情况 ..... 4
5.4 开源代码知识产权 ..... 4
5.4.1 开源许可证规范性 ..... 4
5.4.2 开源许可证互惠性 ..... 4
5.4.3 开源许可证兼容性 ..... 4
5.4.4 开源许可证专利情况 ..... 4
5.4.5 开源许可证适用范围 ..... 4
5.5 开源代码管理能力 ..... 4
5.5.1 开源代码物料清单 ..... 4
5.5.2 开源代码设计 ..... 4
5.5.3 开源代码生成 ..... 5
5.5.4 开源代码管理团队 ..... 5
6 评价方法 ..... 5
6.1 概述 ..... 5
6.1.1 评价流程 ..... 5
6.1.2 评价内容 ..... 5
6.2 开源代码来源评价方法 ..... 5

6.2.1 开源代码规模占比 ..... 5
6.2.2 开源代码编码语言 ..... 6
6.2.3 开源代码著作权人 ..... 6
6.2.4 开源代码贡献量 ..... 6
6.2.5 开源代码丰富度 ..... 7
6.2.6 开源社区安全管理 ..... 7
6.2.7 开源代码托管平台 ..... 7
6.2.8 开源代码下载平台 ..... 7
6.3 开源代码质量评价方法 ..... 8
6.3.1 开源代码漏洞率 ..... 8
6.3.2 开源代码漏洞严重性 ..... 8
6.3.3 开源代码漏洞影响程度 ..... 8
6.3.4 开源代码漏洞利用复杂度 ..... 9
6.3.5 开源代码漏洞修复率 ..... 9
6.3.6 开源代码版本更新情况 ..... 9
6.4 开源代码知识产权评价方法 ..... 9
6.4.1 开源许可证规范性 ..... 9
6.4.2 开源许可证互惠性 ..... 10
6.4.3 开源许可证兼容性 ..... 10
6.4.4 开源许可证专利情况 ..... 10
6.4.5 开源许可证适用范围 ..... 10
6.5 开源代码管理能力评价方法 ..... 10
6.5.1 开源代码物料清单 ..... 11
6.5.2 开源代码设计 ..... 11
6.5.3 开源代码生成 ..... 11
6.5.4 开源代码管理团队 ..... 11
6.6 评价结果 ..... 11
附录 A （资料性） 开源代码安全风险 ..... 13
参考文献 ..... 14

# 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。

本文件由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本文件起草单位：中国信息通信研究院、蚂蚁科技集团股份有限公司、华为技术有限公司、中兴通讯股份有限公司、深圳市腾讯计算机系统有限公司、奇安信网神信息技术（北京）股份有限公司、杭州默安科技有限公司、深圳开源互联网安全技术有限公司、中国移动通信集团有限公司、北京小米移动软件有限公司、北京京东尚科信息技术有限公司、北京金山云网络技术有限公司、北京火山引擎科技有限公司、北京天融信网络安全技术有限公司、恒安嘉新（北京）科技股份公司、启明星辰信息技术集团股份有限公司、用友网络科技股份有限公司、杭州安恒信息技术股份有限公司、北京知道创宇信息技术股份有限公司、长扬科技（北京）股份有限公司、星环信息科技（上海）股份有限公司、浙江大华技术股份有限公司、超聚变数字技术有限公司、北京百度网讯科技有限公司、美的集团股份有限公司、马上消费金融股份有限公司、泰康保险集团股份有限公司、阿里云计算有限公司、阿里巴巴（中国）有限公司、浪潮科学研究院、道普信息技术有限公司、成都卫士通信息产业股份有限公司、国网区块链科技（北京）有限公司、北京安普诺信息技术有限公司、中电科拟态安全技术有限公司、杭州孝道科技有限公司、北京珞安科技有限责任公司、深圳华大生命科学研究院、兴唐通信科技有限公司、墨菲未来科技（北京）有限公司、北京酷德啄木鸟信息技术有限公司、中国科学院软件研究所、中国信息安全测评中心、国家互联网应急中心、中国软件评测中心、国家信息技术安全研究中心、中国科学院信息工程研究所、浙江省电子信息产品检验研究院、中国电子信息产业集团有限公司第六研究所、博鼎实华（北京）技术有限公司、ABB（中国）有限公司、三六零科技集团有限公司、北京神州绿盟科技有限公司、西安交大捷普网络科技有限公司、深圳市能信安科技股份有限公司、深信服科技股份有限公司、腾讯云计算（北京）有限责任公司、联想（北京）有限公司、北京长亭未来科技有限公司、北京山石网科信息技术有限公司、广东云百科技有限公司、武汉安天信息技术有限责任公司、浪潮电子信息产业股份有限公司、北京智游网安科技有限公司、北京九章云极科技有限公司、麒麟软件有限公司等。

