ICS 35.040
L 80

# 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：

a) 漏洞的发现：通过人工或者自动的方法分析、挖掘漏洞的过程，并且该漏洞可以被验证和重现。
b) 漏洞的利用：利用漏洞对计算机信息系统的保密性、完整性和可用性造成损害的过程。
c) 漏洞的修复：通过补丁、升级版本或配置策略等对漏洞进行修补的过程，使得该漏洞不能够被恶意主体所利用。
d) 漏洞的公开：通过公开渠道（如网站、邮件列表等）公布漏洞信息的过程。

## 5 信息安全漏洞管理

### 5.1 原则

信息安全漏洞管理遵循以下原则：

a) 公平、公开、公正原则：厂商在处理自身产品的漏洞时应坚持公开、公正原则。漏洞管理组织在处理漏洞信息时应遵循公平、公开、公正原则。
b) 及时处理原则：用户、厂商和漏洞管理组织在处理漏洞信息时都应遵循及时处理的原则，及时消除漏洞与隐患。
c) 安全风险最小化原则：在处理漏洞信息时应以用户的风险最小化为原则，保障广大用户的利益。

### 5.2 规划

根据漏洞生命周期中漏洞所处的不同状态，将漏洞管理行为对应为预防、收集、消减和发布等实施活动如图1所示。

预防是指通过各种安全手段提高信息系统的安全水平，避免漏洞的产生和恶意利用。

收集是针对已发现的漏洞进行信息的及时跟踪与获取。

消减是指在漏洞被发现后积极采取补救措施，最大限度减少漏洞带来的损失。

发布是指在遵循一定的发布策略的前提下，对漏洞及其修复信息进行发布。

用户、厂商和漏洞管理组织应依据本标准建立符合自身特点的漏洞处理策略和处理流程。

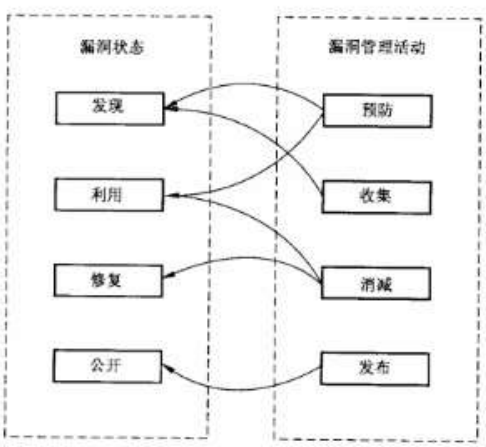


图1 漏洞生命周期和管理活动对应关系

### 5.3 实施

#### 5.3.1 概述

在漏洞管理活动中，漏洞发现者、厂商、漏洞管理组织和用户应规范自身的行为，国家信息安全主管部门应在漏洞发现者、厂商和用户之间发挥协调者的作用，在漏洞处理过程中维护公平、公开、公正原则、及时处理原则和安全风险最小化原则，保障被发现的漏洞得到有效处置。

#### 5.3.2 漏洞的预防

##### 5.3.2.1 厂商

厂商应尽可能地采用安全开发生命周期，在需求、设计、实现、配置、运行等阶段采取风险分析、代码审查、渗透测试等手段，提高产品安全性。

##### 5.3.2.2 用户

用户应对使用的计算机系统进行安全加固(如及时安装升级补丁、关闭不必要的服务等)，安装安全防护产品和开启相应的安全配置。

#### 5.3.3 漏洞的收集

##### 5.3.3.1 漏洞管理组织

漏洞管理组织应与漏洞发现者、用户、厂商等漏洞管理中涉及的各方进行沟通与协调，广泛收集并及时处置漏洞，具体活动包括：

a) 漏洞收集：漏洞管理组织应建立和维护公开的漏洞收集渠道。针对收集到的漏洞信息，应及时进行处置。

b) 漏洞验证：漏洞管理组织应负责联合厂商在规定时间内(见 A.1)验证收集到漏洞是否已公布，漏洞是否真实存在，确定漏洞的危害等级，并依据 GB/T 28458—2012 确定漏洞的标识和描述。

c) 漏洞通报：漏洞管理组织应将漏洞信息及时通知厂商(见 A.3)，危害等级高的漏洞优先处理，以降低因漏洞引起的安全威胁。

##### 5.3.3.2 厂商

厂商应提供接收漏洞信息的渠道，例如，网站、邮件或电话等。

厂商应对漏洞发现者或漏洞管理组织报告的漏洞在规定时间(见 A.1)内确认其是否真实存在，并回复报告方。

##### 5.3.3.3 漏洞发现者

漏洞发现者在发现漏洞的第一时间应向该漏洞的受影响厂商或漏洞管理组织报告漏洞详情。

#### 5.3.4 漏洞的消减

##### 5.3.4.1 厂商

厂商应遵循及时处理原则，依据厂商对漏洞的消减处理策略(见 A.2)，对发现的漏洞在规定时间(见 A.1)内进行修复，依据漏洞的危害等级，优先开发高危漏洞的修复措施。

