国家信息安全漏洞库

CNNVD 漏洞兼容性描述规范

中国信息安全测评中心

二０一五年七月

目录

1. 范围

本标准规定了信息安全漏洞的兼容性描述格式规范。

本标准适用于用户、厂商和漏洞管理组织共享信息安全漏洞的数据。

2. 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，仅所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。

GB/T 28458-2012 信息安全技术 安全漏洞标识与描述规范

GB/T 30279-2013 信息安全技术 安全漏洞等级划分指南

GB/T 25069-2010 信息安全技术 术语

GB/T 15835-2011 出版物上数字用法的规定

《CNNVD 漏洞分类描述规范》

3. 术语和定义

GB/T 25069-2010 和 GB/T 28458-2012 中界定的以及下列术语和定义适用于本文件。

3.1 计算机信息系统 Computer Information System

由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

[GB/T25069-2010，定义 2.1.14]

3.2 安全漏洞 Vulnerability

计算机信息系统在需求、设计、实现、配置、运行等过程中，有意或无意产生的缺陷。这些缺陷以不同形式存在于计算机信息系统的各个层次和环节之中，一旦被恶意主体所利用，就会对计算机信息系统的安全造成损害，从而影响计算机信息系统的正常运行。

[GB/T 28458-2012，定义 3.2]

3.3 安全漏洞分类 Vulnerabilities Classification

安全漏洞分类是指按照安全漏洞的特征属性划分类别。

3.4 国家信息安全漏洞库 China National Vulnerability Database of Information Security

简称"CNNVD"，是中国信息安全测评中心为切实履行漏洞分析和风险评估的职能，负责建设运维的国家信息安全漏洞库，为我国信息安全保障提供基础服务。

3.5 可扩展标记语言 Extensible Markup Language

可扩展标记语言，标准通用标记语言的子集，英文缩写 XML。一种用于标记电子文件使其具有结构性的标记语言。

3.6 文档类型定义 DTD

用置标语言表达并为某个具体文档或一类文档定义内容模型和文档元素(包括控制元素内容与特性的规则)的一种特殊形式的文档定义

3.7 模式schema

一种以含有逻辑约束规则的式样为基础的结构化模式语言。

3.8 元素element

某个数据集内的一个具体数据项。

3.9 属性attribute

给一个具体元素实例添加信息或修改其信息的一个名称—值对。

3.10 属性列表attribute list

与一个具体文档元素相关联的一个或多个属性的集合。

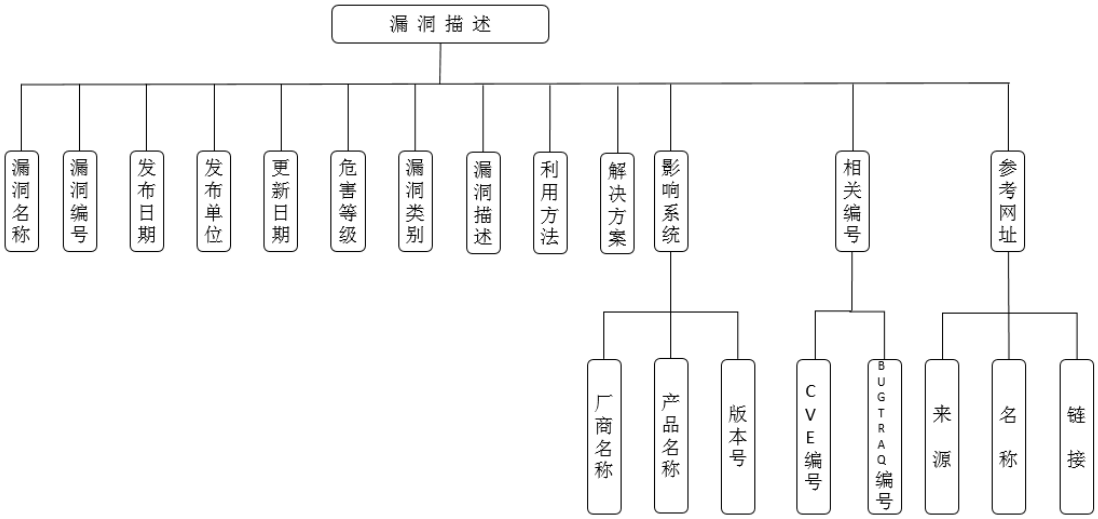
4. XML 描述

4.1 概述

采用可扩展标记语言（XML）对 CNNVD 漏洞兼容性描述规范进行描述。

4.2 描述项

CNNVD 漏洞兼容性描述规范的描述项包括漏洞名称、漏洞编号、发布时间、最后修改时间、危害等级、发布单位、漏洞类别、漏洞描述、相关编号、影响系统、利用方法、解决方案建议、其它描述等，结构模型如下所示：



