ICS 35.040
L80

中 华 人 民 共 和 国 国 家 标 准

GB/T XXXXX—XXXX

信息安全技术　安全漏洞标识与描述规范

Information security technology —— Vulnerability identification and description specification

（报批稿）

（本稿完成日期：2011.8.22）

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

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。

本标准由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本标准起草单位：国家信息技术安全研究中心、中国科学院研究生院国家计算机网络入侵防范中心。

本标准主要起草人：张玉清、宫亚峰、王宏、刘奇旭、付安民。

引　　言

随着计算机及互联网技术的发展，信息安全环境越来越复杂，信息安全隐患越来越严重。计算机信息系统安全漏洞已经成为影响网络信息安全的重要因素。为规范和加强计算机信息系统安全漏洞的管理，制定统一的安全漏洞标识与描述规范是十分必要的。

信息安全技术　安全漏洞标识与描述规范

1　范围

本标准规定了计算机信息系统安全漏洞的标识与描述规范。

本标准适用于计算机信息系统安全管理部门进行安全漏洞信息发布和漏洞库建设。

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 7408-2005　数据元和交换格式信息交换日期和时间表示法

GB 7713-1987　科学技术报告、学位论文和学术论文的编写格式

GB/T 15835-1995　出版物上数字用法的规定

GB/T 25069-2010　信息安全技术术语

3　术语和定义

GB/T 25069-2010界定的以及下列术语和定义适用于本标准。为了便于使用，以下重复列出了GB/T 25069-2010中的一些术语和定义。

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。[选自 GB/T25069-2010，定义 2.1.14]

3.2

安全漏洞 vulnerability

安全漏洞是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。

4　安全漏洞标识与描述

4.1　原则

本标准的制定遵循以下原则：

a) 简明原则：对安全漏洞信息进行筛选，提炼安全漏洞管理所需要的基本内容，保证安全漏洞描述简洁明确。

b) 客观原则：安全漏洞描述便于安全漏洞信息的发布和安全漏洞数据库的建设。

4.2 描述项

安全漏洞描述项如图1所示，包括标识号、名称、发布时间、发布单位、类别、等级、影响系统等必须的描述项（图1实线框描述项），并可根据需要扩充（但不限于）相关编号、利用方法、解决方案建议、其他描述等描述项（图1虚线框描述项）。

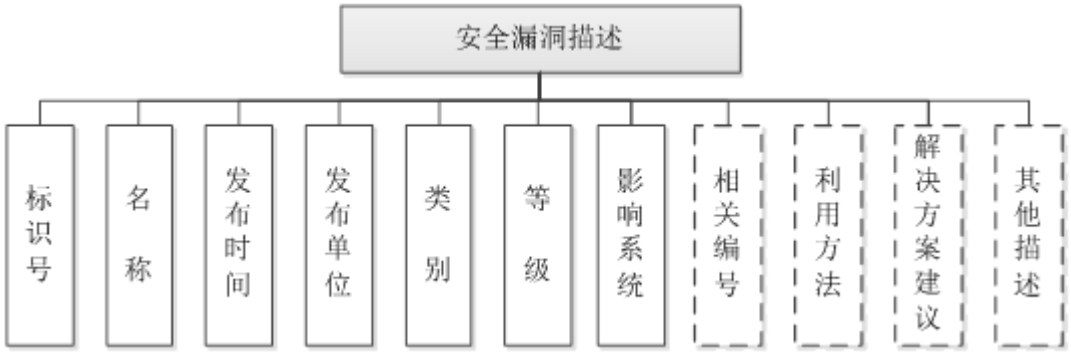

图1 安全漏洞描述项

安全漏洞描述所采用文字、字符、数字等书写形式，采用GB 7713—1987和GB/T 15835-1995标准。

4.2.1 标识号

安全漏洞以CVD-YYYY-NNNNNN格式为标识号。CVD为Common Vulnerabilities Description的缩写；YYYY为4位十进制数字，表示产生本安全漏洞的年份；NNNNNN为6位十进制数字，表示当年内产生的安全漏洞的序号。

4.2.2 名称

安全漏洞标题，概括性描述安全漏洞信息的短语，例如Internet Explorer 8.0缓冲区溢出漏洞。

4.2.3 发布时间

安全漏洞信息发布日期。日期书写采用GB/T 7408-2005，5.2.1.1完全表示法中的扩展格式。

4.2.4 发布单位

发布安全漏洞的单位全称。

4.2.5 类别

安全漏洞所属分类，说明安全漏洞分类归属的信息。

4.2.6 等级

安全漏洞危害级别，说明安全漏洞能够造成的危害程度。

4.2.7 影响系统

安全漏洞所影响系统的信息，例如厂商、产品名称和版本号等。

4.2.8 相关编号

安全漏洞的其他相关编号，例如Bugtraq编号、CVE编号等。

4.2.9 利用方法

安全漏洞利用的方法，例如安全漏洞攻击方案或利用代码。

4.2.10 解决方案建议

安全漏洞的解决方案，例如补丁信息等。

4.2.11 其他描述

安全漏洞描述需要说明的其他相关信息，例如安全漏洞产生的具体原因。

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/