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)

XSS　　跨站脚本(Cross Site Scripting)

5 安全漏洞分类

5.1 原则

安全漏洞的分类遵循以下原则：

a) 唯一性原则：按照属性与特征区分安全漏洞时，漏洞仅属于某一类别，不同时属于两个或两个以上类别。

b) 扩展性原则：允许根据实际情况扩展安全漏洞的类别。

一般的，可按照安全漏洞的形成原因、所处空间和时间进行分类处理，并择一使用。

5.2 分类

5.2.1 按成因分类

安全漏洞按照形成原因，可分为以下类别：

a) 边界条件错误：由于程序运行时未能有效控制操作范围导致的安全漏洞，如缓冲区堆溢出、缓冲区栈溢出、缓冲区越界操作、格式串处理等。

b) 数据验证错误：由于对携带参数或其中混杂操作指令的数据未能进行有效验证和正确处理导致的安全漏洞，如命令参数注入、SQL 注入、LDAP 注入、XPATH 注入、XSS 攻击等。

c) 访问验证错误：由于没有对请求处理的资源做正确授权检查所导致的安全漏洞，如远程或本地文件包含、认证绕过等。

d) 处理逻辑错误：由于程序实现逻辑处理功能时存在问题所导致的安全漏洞，如程序逻辑处理错误、逻辑分支覆盖不全面等。

e) 同步错误：由于程序对操作的同步处理不当所导致的安全漏洞，如竞争条件、不正确的数据序列化等。

f) 意外处理错误：由于程序对意外情况发生后处理不当而导致的安全漏洞。

g) 对象验证错误：由于程序处理使用对象时缺乏验证所导致的安全漏洞，如资源释放后重利用、各类对象错误引用等。

h) 配置错误：由于对计算机信息系统安全配置不当所导致的安全漏洞，如默认配置、默认权限、配置参数错误等。

i) 设计缺陷：由于计算机信息系统在设计时未考虑全面所导致的安全漏洞。

j) 环境错误：由于程序运行的软硬件系统不正确所导致的安全漏洞。

k) 其他：不能归入以上成因的安全漏洞。

5.2.2 按空间分类

安全漏洞按空间，可分为以下类别。

a) 应用层：安全漏洞可处于计算机信息系统的各个层面，应用层漏洞主要来自应用软件或数据的缺陷，如 Web 程序、数据库软件、各种应用软件等。

b) 系统层：系统层漏洞主要来自计算机操作系统的缺陷，如桌面操作系统、服务器操作系统、嵌入式操作系统、网络操作系统等。

c) 网络层：网络层漏洞主要来自网络的缺陷，如网络层身份认证、网络资源访问控制、数据传输保密与完整性、远程接入安全、域名系统安全和路由系统安全等。

5.2.3 按时间分类

5.2.3.1 生成阶段

在计算机信息系统的分析设计、开发实现、配置运维过程引入缺陷或错误等问题，存在的问题在执行时形成了安全漏洞，可分为以下类别。

a) 分析设计：在计算机信息系统的需求分析与设计过程中，由于缺乏风险分析，引用不安全的对象，强调易用和功能、性能使得安全性折中等因素而产生安全漏洞。

b) 开发实现：在计算机信息系统的开发过程中，由于开发人员在技术实现中有意或者无意引入缺陷产生安全漏洞。

c) 配置运维：在计算机信息系统的运行维护过程中，由于运维人员处理计算机信息系统相互关联、配置、结构不当等原因产生安全漏洞。

5.2.3.2 发现阶段

安全漏洞首次被漏洞发现者、使用者或厂商识别，可分为以下类别。

a) 未确认：安全漏洞首次被发现，并未给出漏洞资料和可以确认漏洞成因、危害等证据。

b) 待确认：安全漏洞由漏洞发现者报告厂商或漏洞管理组织，具有漏洞分析报告或能够重现漏洞的场景。

c) 已确认：安全漏洞由漏洞发现者、使用者或厂商正式确认或者发布，具有标识与描述等相关信息。

5.2.3.3 利用阶段

安全漏洞按照信息验证、公开、利用及信息扩散范围，可分为以下类别：

a) 未验证：安全漏洞没有可验证的方法，其成因、危害不可重现。

b) 验证：安全漏洞已有可验证的方法，其成因、危害可被重现。

c) 未公开：安全漏洞相关信息未向公众发布，扩散范围有限。

d) 公开：安全漏洞的相关信息已向公众发布。

5.2.3.4 修补阶段

安全漏洞按照修补状态，可分为以下类别：

a) 未修补：漏洞发现后，尚未进行任何修补。

b) 临时修补：漏洞发现后，采用临时应急修补方案，该方案可能会以损失功能性为代价，但漏洞并未得到实际修补。

c) 正式修补：漏洞发现后，经测试确认并提供修补方案或补丁程序，保证计算机信息系统的正常使用。

附 录 A
（资料性附录）
安全漏洞分类规范图表结构图

安全漏洞分类规范图表结构见图 A.1

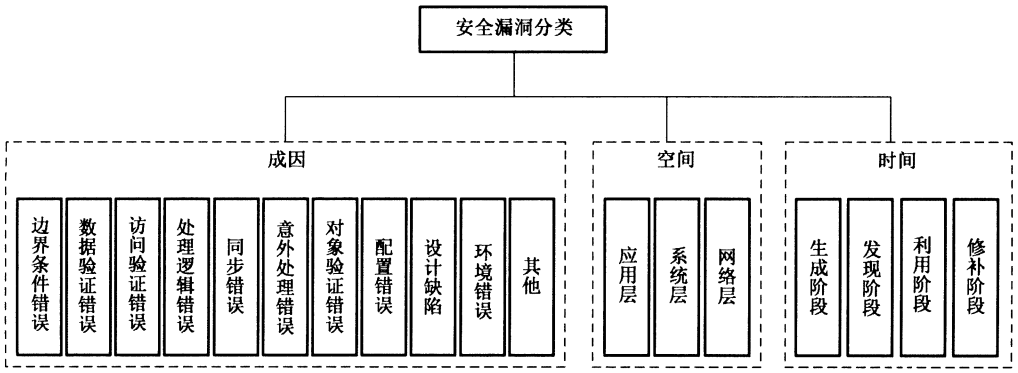

图 A.1 安全漏洞分类规范图表结构图

参 考 文 献

[1] 国家信息安全漏洞共享平台.http://www.cnvd.org.cn/

[2] 中国国家信息安全漏洞库.http://www.cnnvd.org.cn/

[3] Andy Ozment, Vulnerability Discovery&Software Security, University of Cambridge.2007

[4] Anil Bazazl and James D. Arthur, Towards A Taxonomy of Vulnerabilities, Proceedings of the 40th Hawaii International Conference on System Sciences.2007

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

[6] NIST Special Publication 800-51, Rev.1 Guide to Using Vulnerability Naming Schemes, http://csrc.nist.gov/publications/nistpubs/800-51-rev1/SP800-51rev1.pdf

[7] Vulnerability Type Distributions in CVE, Steve Christey, Robert A. Martin. 2007