4.3 描述

4.3.1 安全漏洞描述

XML 标记：CNNVD

定义：CNNVD 漏洞兼容性描述规范的 XML 根元素。

值域 :不作要求

Schema 定义：见表 1。

表 1 安全漏洞描述 Schema 定义

子元素	安全漏洞描述条目
属性列表	版本号、发布时间
命名空间	http://www.cnnvd.org/****
源代码	<xs:element name="cnnvd">

	<xs:complexType> <xs:sequence> <xs:element ref="entry" minOccurs="0" maxOccurs="unbounded"/> </xs:sequence> <xs:attribute name="cnnvd_xml_version" type="xs:NMTOKEN" use="required"> </xs:attribute> <xs:attribute name="pub_date" type="dateType" use="required"> </xs:attribute> </xs:complexType> </xs:element>

4.3.1.1 版本号

XML 标记：cnnvd_xml_version

定 义：记录基于 XML 的 CNNVD 漏洞兼容性描述规范的发布日期

值 域：XML Schema 的版本编号。

Schema 定义：见表 2。

表 2 版本号 Schema 定义

数据类型	xs:string
父元素	安全漏洞描述（CNNVD）
源代码	<xs:attribute name="cnnvd_xml_version" type="xs:NMTOKEN" use="required">

4.3.1.2 发布日期

XML 标记：pub_date

定 义：基于 XML 的 CNNVD 漏洞兼容性描述规范的发布日期

值 域：。遵循 GB/T7408-2005 中 5.2.1.1 完全表示法的扩展格式。

Schema 定义：见表 3。

表 3 发布日期 Schema 定义

数据类型	xs:string

父元素	安全漏洞描述（CNNVD）
源代码	<xs:attribute name="pub_date" type="dateType" use="required">

4.3.2 安全漏洞描述条目

XML 标记：entry

定义：漏洞描述条目，每个漏洞信息从 entry 开始。

值 域 :不做要求。

Schema 定义：见表 4。

表 4 漏洞描述条目 Schema 定义

子元素	漏洞名称、漏洞编号、发布日期、发布单位、更新日期、危害等级、漏洞类别、漏洞描述、利用方法、解决方案、影响系统、相关编号、参考网址
命名空间	http://www.cnnvd.org/****
源代码	<xs:element name="entry"> <xs:complexType> <xs:sequence> <xs:element ref="name"/> <xs:element ref="vuln-id"/> <xs:element ref="published"/> <xs:element ref="modified"/> <xs:element ref="source"/> <xs:element ref="severity"/> <xs:element ref="vuln-type"/> <xs:element ref=”vulnerable-configuration”> <xs:element ref="vuln-software-list"/> <xs:element ref="vuln-descript"/> <xs:element ref="vuln-exploit"/> <xs:element ref="other-id"/> <xs:element ref="vuln-solution"/> <xs:element ref="refs"/>

	</xs:sequence> </xs:complexType> </xs:element>

4.3.2.1 漏洞名称

XML 标记：name

定 义：漏洞的标题，概括性描述漏洞信息的短语。

值 域：不作要求。

Schema 定义：见表 5。

表 5 漏洞名称 Schema 定义

数据类型	xs:string
父元素	安全漏洞描述条目（entry）
源代码	<xs:element name="name" type="xs:string" use="required"/>

4.3.2.2 漏洞编号

XML 标记：vuln-id

定 义：漏洞编号。

值 域：遵循《漏洞标识与描述规范》定义，具体参见 GB/T 28458-2012 中 4.2.1 标识号。

Schema 定义：见表 6。

表 6 漏洞编号 Schema 定义

数据类型	xs:string
父元素	安全漏洞描述条目（entry）
源代码	<xs:element name="vuln-id" use="required"> <xs:restriction base="xs:string"> <xs:pattern value="(CNNVD)\-\d\d\d\d\\d\d-\d\d\d\d"/> </xs:restriction> </xs:element>

