ICS 35.040
L 80

中华人民共和国国家标准

GB/T 30279—2020
代替 GB/T 30279—2013，GB/T 33561—2017

信息安全技术
网络安全漏洞分类分级指南

Information security technology—
Guidelines for categorization and classification of cybersecurity vulnerability

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 …… Ⅰ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 1
5　网络安全漏洞分类 …… 1
5.1　概述 …… 1
5.2　代码问题 …… 2
5.3　配置错误 …… 4
5.4　环境问题 …… 4
5.5　其他 …… 5
6　网络安全漏洞分级 …… 5
6.1　概述 …… 5
6.2　网络安全漏洞分级指标 …… 5
6.3　网络安全漏洞分级方法 …… 9
附录A（规范性附录）　被利用性分级表 …… 11
附录B（规范性附录）　影响程度分级表 …… 13
附录C（规范性附录）　环境因素分级表 …… 14
附录D（规范性附录）　漏洞技术分级表 …… 15
附录E（规范性附录）　漏洞综合分级表 …… 16
附录F（资料性附录）　漏洞分级示例 …… 17
参考文献 …… 19

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 33561—2017《信息安全技术　安全漏洞分类》、GB/T 30279—2013《信息安全技术　安全漏洞等级划分指南》，与 GB/T 33561—2017、GB/T 30279—2013 相比，主要技术变化如下：

——将 GB/T 33561—2017 和 GB/T 30279—2013 的范围进行合并修改（见第 1 章）；

——将 GB/T 33561—2017 和 GB/T 30279—2013 的规范性引用文件进行合并补充（见第 2 章）；

——将 GB/T 33561—2017 和 GB/T 30279—2013 的术语和定义进行合并修改（见第 3 章）；

——删除了 GB/T 33561—2017 中的缩略语；

——将 GB/T 33561—2017 中的“按成因分类”对应本标准的“网络安全漏洞分类”，将 GB/T 33561—2017 采用的线性分类框架调整为树形（见图 1）；

——删除了 GB/T 33561—2017 中的“按空间分类”；

——删除了 GB/T 33561—2017 中的“按时间分类”；

——将 GB/T 30279—2013 中的“等级划分要素”对应本标准的“网络安全漏洞分级指标”，扩展了漏洞分级指标（见图 2）；

——将 GB/T 30279—2013 中的“等级划分”对应本标准的“网络安全漏洞分级方法”，将分级方法修改为技术分级和综合分级（见附录 D 中表 D.1 和附录 E 中表 E.1）。

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：中国信息安全测评中心、北京中测安华科技有限公司、中国电子技术标准化研究院、国家计算机网络应急技术处理协调中心、国家信息技术安全研究中心、北京邮电大学、北京华云安信息技术有限公司、北京华顺信安科技有限公司、国网思极网安科技（北京）有限公司、上海三零卫士信息安全有限公司、国家计算机网络入侵防范中心、中国科学院信息工程研究所、国家计算机网络入侵防范中心、浙江蚂蚁小微金融服务集团有限公司、网神信息技术（北京）股份有限公司、北京长亭科技有限公司、杭州安恒信息技术股份有限公司、深信服科技股份有限公司、腾讯科技（北京）有限公司、四川省信息安全测评中心、上海犇众信息技术有限公司、启明星辰信息技术集团股份有限公司、恒安嘉新（北京）科技股份公司。

本标准主要起草人：郝永乐、郑亮、贾依真、时志伟、张宝峰、李斌、侯元伟、曲泷玉、毛军捷、饶华一、许源、孟德虎、张兰兰、任泽君、上官晓丽、舒敏、王文磊、王宏、连樱、赵旭东、崔宝江、付俊松、沈传宝、赵武、许勇刚、林亮成、李智林、张玉清、刘奇旭、史慧洋、王宇、简云定、柳本金、白健、杨坤、常明政、刘志乐、吴卓群、叶润国、刘桂泽、王丹琛、韩争光、丁斌、胡兵。

本标准所代替标准的历次版本发布情况为：

——GB/T 30279—2013；

——GB/T 33561—2017。

信息安全技术
网络安全漏洞分类分级指南

1 范围

本标准提供了网络安全漏洞(以下简称“漏洞”)的分类方式、分级指标,给出了分级方法的建议。

本标准适用于网络产品和服务的提供者、网络运营者、漏洞收录组织、漏洞应急组织在漏洞管理、产品生产、技术研发、网络运营等相关活动中进行的漏洞分类和危害等级评估等。

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 20984 信息安全技术 信息安全风险评估规范

GB/T 25069 信息安全技术 术语

GB/T 28458 信息安全技术 安全漏洞标识与描述规范

GB/T 30276 信息安全技术 信息安全漏洞管理规范

3 术语和定义

GB/T 25069、GB/T 20984、GB/T 28458、GB/T 30276 界定的以及下列术语和定义适用于本文件。

3.1

受影响组件 impacted component

在网络产品和服务中,漏洞触发受影响的组件。

4 缩略语

下列缩略语适用于本文件。

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

5 网络安全漏洞分类

5.1 概述

网络安全漏洞分类是基于漏洞产生或触发的技术原因对漏洞进行的划分,分类导图如图 1 所示。本标准采用树形导图对漏洞进行分类,首先从根节点开始,根据漏洞成因将漏洞归入某个具体的类别,如果该类型节点有子类型节点,且漏洞成因可以归入该子类型,则将漏洞划分为该子类型,如此递归,直到漏洞归入的类型无子类型节点或漏洞不能归入子类型为止。