ICS 35.040
L 80

中华人民共和国国家标准

GB/T 30276—2020
代替 GB/T 30276—2013

信息安全技术
网络安全漏洞管理规范

Information security technology—
Specification for cybersecurity vulnerability management

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 30276—2013《信息安全技术　信息安全漏洞管理规范》，与 GB/T 30276—2013 相比，主要技术变化如下：

——修改了范围的表述（见第 1 章，2013 年版的第 1 章）；

——增加了规范性引用文件 GB/T 30279—2020，删除了规范性引用文件 GB/T 18336.1—2008（见第 2 章，2013 年版的第 2 章）；

——增加了术语“（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”“漏洞发现”“漏洞报告”“漏洞接收”“漏洞验证”“漏洞发布”（见 3.2、3.3、3.4、3.5、3.6、3.7、3.8、3.9、3.10）；

——删除了术语“修复措施”“厂商”“漏洞管理组织”“漏洞发现者”（2013 年版的 3.1、3.3、3.4、3.5）；

——修改了漏洞管理流程，从漏洞管理的角度出发，重新定义了漏洞管理流程的各阶段，将原来的“预防、收集、消减、发布”管理阶段调整为“漏洞发现和报告、漏洞接收、漏洞验证、漏洞处置、漏洞发布、漏洞跟踪”，并提出各管理阶段中各相关角色应遵循的要求（见第 4 章、第 5 章，2013 年版的第 4 章、第 5 章）；

——删除了“附录 A（规范性附录）　漏洞处理策略”（2013 年版的附录 A）。

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、国家信息技术安全研究中心、中国电子技术标准化研究院、上海交通大学、恒安嘉新（北京）科技股份公司、网神信息技术（北京）股份有限公司、上海斗象信息科技有限公司、北京数字观星科技有限公司、阿里巴巴（北京）软件服务有限公司、公安部第三研究所、中国科学院大学、北京奇虎科技有限公司。

本标准主要起草人：云晓春、舒敏、崔牧凡、王文磊、严寒冰、贾子骁、陈悦、任泽君、崔婷婷、高继明、王桂温、郭亮、谢忱、白晓媛、王宏、李斌、孟魁、姜开达、黄道丽、赵旭东、赵芸伟、蒋凌云、郝永乐、叶润国、刘楠、张玉清、姚一楠。

本标准所代替标准的历次版本发布情况为：

——GB/T 30276—2013。

信息安全技术
网络安全漏洞管理规范

1 范围

本标准规定了网络安全漏洞管理流程各阶段(包括漏洞发现和报告、接收、验证、处置、发布、跟踪等)的管理流程、管理要求以及证实方法。

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、漏洞应急组织等开展的网络安全漏洞管理活动。

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 信息安全技术 术语

GB/T 28458—2020 信息安全技术 网络安全漏洞标识与描述规范

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 28458—2020 界定的以及下列术语和定义适用于本文件。

3.1

用户 user

使用网络产品和服务的个人或组织。

3.2

(网络产品和服务的)提供者 provider of network products and services

提供网络产品和服务的个人或组织。

3.3

网络运营者 network operator

网络的所有者、管理者和网络服务提供者。

3.4

漏洞收录组织 vulnerability repository organization

提供公开渠道接收漏洞信息,并建有相应工作流程的组织。

3.5

漏洞应急组织 vulnerability emergency response organization

与提供者、网络运营者、漏洞收录组织、网络运营者、安全研究机构、网络安全企业等建有成熟的技术协作体系、负责安全漏洞的响应和处置工作的网络安全应急协调组织。

3.6

漏洞发现 vulnerability discovery

通过技术手段,识别出网络产品和服务存在漏洞的过程。