4.3.2.3 漏洞发布时间

XML 标记：published

定 义：漏洞信息发布日期。

值 域：遵循 GB/T7408-2005 中 5.2.1.1 完全表示法的扩展格式。

Schema 定义：见表 7。

表 7 漏洞发布时间 Schema 定义

数据类型	xs:string
父元素	安全漏洞描述条目（entry）
源代码	<xs:element name="published" use="required"> <xs:simpleType> <xs:restriction base="xs:string"> <xs:pattern value ="(19|20)\d\d-((01|03|05|07|08|10|12)-(0[1-9]|[1-2]\d|3[01])|(04|06|09|11)-(0[1-9]|[1-2]\d|30)|02-(0[1-9]|1\d|2\d))"/> </xs:restriction> </xs:simpleType> </xs:element>

4.3.2.4 漏洞更新时间

XML 标记：modified

定 义：漏洞信息更新日期。

值 域：遵循 GB/T7408-2005 中 5.2.1.1 完全表示法的扩展格式。

Schema 定义：见表 8。

表 8 漏洞更新时间 Schema 定义

数据类型	xs:string
父元素	安全漏洞描述条目（entry）
源代码	<xs:element name="modified"> <xs:simpleType>

	<xs:restriction base="xs:string"> <xs:pattern value ="(19|20)\d\d-((01|03|05|07|08|10|12)-(0[1-9]|[1-2]\d|3[01])|(04|06|09|11)-(0[1-9]|[1-2]\d|30)|02-(0[1-9]|1\d|2\d))"/> </xs:restriction> </xs:simpleType> </xs:element>

4.3.2.5 漏洞发布单位

XML 标记：source

定 义：发布漏洞的单位全称。

值 域：遵循《漏洞标识与描述规范》定义，具体参见 GB/T 28458-2012 中 4.2.4 漏洞发布单位。

Schema 定义：见表 9。

表 9 漏洞发布单位 Schema 定义

数据类型	xs:string
父元素	安全漏洞描述条目（entry）
源代码	<xs:element name="source" type="xs:string" minOccurs="0"/>

4.3.2.6 危害等级

XML 标记：severity

定 义：漏洞危害等级。

值 域：遵循《安全漏洞等级划分指南》定义，具体参见 GB/T 30279-2013。

Schema 定义：见表 10

表 10 危害等级 Schema 定义

数据类型	xs:string
父元素	安全漏洞描述条目（entry）
源代码	<xs:complexType name="severity"> <xs:sequence>

	<xs:simpleType> <xs:restriction base="xs:NMTOKEN"> <xs:enumeration value="超危"/> <xs:enumeration value="高危"/> <xs:enumeration value="中危"/> <xs:enumeration value="低危"/> </xs:restriction> </xs:simpleType> </xs:sequence> </xs:complexType>

4.3.2.7 漏洞类别

XML 标记：vuln-type

定 义：漏洞所属分类，说明漏洞分类归属的信息。

值 域：遵循《CNNVD 漏洞分类描述规范》定义。

Schema 定义：见表 11

表 11 漏洞类别 Schema 定义

数据类型	xs:string
父元素	安全漏洞描述条目（entry）
源代码	<xs:complexType name="vuln-type"> <xs:sequence> <xs:simpleType> <xs:restriction base="xs:NMTOKEN"> <xs:enumeration value="代码"/> <xs:enumeration value="源代码"/> <xs:enumeration value="数据处理"/> <xs:enumeration value="输入验证"/> <xs:enumeration value="命令注入"/> <xs:enumeration value="操作系统命令注入"/>

```
                    <xs:enumeration value=" SQL 注入"/>
                    <xs:enumeration value="跨站脚本"/>
                    <xs:enumeration value="代码注入"/>
                    <xs:enumeration value="路径等价"/>
                    <xs:enumeration value="路径遍历"/>
                    <xs:enumeration value="后置链接"/>
                    <xs:enumeration value="数字错误"/>
                    <xs:enumeration value="信息管理错误"/>
                    <xs:enumeration value="信息泄露"/>
                    <xs:enumeration value="资源管理错误"/>
                    <xs:enumeration value="缓冲区溢出"/>
                    <xs:enumeration value="格式化字符串"/>
                    <xs:enumeration value="注入"/>
                    <xs:enumeration value="竞争条件"/>
                    <xs:enumeration value="安全特征/功能"/>
                    <xs:enumeration value="跨站请求伪造"/>
                    <xs:enumeration value="未充分验证数据权限"/>
                    <xs:enumeration value="信任管理"/>
                    <xs:enumeration value="权限许可和访问控制"/>
                    <xs:enumeration value="授权问题"/>
                    <xs:enumeration value="加密问题"/>
                    <xs:enumeration value="访问控制错误"/>
                    <xs:enumeration value="配置错误"/>
                    <xs:enumeration value="资料不足"/>
                    <xs:enumeration value="其他"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:sequence>
    </xs:complexType>
```