本标准主要起草人：栗蔚、郭雪、李晓明、吴江伟、程岩、白晓媛、高琨、崔锦国、张宇、项曙明、张晓波、黄超、郑剑锋、董国伟、黄永刚、沈锡镛、孟瑾、王颉、汪杰、武晓慧、马洁、陈长林、钱佳煜、李欣博、赵南、李新、李晓川、张志文、杨剑、李鹏超、张东升、吕留东、李豪、陈星、田丽丹、叶润国、周景平、万耀东、赵华、刘汪根、张剑青、惠静、郭建领、张亮亮、刘志强、安丙春、曾林青、方强、袁永春、韩明军、王会波、杨珂、子芽、侯大鹏、谢国苗、延鹏、蔡国瑜、郝高健、欧阳强斌、史明超、晏敏、王晓萌、吴倩、袁薇、刘楠、许丽丽、尹肖栋、王绍杰、董霁、王缀、张杰、刘军、何建锋、李德庆、赵振阳、武杨、刘俊、翟羽佳、陈芳毅、刘超、余丽娜、曹柱、韩云、李学峰、刘敏等。

# 信息安全技术 软件产品开源代码安全评价方法

## 1 范围

本文件给出了软件产品中的开源代码安全评价目标、评价指标体系和评价方法，评价指标体系涵盖开源代码来源、开源代码质量、开源代码知识产权和开源代码管理能力。

本文件适用于软件产品包含的开源代码安全评价工作，为各企事业单位对于软件产品中的开源代码进行安全性自评价提供参考，为第三方机构开展此类工作提供依据。

## 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

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、应用等技术服务时提供的计算机软件，表现形式为一组计算机代码、规程以及可能的相关文档和数据。

[来源：GB/T 36475—2018，3.1，有修改]

3.2

**开源代码** open source code

一种可以获取源代码的软件代码，其著作权人通过开源许可证将代码的复制、修改、再发布的权利向公众开放。

3.3

**开源许可证** open source license

一种具有法律效力的、允许用户自由使用、修改、复制或分发软件代码的授权条款格式合同或协议。

3.4

**开源社区** open source community

以开源代码的贡献者为主体，在开源代码贡献过程中形成的具有特定文化、组织结构、运行机制的共同体。

## 4 评价目标

当前开源代码被广泛应用在软件产品的同时，存在开源代码网络安全风险、知识产权风险和持续性风险（见附录A）。

软件产品包含的开源代码安全评价应达到以下目标：

a) 可控性：通过评价软件产品中开源代码编码语言、贡献量、丰富度等情况掌握开源代码来源，最大程度降低开源代码供应中断风险，保障软件产品包含的开源代码部分使用过程中能够持续使用开源代码。

