



中华人民共和国国家标准

GB/T 30276—2013

信息安全技术 信息安全漏洞管理规范

Information security technology—
Vulnerability management criterion specification

2013-12-31 发布

2014-07-15 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

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。

本文件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。

本标准起草单位:中国信息安全测评中心、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。

本标准主要起草人:刘晖、王明华、宫亚峰、易锦、刘彦钊、熊琦、张磊、赵向辉、刘林、吴润浦、李娟、姚原岗、何世平、王宏。

信息安全技术

信息安全漏洞管理规范

1 范围

本标准规定了信息安全漏洞的管理要求,涉及漏洞的发现、利用、修复和公开等环节。

本标准适用于用户、厂商和漏洞管理组织进行信息安全漏洞的管理活动,包括漏洞的预防、收集、消减和发布。

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 18336.1—2008 信息技术 安全技术 信息技术安全性评估准则

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 和 GB/T 18336.1—2008 中界定的以及下列术语和定义适用于本文件。

3.1

修复措施 remediation

用以修复漏洞的补丁、升级版本、配置策略等。

3.2

用户 user

使用信息系统的个人或组织。

3.3

厂商 vendor

开发信息系统的组织。

3.4

漏洞管理组织 vulnerability management organization

协调厂商和漏洞发现者处理漏洞信息的组织。

注:组织包括国家信息安全主管部门等。

3.5

漏洞发现者 vulnerability finder

发现信息系统中潜在漏洞的个人或组织。

4 信息安全漏洞生命周期

依据信息安全漏洞(简称漏洞)从产生到消亡的整个过程,信息安全漏洞生命周期分以下几个阶段: