ICS 35.040
L 80

中华人民共和国国家标准

GB/T 28458—2020
代替 GB/T 28458—2012

信息安全技术
网络安全漏洞标识与描述规范

Information security technology—
Cybersecurity vulnerability identification and description specification

2020-11-19 发布　　2021-06-01 实施

国家市场监督管理总局
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。

本标准代替 GB/T 28458—2012《信息安全技术　安全漏洞标识与描述规范》，与 GB/T 28458—2012 相比，主要技术变化如下：

——修改了网络安全漏洞的术语和定义（见 3.1，2012 年版的 3.2）；

——增加了缩略语（见第 4 章）；

——将标识与描述作为两个方面表述，增加了标识字段描述内容（见 5.2）；

——增加了验证者、发现者、存在性说明和检测方法等描述项内容（见 5.3.4、5.3.5、5.3.10、5.3.11）；

——修改了标识项、名称、受影响产品或服务、相关编号、解决方案等内容（见 5.2、5.3.1、5.3.8、5.3.9、5.3.12，2012 年版的 4.2.1、4.2.2、4.2.7、4.2.8、4.2.10）；

——删除了利用方法描述项（见 2012 年版的 4.2.9）。

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/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、国家计算机网络应急技术处理协调中心、中国信息安全测评中心、中国科学院大学国家计算机网络入侵防范中心、中国电子技术标准化研究院、中国科学院信息工程研究所、启明星辰信息技术集团股份有限公司、北京百度网讯科技有限公司、奇安信科技集团股份有限公司、北京神州绿盟信息安全科技股份有限公司、上海斗象信息科技有限公司、阿里巴巴（北京）软件服务有限公司、深圳市腾讯计算机系统有限公司、北京知道创宇信息技术有限公司、恒安嘉新（北京）科技股份公司、哈尔滨安天科技集团股份有限公司、浙江蚂蚁小微金融服务集团股份有限公司、深信服科技股份有限公司、北京数字观星科技有限公司、北京摄星科技有限公司。

本标准主要起草人：王宏、张玉清、谢安明、刘奇旭、高红静、舒敏、郝永乐、郭亮、黄正、上官晓丽、任泽君、崔牧凡、曲泷玉、贾依真、陈悦、贾子骁、郑亮、何茂根、赵旭东、李霞、傅强、赵焕菊、李柏松、刘楠、王文杰、王鹤。

本标准所代替标准的历次版本发布情况为：

——GB/T 28458—2012。

信息安全技术
网络安全漏洞标识与描述规范

1 范围

本标准规定了网络安全漏洞(以下简称“漏洞”)的标识与描述信息。

本标准适用于从事漏洞发布与管理、漏洞库建设、产品生产、研发、测评与网络运营等活动的所有相关方。

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/T 25069 信息安全技术 术语

GB/T 30276—2020 信息安全技术 网络安全漏洞管理规范

GB/T 30279—2020 信息安全技术 网络安全漏洞分类分级指南

3 术语和定义

GB/T 25069、GB/T 30276—2020、GB/T 30279—2020 界定的以及下列术语和定义适用于本文件。

3.1

网络安全漏洞 cybersecurity vulnerability

网络产品和服务在需求分析、设计、实现、配置、测试、运行、维护等过程中,无意或有意产生的、有可能被利用的缺陷或薄弱点。

注:这些缺陷或薄弱点以不同形式存在于网络产品和服务的各个层次和环节中,一旦被恶意主体所利用,就会对网络产品和服务的安全造成损害,从而影响其正常运行。

4 缩略语

下列缩略语适用于本文件。

CNCVD:中国国家网络安全漏洞库(China National Cybersecurity Vulnerability Database)

CVE:公共漏洞和暴露(Common Vulnerabilities and Exposures)

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

5 网络安全漏洞标识与描述

5.1 框架

针对每一个漏洞进行标识与描述的框架如图 1 所示,分为标识项和描述项两大类,其中描述项包括