b) 安全性：通过考察软件产品中开源代码安全漏洞率、版本更新等情况，最大程度降低开源安全事件发生的可能性，保障软件产品中开源代码安全性不遭到破坏。

c) 合规性：通过考察软件产品中开源代码开源许可证互惠性、兼容性等情况，最大程度降低开源许可证知识产权风险，保障软件产品中开源代码符合开源许可证相关要求。

d) 稳定性：通过考察软件产品中开源代码物料清单、开源代码管理团队等情况，应对开源代码管理能力不足，保障软件产品包含的开源代码的稳定运行。

## 5 评价指标

### 5.1 指标体系

针对软件产品中的开源代码部分，本文件从开源代码来源、开源代码质量、开源代码知识产权、开源代码管理能力四个维度设置安全评价指标体系，见表1。

**表 1 软件产品包含的开源代码安全评价指标体系**

| 一级指标 | 二级指标 |
|---|---|
| 开源代码来源 | 开源代码规模占比 |
| | 开源代码编码语言 |
| | 开源代码著作权人 |
| | 开源代码贡献量 |
| | 开源代码丰富度 |
| | 开源社区安全管理 |
| | 开源代码托管平台 |
| | 开源代码下载平台 |
| 开源代码质量 | 开源代码漏洞率 |
| | 开源代码漏洞严重性 |
| | 开源代码漏洞影响程度 |
| | 开源代码漏洞利用复杂度 |
| | 开源代码漏洞修复率 |
| | 开源代码版本更新情况 |
| 开源代码知识产权 | 开源许可证规范性 |
| | 开源许可证互惠性 |
| | 开源许可证兼容性 |
| | 开源许可证专利情况 |
| | 开源许可证适用范围 |
| 开源代码管理能力 | 开源代码物料清单 |
| | 开源代码设计 |

| | |
|---|---|
| | 开源代码生成 |
| | 开源代码管理团队 |

## 5.2 开源代码来源

### 5.2.1 开源代码规模占比

主要统计软件产品包含的各开源代码模块字节数在软件产品代码中所占比例。

### 5.2.2 开源代码编码语言

主要统计软件产品包含的开源代码模块所使用的编码语言种类及其所开发代码占软件产品的比例，并据此做出评价。

### 5.2.3 开源代码著作权人

主要统计软件产品所包含的各开源代码著作人基本信息，包括名称、所属国家或地区等，并据此做出评价。

### 5.2.4 开源代码贡献量

主要统计软件产品所包含的开源代码贡献量情况，包括但不限于：

a) 贡献者数量及基本信息，包括名称、所属国家或地区等，并据此做出评价；
b) 各开源代码贡献者贡献代码量及占比，并据此做出评价。

### 5.2.5 开源代码丰富度

主要统计软件产品所包含的开源代码在功能、性能等方面具有等同实现的其他代码（含开源或商业代码）情况，并据此做出评价。

### 5.2.6 开源社区安全管理

主要统计软件产品包含的开源代码所依赖的开源社区安全管理情况，包括但不限于：

a) 对于开源代码的安全扫描情况，并据此做出评价；
b) 对于开源代码的贡献管理，如签署开源贡献协议、具备代码审查机制、具备数字签名，并据此做出评价。

### 5.2.7 开源代码托管平台

主要统计软件产品包含的开源代码托管平台运营方基本信息，并据此做出评价。

### 5.2.8 开源代码下载平台

主要统计软件产品包含的开源代码下载平台运营方基本信息和开源代码下载平台对开源代码完整性具备保障情况，并据此做出评价。

## 5.3 开源代码质量

### 5.3.1 开源代码漏洞率

主要统计软件产品包含的开源代码模块原始漏洞数量和千行漏洞率情况，并据此做出评价。

### 5.3.2 开源代码漏洞严重性

主要统计软件产品包含的开源代码模块原始漏洞严重性，并据此做出评价，指标项可参考GB/T30279-2020中6.3.3要求。

#### 5.3.3 开源代码漏洞影响程度

主要统计软件产品包含的开源代码模块原始漏洞影响范围，并据此做出评价，指标项可参考GB/T30279-2020 6.2.2中影响程度要求。

#### 5.3.4 开源代码漏洞利用复杂度

主要统计软件产品包含的开源代码模块原始漏洞攻击复杂性，并据此做出评价，指标项可参考GB/T30279-2020 6.2.1中被利用性要求。

#### 5.3.5 开源代码漏洞修复率

主要统计软件产品中针对开源代码的漏洞修复率及修复时间，并据此做出评价。

#### 5.3.6 开源代码版本更新情况

主要统计软件产品包含的开源代码所用版本和最新版本情况，并据此做出评价。

### 5.4 开源代码知识产权

#### 5.4.1 开源许可证规范性

主要统计软件产品开源许可证规范性情况，包括但不限于：

a) 软件产品包含的开源代码相关许可证的规范性，评价内容涉及授权范围、授权条件、违约与授权终止、免责声明等；
b) 软件产品履行开源许可证规定的相关条款、义务情况。