4.3.2.8 影响实体描述

XML 标记：vulnerable-configuration

定 义：漏洞所影响实体的信息，包括厂商、产品名称和版本号等。

值 域：遵循《CNNVD 漏洞影响实体描述规范》定义。

Schema 定义：见表 12。

表 12 影响实体 Schema 定义

子元素	漏洞影响实体
父元素	安全漏洞描述条目（entry）
源代码	<xs:element name="vulnerable-configuration" maxOccurs="unbounded"> <xs:complexType> <xs:sequence> <xs:element ref="cncpe"/> </xs:sequence> </xs:complexType> </xs:element> <xsd:element name="cncpe"> <xs:complexType> <xsd:sequence> <xsd:element name="cncpe-software" type="cncpetype" minOccurs="0" maxOccurs="unbounded"/> <xsd:element name="cncpe-terrace" type="cncpetype " minOccurs="0" maxOccurs="unbounded"/> </xsd:sequence> <xsd:attribute name="operator" type="OperatorEnumeration" use="required"/> </xsd:complexType> </xs:element> <xsd:complexType name="cncpetype">

```
            <xsd:sequence>
                <xsd:element name="cncpe-lang" type="cncpe-lang-type"
minOccurs="0" maxOccurs="unbounded"/>
            </xsd:sequence>
            <xsd:attribute name="operator" type="OperatorEnumeration"
use="required"/>
</xsd:complexType>

<xsd:complexType name="cncpe-lang">
            <xsd:attribute name="name" type="namePattern" use="required"/>
</xsd:complexType>

<xsd:simpleType name="OperatorEnumeration">
            <xsd:restriction base="xsd:string">
                <xsd:enumeration value="AND"/>
                <xsd:enumeration value="OR"/>
            </xsd:restriction>
        </xsd:simpleType>

<xsd:simpleType name="namePattern">
    <xsd:restriction base="xsd:string">
            <xsd:pattern
value="cncpe:/([aho](:[A-Za-z0-9\._\-~]*(:[A-Za-z0-9\._\-~]*(:[A-Za-z0-9\._\.\-~]*(:[A-
Za-z0-9\._\-~]*)?)?)?)?)?"/>
    </xsd:restriction>
</xsd:simpleType>
```

4.3.2.9 影响产品描述

XML 标记：vuln-software-list

定 义：影响的产品信息。

值 域：遵循《CNNVD 漏洞影响实体描述规范》定义。

Schema 定义：见表 13

表 13 影响产品描述 Schema 定义

数据类型	xs:string
父元素	安全漏洞描述条目（entry）
源代码	<xs: element ref="product" type="xs:string" use="required"/>

4.3.2.10漏洞描述

XML 标记：vuln-descript

定 义：漏洞描述需要说明的相关信息，例如漏洞产生的具体原因。

值 域：不作要求。

Schema 定义：见表 13。

表 13 漏洞描述 Schema 定义

数据类型	xs:string
父元素	安全漏洞描述条目（entry）
源代码	<xs:element name="vuln-descript" type="xs:string" minOccurs="0"/>

4.3.2.11 利用方法

XML 标记：vuln- exploit

定 义：漏洞利用的方法，例如漏洞攻击方案或利用代码。

值 域：不作要求。

Schema 定义：见表 14。

表 14 利用方法 Schema 定义

数据类型	xs:string

父元素	安全漏洞描述条目（entry）
源代码	<xs:element name="vuln-exploit" type="xs:string" minOccurs="0"/>

4.3.2.12 相关编号

XML 标记：other-id

定 义：漏洞的其他相关编号，例如 Bugtraq 编号、CVE 编号等。

值 域：不作要求。

Schema 定义：见表 15。

表 15 相关编号 Schema 定义

子元素	CVE 编号、Bugtraq 编号
父元素	安全漏洞描述条目（entry）
源代码	<xs:element name="other-id" minOccurs="0"> <xs:complexType> <xs:sequence> <xs:element ref="cve-id"/> <xs:element ref="bugtraq-id"/> </xs:sequence> </xs:complexType> </xs:element>

