ICS 35.040
L 80

中华人民共和国国家标准

GB/T 33561—2017

信息安全技术　安全漏洞分类

Information security technology—Vulnerabilities classification

2017-05-12 发布　　2017-12-01 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。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:国家信息技术安全研究中心、中国信息安全测评中心、中国科学院研究生院国家计算机网络入侵防范中心、国家计算机网络应急技术处理协调中心。

本标准主要起草人:宫亚峰、杜霖、魏方方、李冰、王宏、彭恒斌、原伟强、郭涛、郝永乐、张翀斌、张玉清、刘奇旭。

引　言

为客观认识安全漏洞，加强计算机信息系统安全漏洞的管理工作，科学规范安全漏洞的分类是十分必要的。

本标准是GB/T 28458—2012的配套标准，也可独立使用。

信息安全技术　安全漏洞分类

1　范围

本标准规定了计算机信息系统安全漏洞分类的原则和类别。

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管理和技术研究部门开展安全漏洞分析研究工作。

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 25069—2010　信息安全技术　术语

GB/T 28458—2012　信息安全技术　安全漏洞标识与描述规范

3　术语和定义

GB/T 25069—2010、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/T 25069—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

按照安全漏洞的特征来划分类别的操作。

4　缩略语

下列缩略语适用于本文件。

LDAP　轻量目录访问协议(Lightweight Directory Access Protocol)

SQL　结构化查询语言(Structured Query Language)

XML　可扩展置标语言(Extensible Markup Language)

XPATH　XML 路径语言 (XML Path Language)