#### 5.4.2 开源许可证互惠性

主要统计软件产品包含的开源代码是否存在互惠性开源许可证，对自由互惠的开源许可证进行识别和风险评估，判断自研代码与开源代码之间的合规使用情况。

#### 5.4.3 开源许可证兼容性

主要统计软件产品包含的开源许可证兼容性情况，判断开源代码之间的许可证合规使用情况。

#### 5.4.4 开源许可证专利情况

主要统计软件产品包含的开源代码涉及专利是否得到授予，并据此做出评价。

#### 5.4.5 开源许可证适用范围

主要统计软件产品包含的开源许可证的适用范围和出现纠纷时法律声明情况，并据此做出评价。

### 5.5 开源代码管理能力

#### 5.5.1 开源代码物料清单

主要统计软件产品包含的开源代码物料清单的完备性，包括建立和维护可追溯性的策略和程序，记录和保留开源代码的原始供应方、开源社区或开发贡献者等相关信息，并据此做出评价。

#### 5.5.2 开源代码设计

主要统计软件产品设计阶段开源代码使用部分设计文档的完备性，以及梳理开源代码兼容性、使用规范性情况，并据此做出评价。

#### 5.5.3 开源代码生成

主要统计软件产品程序的源代码编写完成后，在编译以及链接过程中对使用的开源代码采取的安全措施，包括配置检查，漏洞扫描等，达到代码生成安全。

#### 5.5.4 开源代码管理团队

主要统计软件产品中开源代码的管理团队完善程度，内容包括但不限于：

a) 建立管理团队对开源代码进行统一管控，并进行相应管理角色划分，并据此做出评价；
b) 建立开源代码管理人员白名单和退出机制，并据此做出评价。

## 6 评价方法

### 6.1 概述

#### 6.1.1 评价流程

评价流程主要包括评价准备、方案制定、现场实施、分析评估4个阶段：

a) 在评价准备阶段，评价实施方接收被评价单位提交的评价申请后，与被评价单位沟通所需的评价材料，包括拟提供的软件产品、材料和证据等，依据本文件中的评价体系审核被评价单位提供的评价材料是否满足条件，通过审核后，组建评价实施团队，根据需要可设置专家组；
b) 在方案制定阶段，评价实施方确定评价方法、程序和进度，形成评价方案；
c) 在现场实施阶段，评价实施方依据评价方案，结合被评价单位提供的评价材料逐项核查，必要时可要求被评价单位补充相关材料，双方对现场实施结果进行确认；
d) 在分析评估阶段，评价实施方依据现场实施情况对软件产品包含的开源代码部分进行具体评价和打分。

#### 6.1.2 评价内容

评价实施方依据国家相关规定，主要对软件产品中的开源代码来源、开源代码质量、开源代码知识产权和开源代码管理能力进行评价。

评价实施方在开展开源代码安全评价工作中应综合采用访谈、检查和测试等基本评价方法，以核实被评价单位所提供评价材料是否满足指标考查内容要求：

a) 访谈：评价实施方通过与被评价单位相关人员进行有针对性的交流以帮助理解、厘清或取得证据，访谈的对象为个人或团体，如技术团队负责人、核心技术工程师等；
b) 检查：评价实施方对被评价单位提供的相关材料进行观察、查验、分析以帮助理解、厘清或取得证据，检查的对象为制度、文档和记录，如必要的开源代码物料清单、技术设计文档、安全扫描报告、开源代码管理团队背景信息等；
c) 测试：评价实施方使用具备开源代码成分识别功能、漏洞检出功能和代码缺陷检出功能的方法/工具使测试对象产生特定的结果，并将运行结果与预期的结果进行比对。