4.3.2.12.1 CVE编号

XML 标记：cve-id

定 义：漏洞的 cve 编号。

值 域：不作要求。

Schema 定义：见表 16。

表 16 CVE 编号 Schema 定义

数据类型	xs:string
父元素	相关编号（other-id）
源代码	<xs:element name="cve-id" type="xs:string" minOccurs="0"/>

4.3.2.12.2 Bugtraq编号

XML 标记：bugtraq-id

定 义：漏洞的 Bugtraq 编号。

值 域：不作要求。

Schema 定义：见表 17。

表 17 Bugtraq 编号 Schema 定义

数据类型	xs:string
父元素	相关编号（other-id）
源代码	<xs:element name="bugtraq-id" type="xs:string" minOccurs="0"/>

4.3.2.13 解决方案

XML 标记：vuln- solution

定 义：漏洞的解决方案，例如补丁信息等。

值 域：不作要求。

Schema 定义：见表 18。

表 18 解决方案 Schema 定义

数据类型	xs:string
父元素	安全漏洞描述条目（entry））
源代码	<xs:element name="vuln- solution" type="xs:string" minOccurs="0"/>

4.3.2.14 参考网址

XML 标记：refs

定 义：漏洞信息相关网址。

值 域：不作要求。

Schema 定义：见表 19。

表 19 参考网址 Schema 定义

子元素	来源、名称、链接
父元素	安全漏洞描述条目（entry）

源代码	<xs:element name="refs" minOccurs="0" maxOccurs="unbounded"> <xs:complexType> <xs:sequence> <xs:element ref="ref-source"/> <xs:element ref="ref-name"/> <xs:element ref="ref-url"/> </xs:sequence> </xs:complexType> </xs:element>

4.3.2.14.1 来源

XML 标记：ref-source。

定 义：漏洞信息相关网站的网址。

值 域：不作要求。

Schema 定义：见表 20。

表 20 来源 Schema 定义

数据类型	xs:string
父元素	参考网址（refs）
源代码	<xs:element name="ref-source" type="xs:string" minOccurs="0"/>

4.3.2.14.2 名称

XML 标记：ref-name。

定 义：漏洞信息相关网站的名称。

值 域：不作要求。

Schema 定义：见表 21。

表 21 名称 Schema 定义

数据类型	xs:string
父元素	参考网址（refs）
源代码	<xs:element name="ref-name" type="xs:string" minOccurs="0"/>

4.3.2.14.3 链接

XML 标记：ref-url。

定 义：漏洞信息相关的网址。

值 域：不作要求。

Schema 定义：见表 22。

表 22 链接 Schema 定义

数据类型	xs:string
父元素	参考网址（refs）
源代码	<xs:element name="ref-url" type="xs:string" minOccurs="0"/>

5. Schema 定义

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://www.cnnvd.org/****" elementFormDefault="qualified"
attributeFormDefault="unqualified" version="1.0">
    <xs:element name="cnnvd">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="entry" minOccurs="0" maxOccurs="unbounded"/>
            </xs:sequence>
            <xs:attribute name="cnnvd_xml_version" type="xs:NMTOKEN"
use="required"/>
            <xs:attribute name="pub_date" type="dateType" use="required"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="entry">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="name"/>
                <xs:element ref="vuln-id"/>
                <xs:element ref="published"/>
                <xs:element ref="modified"/>
                <xs:element ref="source"/>
                <xs:element ref="severity"/>
                <xs:element ref="vuln_type"/>
                <xs:element ref="vuln-soft"/>
                <xs:element ref="vuln-descript"/>
                <xs:element ref="vuln-exploit"/>
```

```
                        <xs:element ref="other-id"/>
                        <xs:element ref="vuln-solution"/>
                        <xs:element ref="refs"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="name" type="xs:string" use="required"/>
            <xs:element name="vuln-id" use="required">
                <xs:restriction base="xs:string">
                    <xs:pattern value="(CNNVD)\-\d\d\d\d\\d\d-\d\d\d\d"/>
                </xs:restriction>
            </xs:element>
            <xs:element name="published" use="required">
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:pattern value
="(19|20)\d\d-((01|03|05|07|08|10|12)-(0[1-9]|[1-2]\d|3[01])|(04|06|09|11)-(0[1-9]|[1-2]\d|
30)|02-(0[1-9]|1\d|2\d))"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
            <xs:element name="modified">
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:pattern value
="(19|20)\d\d-((01|03|05|07|08|10|12)-(0[1-9]|[1-2]\d|3[01])|(04|06|09|11)-(0[1-9]|[1-2]\d|
30)|02-(0[1-9]|1\d|2\d))"/>
                    </xs:restriction>
                </xs:simpleType>
```