厂商应保证补丁的有效性和安全性，并进行兼容性测试，避免因更新补丁而对产品或系统带来影响

或新的安全风险。

#### 5.3.4.2 漏洞管理组织

漏洞管理组织应督促厂商及时开发修复措施，以降低因该漏洞引起的安全问题。若在规定时间内，厂商未及时回复或未给出修复措施，则漏洞管理组织可以联系信息安全厂商或其他安全机构针对该漏洞给出修复措施(见 A.4)。

#### 5.3.4.3 用户

用户应及时跟踪公开漏洞库所公布的漏洞信息和相关厂商的安全公告，并根据其资产重要性以及漏洞的危害程度，进行及时修复。

### 5.3.5 漏洞的发布

#### 5.3.5.1 漏洞管理组织

漏洞管理组织应遵循公平、公开、公正的原则，在规定时间内(见 A.1)发布漏洞及修复措施等信息(见 GB/T 28458—2012)。

注：漏洞发布应是在风险最小化的原则下有条件地公开，例如，0day 漏洞不宜公开。

#### 5.3.5.2 厂商

厂商应建立发布渠道，在规定时间内(见 A.1)发布漏洞信息及修复措施，并通知用户。

## 5.4 评审

跟踪并监测漏洞管理活动的实施情况，定期对实施方案和实施效果进行检查、评审，审查内容包括：

a) 预防措施是否落实到位，漏洞是否得到有效预防。
b) 已发现的漏洞是否得到有效处置。
c) 参与漏洞管理的各方是否协调一致。
d) 漏洞处理过程是否符合及时处理和安全风险最小化等原则。

## 5.5 改进

改进的内容包括：

a) 根据现有漏洞管理的评审结果，核查管理方案。
b) 合理改进漏洞管理方案及其相关文档。

# 附 录 A
（规范性附录）
漏洞处理策略

## A.1 漏洞处理时间表

在不同的漏洞管理活动中对漏洞进行处理时所规定的时间如表 A.1 所示，相关人员或组织应在规定时间内完成对漏洞的处理。

表 A.1 漏洞处理时间表

| 对漏洞的处理 | 时间段（不大于） |
| --- | --- |
| 验证 | 10 个工作日 |
| 反馈 | 5 个工作日 |
| 开发修复措施 | 30 个工作日 |
| 通报漏洞管理组织 | 5 个工作日 |
| 发布漏洞信息及修复措施 | 5 个工作日 |

## A.2 厂商针对漏洞的消减处理策略

厂商应为发现的漏洞开发解决方案。解决方案的开发过程包含更加细致的调查过程，包括调查漏洞更深层的原因，以及确定其他产品是否有同样或者类似的漏洞。厂商最终需开发出补丁或者临时修复措施，同时测试检验修复措施的有效性、安全性和兼容性，不能破坏原系统的功能。厂商在发布漏洞信息和修复措施后，关注用户反馈，考虑是否需对漏洞修复进一步完善。

## A.3 漏洞管理组织关于漏洞通报的处理策略

漏洞管理组织在对漏洞进行验证之后，应对受影响产品的厂商进行通报，敦促其及时开发修复补丁。厂商应在接到通知后 5 个工作日内给予正式反馈，并给出漏洞修复时间表，如逾期不予反馈，或无法与厂商取得联系，则漏洞管理组织有权对漏洞内容进行公布，以提示用户修复，因漏洞公布给用户带来的损失，由厂商承担。

## A.4 漏洞管理组织关于厂商修复漏洞的处理策略

厂商应在确认漏洞信息后 30 个工作日内提供补丁或修复措施，由于技术或其他不可抗拒的原因导致 30 个工作日内无法完成补丁开发，可根据厂商申请情况酌情延长漏洞修复时间。否则漏洞管理组织有权对漏洞内容进行公布，以提示用户修复，因漏洞公布给用户带来的损失，由厂商承担。漏洞管理组织可以联系信息安全厂商或其他安全机构针对该漏洞给出修复措施。

## 参 考 文 献

[1] Creating a Patch and Vulnerability Management Program, NIST, Special Publication 800-40, 2005.11

[2] ISO/IEC 30111 Information technology—Security techniques—Vulnerability handing processes

[3] ISO/IEC 29147 Information technology—Security techniques—Vulnerability disclosure

[4] DISA IAVA Process Handbook v2.1, 2002, 6

[5] Common Vulnerability and Explore, http://cve.mitre.org

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

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

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

中华人民共和国
国家标准
信息安全技术 信息安全漏洞管理规范
GB/T 30276—2013
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 0.75 字数 14 千字
2014年5月第一版 2014年5月第一次印刷
*
书号:155066·1-49029 定价 16.00 元



GB/T 30276-2013

打印日期:2014年5月17日 F009A