### 6.2 开源代码来源评价方法

#### 6.2.1 开源代码规模占比

开源代码规模占比的评价方法如下：

a) 评价方法：
   1) 测试软件产品中未经改动的开源代码成分，形成开源代码成分测试报告；
   2) 检查软件产品是否包含开源代码，对软件产品包含的开源代码的名称、数量、规模大小及所占比例进行记录。
b) 预期结果：
   软件产品包含开源代码，名称、数量、规模大小及所占比例能被识别和记录。

### 6.2.2 开源代码编码语言

开源代码编码语言的评价方法如下：

a) 评价方法：
   1) 测试软件产品中未经改动的开源代码成分，形成开源代码成分测试报告；
   2) 检查测试报告中软件产品开源代码编码语言名称；
   3) 检查各类型编码语言对应的安装包下载量；
   4) 访谈软件研发相关研发人员获取软件产品研发常用编码语言信息；
   5) 判断编码语言是否为应用范围广、规范程度高、参与人数多的。
b) 预期结果：
   软件产品包含的开源代码编码语言使用应用范围广、规范程度高、参与人数多的占比为80%及以上。

### 6.2.3 开源代码著作权人

开源代码著作权人的评价方法如下：

a) 评价方法：
   1) 测试软件产品中未经改动的开源代码成分，形成开源代码成分测试报告；
   2) 检查测试报告中软件产品包含的开源代码所在托管地址著作权人的地址信息、所属组织信息；
   3) 检查软件产品开源代码是否受国际政治、战争、贸易管制、知识产权等一种或多种国际环境影响。
b) 预期结果：
   软件产品包含的开源代码不受国际政治、战争、贸易管制、知识产权等一种或多种国际环境影响的比例为60%及以上。

### 6.2.4 开源代码贡献量

开源代码贡献量的评价方法如下：

a) 评价方法：
   1) 测试软件产品中未经改动的开源代码成分，形成开源代码成分测试报告；
   2) 检查测试报告中软件产品开源代码所在托管平台地址贡献者信息；
   3) 检查贡献者的地址信息和所属组织信息；
   4) 软件产品包含的开源代码贡献者是否不受国际政治、战争、贸易管制、知识产权等一种或多种国际环境影响。
b) 预期结果：
   1) 软件产品使用的开源代码60%及以上具备不受国际政治、战争、贸易管制、知识产权等一种或多种国际环境影响的代码贡献者；

2) 不受国际政治、战争、贸易管制、知识产权等一种或多种国际环境影响的代码贡献者占比平均值超过30%。

### 6.2.5 开源代码丰富度

开源代码丰富度的评价方法如下：

a) 评价方法：
   1) 测试软件产品中未经改动的开源代码成分，形成开源代码成分测试报告；
   2) 检查软件产品开源代码是否存在不受国际政治、战争、贸易管制、知识产权等一种或多种国际环境影响的等同实现的代码。
b) 预期结果：
   软件产品包含的开源代码存在不受国际政治、战争、贸易管制、知识产权等一种或多种国际环境影响的等同实现的代码比例为60%及以上。

### 6.2.6 开源社区安全管理

开源社区安全管理的评价方法如下：

a) 评价方法：
   1） 测试软件产品中未经改动的开源代码成分，形成开源代码成分测试报告；
   2） 检查软件产品开源代码所在的开源社区声明文档是否定期发布安全问题；
   3） 检查软件产品开源代码所在的开源社区开源代码合并是否具备安全测试标记；
   4） 检查软件产品包含的开源代码所在的开源社区贡献规则文档，确认是否要求开源贡献者签署协议要求；
   5） 检查软件产品包含的开源代码所在的开源社区组织架构，确认是有人员进行代码审查；
   6） 检查软件产品直接引入和和间接依赖的开源代码所在的开源社区贡献代码，确认是否具备数字签名；
   7） 检查软件产品包含的开源代码所在的开源社区是否具备代码发布安全机制措施。
b) 预期结果：
   软件产品包含的开源代码形成的开源社区对于正式版本发布进行安全扫描比例和对代码发布安全机制措施比例均为60%及以上。

