SCA知识库总体技术要求

XXXX - XX - XX发布

XXXX - XX - XX实施

团体标准

T/ISC XXXX—XXXX

|  |
| --- |
|  |

中 国 互 联 网 协 会 发布

ICS

|  |
| --- |
|  |
| （征求意见稿） |

L

目  次

[前  言 II](#_Toc126585726)

[引 言 III](#_Toc126585727)

[1 范围 1](#_Toc126585728)

[2 规范性引用文件 1](#_Toc126585729)

[3 术语和定义 1](#_Toc126585730)

[3.1 1](#_Toc126585731)

[术语名称1　项目 1](#_Toc126585732)

[3.2 1](#_Toc126585733)

[术语名称2　组件 1](#_Toc126585734)

[3.3 1](#_Toc126585735)

[术语名称3　SCA 1](#_Toc126585736)

[3.4 1](#_Toc126585737)

[术语名称4　知识库 1](#_Toc126585738)

[4 SCA知识库总体技术要求 1](#_Toc126585739)

[4.1 总体要求 1](#_Toc126585740)

[4.2 知识库内容 2](#_Toc126585741)

[4.3 知识库存储、修改与更新 3](#_Toc126585742)

[附 录 A （资料性附录） 常见公开漏洞库 4](#_Toc126585743)

[附 录 B （资料性附录） 漏洞分析结果字段参考 4](#_Toc126585744)

前  言

本标准按照GB/T 1.1-2009给出的规则起草。

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这些专利的责任。

本标准由中国互联网协会归口。

本标准主要起草单位：中国信息通信研究院 上海安势信息技术有限公司

本标准主要起草人：……

引 言

（可无此部分）

SCA知识库总体技术要求

1. 范围

本标准提出了/规定了/给出了SCA知识库系统设计的总体技术要求

本标准适用于SCA知识库系统的设计、应用和评价

1. 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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。

《信息安全技术　数据库扫描产品安全技术要求》（GA/T 1139-2014）

1. 术语和定义

下列术语和定义适用于本文件。



术语名称1　项目

包含开源代码或开源软件的开源项目。



术语名称2　组件

开源项目内具有独立的工作逻辑的功能模块。



术语名称3　SCA

软件组件分析



术语名称4　知识库

知识库是用于知识管理的一种特殊的数据库,以便于有关领域知识的采集、整理以及提取。

1. SCA知识库总体技术要求
   1. 总体要求

SCA数据库应满足如下功能和性能要求：

a）知识库内容需全面准确

b）知识库需提供存储、更新与修改能力

c）具备写入、 存储、 查询、 管理数据的基本功能；

d）具备与主流外围软硬件系统；

e）具备一定的管理能力， 包括安装部署能力、 配置管理能力及实时监控能力、 用户管

理能力、在线升级能力、 元数据查看以及导入导出能力。

f）应具备容错能力， 以确保在发生故障时， 不会影响到业务的运行， 故障包括但不限

于硬件故障、 操作系统故障、 数据库服务故障；

g）具备过载保护能力以及数据多副本能力；

h）具备扩展性， 包括集群的在线扩容能力和缩容能力；

i）具备安全性， 保证数据在传输和使用过程中的安全， 包括对用户进行身份认证的能

力、 操作审计能力以及加解密能力；

j）具备较高的性能， 需要考察写入性能、 查询性能、 数据导入性能及数据压缩能力。

* 1. 知识库内容
     1. 源代码库
        1. 代码来源

代码来源是否足够广，是否包含主流开源仓库/平台的开源源代码

* + - 1. 元数据齐全和完整性

单个项目元数据应齐全和完整。

1. 元数据颗粒度：项目级别、组件级别、文件级别、代码片段级别
2. 元数据完整和准确：

项目或社区活跃度：最近更新时间，最近commit数量，contributor数量、star数量、fork数量，PR数量，issue数，下载数，资源库大小，所属开源基金会等

组件级元数据：组件名称、描述、创建时间、版本、许可证、URL、拥有者、程序语言

文件级元数据：文件名称、URL、创建时间、最近更新时间、最近更新人

1. 元数据关联关系：父子关系、依赖信息、许可证信息、版权信息、额外的许可要求等
   * + 1. 数据准确性

原样获取和经过处理的数据均需与来源一致。

* + 1. 许可证库

a）来源是否齐全：业界主要开源软件的许可证

b）信息齐全：许可证SPDX简称、许可证全称、许可证原文URL、许可证原文文本、是否OSI认证、是否FSF认证、所属家族

c）许可证解读：权力、义务、约束条件

* + 1. 漏洞库

a）来源是否齐全：至少包含NVD、CNNVD、CNVD、CVE和GitHub Advisory漏洞库。（更广泛的漏洞来源参见附录A）

b）漏洞时效性：是否在漏洞被发现第一时间能收录

c）漏洞关联的准确性：是否能识别到所有受影响的版本

d）漏洞关联的颗粒度：关联到项目级别、组件级别、文件级别、函数级别、代码片段级别

e）漏洞分析：至少包含解决建议（修复或规避建议）、漏洞分级、影响范围。（体现更强漏洞分析能力的指标参见附录B）

* + 1. 加密算法库

1. 来源是否齐全：是否包含业界各常用加密算法，尤其是非标准加密算法
2. 加密算法特征库：针对具体某个加密算法，其特征库是否涵盖各主流编程语言的特征，不因编程语言不同而影响识别
3. 加密算法和组件关联关系：是否能准确方便地识别到使用加密算法的组件/版本
4. 是否能区分标准加密算法和非标准加密算法
   1. 知识库存储、修改与更新
      1. 知识库的组织方式

以合理的组织方式存储或压缩，尽量减少知识库大小，方便存储、更新和检索，

数据格式方便转换，至少支持json、txt等目标格式。

* + 1. 更新能力

a）更新能力：出现新的组件和漏洞等知识数据，需要及时更新

b）更新方式：支持在线更新（不影响软件正常运行），离线更新

* + 1. 修改与定制化能力

知识库需提供接口供用户按照约定的格式进行内容修改与定制化

附 录 A  
（资料性附录）  
常见公开漏洞库

* NVD (National Vulnerability Database)
* CVE (Common Vulnerabilities and Exposures)
* CNNVD (国家信息安全漏洞库)
* CNVD (国家信息安全漏洞共享平台)
* GitHub Advisory Database
* GitLab Advisory Database
* OSV (Open Source Vulnerability)
* GSD (Global Security Database)

附 录 B  
（资料性附录）  
漏洞分析结果字段参考

* 漏洞原因分析
* 漏洞危害描述
* 漏洞分级
* 漏洞类型
* 影响范围（含影响软件及版本）
* 解决建议（修复或规避建议）
* 可利用的证明代码(PoC)
* 利用条件
* 利用成本
* 利用成熟度
* 处置优先级
* 漏洞可达性说明
* 参考链接

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_