```
        </xs:element>
        <xs:element name="source" type="xs:string" minOccurs="0"/>
        <xs:complexType name="vulnSeverity">
            <xs:sequence>
                <xs:simpleType>
                    <xs:restriction base="xs:NMTOKEN">
                        <xs:enumeration value="超危"/>
                        <xs:enumeration value="高危"/>
                        <xs:enumeration value="中危"/>
                        <xs:enumeration value="低危"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:sequence>
        </xs:complexType>
    <xs:element name="vulnerable-configuration" maxOccurs="unbounded">
        <xs:complexType>
        <xs:sequence>
            <xs:element ref="cncpe"/>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
        <xsd:element name="cncpe">
            <xs:complexType>
                <xsd:sequence>
                    <xsd:element name="cncpe-software" type="cncpetype" minOccurs="0"
maxOccurs="unbounded"/>
                    <xsd:element name="cncpe-terrace" type="cncpetype " minOccurs="0"
maxOccurs="unbounded"/>
                </xsd:sequence>
```

```
                    <xsd:attribute name="operator" type="OperatorEnumeration"
use="required"/>
                </xsd:complexType>
            </xs:element>
        <xsd:complexType name="cncpetype">
                <xsd:sequence>
                    <xsd:element name="cncpe-lang" type="cncpe-lang-type" minOccurs="0"
maxOccurs="unbounded"/>
                </xsd:sequence>
                <xsd:attribute name="operator" type="OperatorEnumeration" use="required"/>
        </xsd:complexType>

        <xsd:complexType name="cncpe-lang">
                    <xsd:attribute name="name" type="namePattern" use="required"/>
        </xsd:complexType>

        <xsd:simpleType name="OperatorEnumeration">
                <xsd:restriction base="xsd:string">
                    <xsd:enumeration value="AND"/>
                    <xsd:enumeration value="OR"/>
                </xsd:restriction>
            </xsd:simpleType>

        <xsd:simpleType name="namePattern">
            <xsd:restriction base="xsd:string">
                <xsd:pattern
value="cncpe:/([aho](:[A-Za-z0-9\._\-~]*(:[A-Za-z0-9\._\-~]*(:[A-Za-z0-9\._\.\-~]*(:[A-Za-z0-9\._\-
~]*)?)?)?)?)?"/>
            </xsd:restriction>
```

```
    </xsd:simpleType>
        <xs:element name=" vuln-software-list" use="required" maxOccurs="unbounded">
            <xs:complexType>
                <xs:sequence>
                    <xs:element ref="product"/>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
        <xs:element ref="product" type="namePattern" minOccurs="0"
maxOccurs="unbounded"/>
        <xs:element name="vuln-descript" type="xs:string" minOccurs="0"/>
        <xs:element name="vuln-exploit" type="xs:string" minOccurs="0"/>
        <xs:element name="other-id" minOccurs="0">
            <xs:complexType>
                <xs:sequence>
                    <xs:element ref="cve-id"/>
                    <xs:element ref="bugtraq-id"/>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
        <xs:element ref="cve-id" type="xs:string" minOccurs="0"/>
        <xs:element name="bugtraq-id" type="xs:string" minOccurs="0"/>
        <xs:element name="vuln-solution" type="xs:string" minOccurs="0"/>
        <xs:element name="refs" minOccurs="0">
            <xs:complexType>
                <xs:sequence>
                    <xs:element ref="ref-source"/>
                    <xs:element ref="ref-name"/>
                    <xs:element ref="ref-url"/>
```