### 6.2.7 开源代码托管平台

开源代码托管平台的评价方法如下：

a) 评价方法：
   1) 测试软件产品中未经改动的开源代码成分，形成开源代码成分扫描报告；
   2) 检查软件产品包含的开源代码所在的代码托管平台运营方地址是否不受国际政治、战争、贸易管制、知识产权等一种或多种国际环境影响；
b) 预期结果：
   软件产品包含的开源代码托管平台运营方地址在不受国际政治、战争、贸易管制、知识产权等一种或多种国际环境影响的数量占比为60%及以上。

### 6.2.8 开源代码下载平台

开源代码下载平台的评价方法如下：

a) 评价方法：
   1) 测试软件产品中未经改动的开源代码成分，形成开源代码成分扫描报告；

2) 检查软件产品包含的开源代码下载运营方地址是否从不受国际政治、战争、贸易管制、知识产权等一种或多种国际环境影响；
3) 检查软件产品包含的开源代码哈希值和数字签名；
4) 检查开源代码官网地址哈希值和数字签名，与软件产品使用的开源代码进行比对；
5) 检查软件产品使用的开源代码是否被篡改。

b) 预期结果：
1) 软件产品包含的开源代码地址下载运营方地址从不受国际政治、战争、贸易管制、知识产权等一种或多种国际环境影响的数量占比为80%及以上；
2) 软件产品包含的开源代码不被篡改。

## 6.3 开源代码质量评价方法

### 6.3.1 开源代码漏洞率

开源代码漏洞率的评价方法如下：

a) 评价方法：
1) 测试软件产品中未经改动的开源代码漏洞，形成漏洞扫描报告；
2) 检查软件产品包含的开源代码是否存在漏洞；
3) 检查千行漏洞率；
4) 检查有漏洞的开源代码中平均漏洞个数。

b) 预期结果：
1) 软件产品包含的开源代码存在漏洞的千行漏洞率为1.5及以下；
2) 软件产品有漏洞的开源代码中平均漏洞个数为1个。

### 6.3.2 开源代码漏洞严重性

开源代码漏洞严重性的评价方法如下：

a) 评价方法：
1) 测试软件产品中未经改动的开源代码漏洞，形成漏洞扫描报告；
2) 对被利用性指标进行赋值，根据赋值结果，参考GB/T30279-2020附录A计算得出漏洞被利用性分级；
3) 对影响程度指标进行赋值，根据赋值结果，参考GB/T30279-2020附录B得到影响程度分级；
4) 根据被利用性和影响程度分级的结果，参考GB/T30279-2020附录D，计算得到安全漏洞分级结果；
5) 检查软件产品包含的开源代码是否存在中危及以上漏洞。

b) 预期结果：
软件产品包含的开源代码无中危及以上漏洞。

### 6.3.3 开源代码漏洞影响程度

开源代码漏洞影响程度的评价方法如下：

a) 评价方法：
1) 测试软件产品中未经改动的开源代码漏洞，形成漏洞扫描报告；
2) 检查软件产品包含的开源代码保密性影响，即漏洞对受影响实体承载信息的保密性的影响程度，判断赋值是否为严重；
3) 检查软件产品包含的开源代码完整性影响，即漏洞对受影响实体承载信息的完整性的影响程度，判断赋值是否为严重；

4) 检查软件产品包含的开源代码可用性影响，即漏洞对受影响实体承载信息的可用性的影响程度，判断赋值是否为严重；
5) 检查结果中软件产品开源代码漏洞是否存在保密性、完整性、可用性两项及以上等级为严重的漏洞。

b) 预期结果：
软件产品包含的开源代码保密性、完整性、可用性无两项及以上等级为严重的漏洞。

#### 6.3.4 开源代码漏洞利用复杂度

开源代码漏洞利用复杂度的评价方法如下：

a) 评价方法：
1) 测试软件产品中未经改动的开源代码漏洞，形成漏洞扫描报告；
2) 检查软件产品包含的开源代码漏洞访问路径为网络、邻接、本地还是物理；
3) 检查软件产品包含的开源代码漏洞触发要求为低还是高；
4) 检查软件产品包含的开源代码漏洞权限需求为无、低还是高；
5) 检查软件产品包含的开源代码漏洞交互条件为不需要还是需要；
6) 根据访问路径、触发要求、权限需求和交互条件分级的结果，参考GB/T30279-2020附录A，计算得到安全漏洞攻击复杂度结果；
7) 检查结果中软件产品包含的开源代码漏洞是否存在漏洞利用复杂度等级为较低及中危。

b) 预期结果：
软件产品包含的开源代码漏洞利用复杂度等级无较低及中危。

#### 6.3.5 开源代码漏洞修复率

开源代码漏洞修复率的评价方法如下：

a) 评价方法：
1) 检查软件产品包含的开源代码漏洞修复记录的时间；
2) 检查漏洞出现正式编号的时间；
3) 检查修复记录中是否存在中高危漏洞出现3个月内未修复情况。

b) 预期结果：
软件产品在开源代码高危漏洞出现3个月内修复漏洞比例为80%及以上。

#### 6.3.6 开源代码版本更新情况

开源代码版本更新情况的评价方法如下：

a) 评价方法：
1) 测试软件产品中未经改动的开源代码成分，形成开源代码成分扫描报告；
2) 检查扫描结果中软件产品包含的开源代码当前版本时间；
3) 检查扫描中软件产品包含的开源代码最新版本时间；
4) 检查软件产品包含的开源代码是否为3年内发布较新稳定版本。

b) 预期结果：
软件产品包含的开源代码均为3年内发布较新稳定版本。

注：开源代码版本更新时间指标项中活跃社区3年内未发布新版本，可使用最新稳定版本。

### 6.4 开源代码知识产权评价方法

#### 6.4.1 开源许可证规范性

开源许可证规范性的评价方法如下：

a) 评价方法：
   1) 测试软件产品中未经改动的开源代码成分，形成开源代码成分扫描报告；
   2) 检查扫描结果中软件产品开源代码包含的开源许可证完整性；
   3) 检查扫描结果中软件产品开源代码包含的开源许可证是否全部为编写规范的开源许可证。
b) 预期结果：
   软件产品开源代码包含的开源许可证全部为规范使用，且全部为编写规范的开源许可证。

### 6.4.2 开源许可证互惠性

开源许可证互惠性的评价方法如下：

a) 评价方法：
   1) 测试软件产品中未经改动的开源代码成分，形成开源代码成分扫描报告；
   2) 检查扫描结果中软件产品包含的开源代码使用的弱互惠性开源许可证是否通过弱隔离方式引入，如静态链接和动态链接等；
   3) 检查扫描结果中软件产品包含的开源代码使用的强互惠性开源许可证是否通过强隔离方式引入，如聚合体。
b) 预期结果：
   软件产品开源代码包含的开源许可证若使用互惠性开源许可证，应全部合规使用。

### 6.4.3 开源许可证兼容性

开源许可证兼容性的评价方法如下：

a) 评价方法：
   1) 测试软件产品中未经改动的开源代码成分，形成开源代码成分扫描报告；
   2) 检查扫描结果中软件产品包含的开源代码使用的开源许可证之间是否兼容。
b) 预期结果：
   软件产品开源代码包含的开源许可证之间全部满足兼容性要求。

### 6.4.4 开源许可证专利情况

开源许可证专利情况的评价方法如下：

a) 评价方法：
   1) 测试软件产品中未经改动的开源代码成分，形成开源代码成分扫描报告；
   2) 检查扫描结果中软件产品包含的开源代码使用的开源许可证是否全部有明确专利授予。
b) 预期结果：
   软件产品开源代码包含的开源许可证未有明确专利权授予比例为20%及以下。

### 6.4.5 开源许可证适用范围

开源许可证适用范围的评价方法如下：

a) 评价方法：
   1) 测试软件产品中未经改动的开源代码成分，形成开源代码成分扫描报告；
   2) 检查扫描结果中软件产品包含的开源代码使用的开源许可证适用范围是否为全球。
b) 预期结果：
   软件产品开源代码包含的开源许可证适用范围为全球。