```
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="ref-source" type="xs:string" minOccurs="0"/>
    <xs:element name="ref-name" type="xs:string" minOccurs="0"/>
    <xs:element name="ref-url" type="xs:string" minOccurs="0"/>
    <xs:complexType name="vuln-type">
        <xs:sequence>
            <xs:simpleType>
                <xs:restriction base="xs:NMTOKEN">
                    <xs:enumeration value="代码"/>
                    <xs:enumeration value="源代码"/>
                    <xs:enumeration value="数据处理"/>
                    <xs:enumeration value="输入验证"/>
                    <xs:enumeration value="命令注入"/>
                    <xs:enumeration value="操作系统命令注入"/>
                    <xs:enumeration value=" SQL 注入"/>
                    <xs:enumeration value="跨站脚本"/>
                    <xs:enumeration value="代码注入"/>
                    <xs:enumeration value="路径等价"/>
                    <xs:enumeration value="路径遍历"/>
                    <xs:enumeration value="后置链接"/>
                    <xs:enumeration value="数字错误"/>
                    <xs:enumeration value="信息管理错误"/>
                    <xs:enumeration value="信息泄露"/>
                    <xs:enumeration value="资源管理错误"/>
                    <xs:enumeration value="缓冲区溢出"/>
                    <xs:enumeration value="格式化字符串"/>
                    <xs:enumeration value="注入"/>
```

```
                        <xs:enumeration value="竞争条件"/>
                        <xs:enumeration value="安全特征/功能"/>
                        <xs:enumeration value="跨站请求伪造"/>
                        <xs:enumeration value="未充分验证数据权限"/>
                        <xs:enumeration value="信任管理"/>
                        <xs:enumeration value="权限许可和访问控制"/>
                        <xs:enumeration value="授权问题"/>
                        <xs:enumeration value="加密问题"/>
                        <xs:enumeration value="访问控制错误"/>
                        <xs:enumeration value="配置错误"/>
                        <xs:enumeration value="资料不足"/>
                        <xs:enumeration value="其他"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:sequence>
        </xs:complexType>
    </xs:schema>
```

6. XML 示例

```
<?xml version="1.0" encoding="UTF-8"?>
    <cnnvd xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://www.cnnvd.org.cn/***"
    xsi:schemaLocation="http://www.cnnvd.org.cn/*** http://www.cnnvd.org.cn/***.xsd"
            cnnvd_xml_version="*.*" pub_date="****-**-**" >
        <entry>
            <name>Cherokee 授权问题漏洞 </name>
            <vuln-id>CNNVD-201407-063</vuln-id>
```

```
<published>2014-07-03</published>
<modified>2014-07-03</modified>
<source></source>
<severity>中危</severity>
<vuln-type>授权问题</vuln-type>
<vulnerable-configuration>
    <cncpe operator="AND">
        <cncpe-software operator="OR">
            < cncpe-lang name="cpe:/a:redhat:libvirt:1.2.0"/>
            < cncpe-lang name="cpe:/a:redhat:libvirt:1.2.1"/>
        </cncpe- software >
        <cncpe-terrace operator="OR">
            < cncpe -lang name="cpe:/o:novell:opensuse:13.2"/>
            < cncpe -lang name="cpe:/o:novell:opensuse:13.1"/>
        </ cncpe -terrace>
    </cncpe>
</vulnerable-configuration>
<vuln-software-list>
    <product>cpe:/a:redhat:libvirt:1.2.0></product>
    <product> cpe:/a:redhat:libvirt:1.2.1</product>
</vuln-software-list>
<vuln-descript>Cherokee 是一款 Web 服务器，它支持 HTTP 负载平衡、日志记录和 HTTP 反向代理等。Cherokee 1.2.103 及之前版本的 validator_ldap.c 文件中的‘cherokee_validator_ldap_check’函数存在安全漏洞，该漏洞源于程序使用 LDAP 时，没有正确处理空密码。远程攻击者可利用该漏洞绕过身份验证。
</vuln-descript>
<other-id>
    <cve-id>CVE-2014-4668</cve-id>
    <bugtraq-id></bugtraq-id>
```

```
            </other-id>
            <refs>
                <ref-source> MLIST </ref-source>
                <ref-name></ref-name>
                <ref-url>http://openwall.com/lists/oss-security/2014/06/28/7 </ref-url>
            </refs>
            <refs>
                <ref-source> MLIST </ref-source>
                <ref-name></ref-name>
                <ref-url>http://openwall.com/lists/oss-security/2014/06/28/3 </ref-url>
            </refs>
            <vuln-solution></vuln-solution>
        </entry>
        <entry>
        </entry>
    </cnnvd>
```

参 考 文 献

[1] NIST Special Publication 800-51, Use of Common Vulnerabilities and Exposures(CVE) Vulnerability Naming Scheme, http://csrc.nist.gov/publications/nistpubs/800-51/sp800-51.pdf

[2] National Vulnerability Database. http://nvd.nist.gov/