## 6.5 开源代码管理能力评价方法

### 6.5.1 开源代码物料清单

开源代码物料清单的评价方法如下：

a) 评价方法：
   1) 检查软件产品是否具备开源代码物料清单，物料清单应包括物料清单信息、直接引入的开源代码基本信息、间接依赖的开源代码基本信息和相关说明材料；
   2) 检查软件产品包含的开源代码物料清单是否具备可追溯性。
b) 预期结果：
   软件产品包含的开源代码存在规范的物料清单，开源代码信息有记录、可追溯。

### 6.5.2 开源代码设计

开源代码设计的评价方法如下：

a) 评价方法：
   1) 检查软件产品是否具备开源代码部分的设计文档；
   2) 检查软件产品包含的开源代码是否与运行环境兼容；
   3) 检查软件产品包含的开源代码是否具备外包接口兼容和版本接口兼容；
   4) 检查软件产品包含的开源代码是否具备外部数据兼容和版本数据兼容；
   5) 检查软件产品包含的开源代码使用是否具备代码、数据和注释的规范性。
b) 预期结果：
   软件产品包含的开源代码未出现与其他代码产生兼容性冲突、使用不规范情况。

### 6.5.3 开源代码生成

开源代码生成的评价方法如下：

a) 评价方法：
   1) 检查软件产品在生成阶段是否具备开源代码部分的安全扫描报告；
   2) 检查软件产品包含的开源代码安全扫描策略配置是否合理。
b) 预期结果：
   软件产品包含的开源代码生成均经过安全检查，安全扫描策略配置合理。

### 6.5.4 开源代码管理团队

开源代码管理团队评价方法如下：

a) 评价方法：
   1) 检查组织架构图，确认软件产品是否具备开源代码管理团队；
   2) 检查软件产品开源代码管理团队是否具备明确角色划分；
   3) 访谈软件产品团队人员获取人员从业经历情况，确认是否符合项目管理要求。
b) 预期结果：
   1) 具备完善的软件产品开源代码管理团队；
   2) 人员分工清晰；
   3) 从业人员符合项目管理要求。

## 6.6 评价结果

被评价单位结合所属行业和企业规模大小实际情况，依据评价体系及评价细则确认软件产品包含的开源代码安全性：

a) 对于重点行业软件产品，至少按照本文件各指标项要求确认软件产品包含的开源代码安全性，开源代码来源、开源代码质量、开源代码知识产权、开源代码管理能力均达到较高水平；
b) 对于其他软件产品应根据自身情况酌情进行开源代码安全评价，满足核心系统持续稳定使用需求。

# 附录 A
（资料性）
开源代码安全风险

## A.1 开源网络安全风险

开源网络安全风险大致分为开源代码漏洞风险、开源代码缺陷风险两大类。

a）开源代码漏洞风险是指由于源代码公开，资产直接暴露在互联网，在开源代码出现漏洞时容易被黑客读取，降低黑客攻击门槛导致代码安全性受到挑战。

b）开源代码缺陷风险是指开源具备广泛协作特性，若开源代码贡献者本身的技术能力和安全开发知识存在问题，将导致提交的开源代码存在代码缺陷。

## A.2 开源知识产权风险

开源知识产权风险大致分为版权侵权风险、专利侵权风险、商标侵权风险和许可证冲突四类。

a）版权侵权由于不遵守开源许可协议造成，此类风险较易规避。

b）专利侵权由于开源代码中包含诸多软件专利，使用开源代码未得到软件专利权人的专利许可，从而导致专利侵权，此类风险较难规避。

c）商标侵权由于未经许可使用开源代码的商标造成，此类风险较易规避。

d）许可证冲突由于未遵守许可证的兼容性要求造成，此类风险较难规避。

## A.3 开源持续性风险

开源持续性风险是指开源代码能否持续使用的风险。开源会因自然等不可抗力、政治、外交、国际经贸等原因造成使用中断。

## 参考文献

[1] GB/T 36475—2018 软件产品分类

[2] GB/T 30279—2020 信息安全技术 网络安全漏洞分类分级指南