ICS 35.040
L 80

中华人民共和国国家标准

GB/T 30279—2013

信息安全技术
安全漏洞等级划分指南

Information security technology—Vulnerability classification guide

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、中国科学院研究生院国家计算机网络入侵防范中心、北京航空航天大学。

本标准主要起草人:张翀斌、张玉清、张宝峰、刘奇旭、张奕、郭涛、毛军捷、吴毓书、郭颖、李舟军、饶华一、许源、李凤娟、杨永生。

信息安全技术
安全漏洞等级划分指南

1 范围

本标准规定了信息系统安全漏洞(简称漏洞)的等级划分要素和危害程度级别。

本标准适用于信息安全漏洞管理组织和信息安全漏洞发布机构对信息安全漏洞危害程度的评估和认定,适用于信息安全产品生产、技术研发、系统运营等组织、机构在相关工作中参考。

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—2010 信息安全技术 术语

3 术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

安全漏洞 vulnerability

计算机信息系统在需求、设计、实现、配置、运行等过程中,有意或无意产生的缺陷。这些缺陷以不同形式存在于计算机信息系统的各个层次和环节之中,一旦被恶意主体所利用,就会对计算机信息系统的安全造成损害,从而影响计算机信息系统的正常运行。

[GB/T 28458—2012,定义 3.2]

3.2

完整性 integrity

保证信息及信息系统不会被非授权更改或破坏的特性。包括数据完整性和系统完整性。

[GB/T 20984—2007,定义 3.10]

3.3

可用性 availability

数据或资源的特性,被授权实体按要求能访问和使用数据或资源。

[GB/T 20984—2007,定义 3.3]

3.4

保密性 confidentiality

数据所具有的特性,即表示数据所达到的未提供或未泄露给非授权的个人、过程或其他实体的程度。

[GB/T 20984—2007,定义 3.5]

3.5

访问路径 access path

攻击者利用安全漏洞影响目标系统的路径前提。

3.6

利用复杂度 exploit complexity

对于安全漏洞可被利用于影响目标系统的技术、环境等条件的难度。

3.7

影响程度 impact level

利用安全漏洞对目标系统造成的损害程度。

4 安全漏洞等级划分方法

4.1 等级划分要素

4.1.1 概述

安全漏洞等级划分要素包括访问路径、利用复杂度和影响程度三方面。

4.1.2 访问路径

访问路径的赋值包括本地、邻接和远程，通常可被远程利用的安全漏洞危害程度高于可被邻接利用的安全漏洞，可本地利用的安全漏洞次之，见表1。

表1 访问路径赋值说明表

赋 值	描 述
本地	利用该安全漏洞要求攻击者物理接触到受攻击的系统，或者已具有一个本地账号。本地攻击示例：本地权限提升等
邻接	利用该安全漏洞要求攻击者与受攻击系统同处于一个广播域或冲突域中。邻接攻击示例：蓝牙、IEEE 802.11 等
远程	不局限于本地和邻接。远程攻击示例：RPC 缓冲区溢出漏洞

4.1.3 利用复杂度

利用复杂度的赋值包括简单和复杂，通常利用复杂度为简单的安全漏洞危害程度高，见表2。

表2 攻击复杂度赋值说明表

赋 值	描 述
简单	无需借助外部条件，例如自动操作、无需授权即可完成攻击
复杂	需要借助外部条件，例如需要人工参与点击文件、点击按钮或者用户授权

4.1.4 影响程度

影响程度的赋值包括完全、部分、轻微和无，通常影响程度为完全的安全漏洞危害程度高于影响程度为部分的安全漏洞，影响程度为轻微的安全漏洞次之，影响程度为无的安全漏洞可被忽略，见表3。

表 3　影响程度赋值说明表

赋　值	描　　述
完全	安全漏洞对保密性、完整性和可用性的影响较严重，见表 5 序号 1～7
部分	安全漏洞对保密性、完整性和可用性影响相对较轻，见表 5 序号 8～17
轻微	安全漏洞对保密性、完整性和可用性影响最轻，见表 5 序号 18～26
无	安全漏洞对保密性、完整性和可用性影响均为无，见表 5 序号 27

影响程度的赋值由安全漏洞对目标的保密性、完整性和可用性三个方面的影响共同导出，每个方面的影响赋值为完全、部分和无，见表 4。

表 4　保密性、完整性和可用性影响赋值说明表

赋　值	描　　述
完全	安全漏洞对保密性、完整性或可用性的影响较严重
部分	安全漏洞对保密性、完整性或可用性影响相对较轻
无	安全漏洞对保密性、完整性或可用性无影响

按照安全漏洞对系统保密性、可用性和完整性三方面的影响赋值即可得出影响程度赋值，见表 5。

表 5　影响程度赋值对应表

序　号	保密性影响	完整性影响	可用性影响	影响程度
1	完全	完全	完全	完全
2	完全	完全	部分	完全
3	完全	部分	完全	完全
4	完全	部分	部分	完全
5	部分	完全	完全	完全
6	部分	完全	部分	完全
7	部分	部分	完全	完全
8	完全	完全	无	部分
9	完全	部分	无	部分
10	完全	无	完全	部分
11	完全	无	部分	部分
12	部分	无	完全	部分
13	部分	完全	无	部分
14	无	完全	完全	部分
15	无	完全	部分	部分
16	无	部分	完全	部分
17	部分	部分	部分	部分

表 5（续）

序　号	保密性影响	完整性影响	可用性影响	影响程度
18	完全	无	无	轻微
19	部分	部分	无	轻微
20	部分	无	部分	轻微
21	部分	无	无	轻微
22	无	完全	无	轻微
23	无	部分	部分	轻微
24	无	部分	无	轻微
25	无	无	完全	轻微
26	无	无	部分	轻微
27	无	无	无	无
注：序号 27 表示对保密性、完整性、可用性均无影响，忽略此组合。				

4.2　等级划分

安全漏洞的危害程度从低至高依次为低危、中危、高危和超危，具体危害等级划分方法见表 6。

表 6　安全漏洞危害等级划分表

序　号	访问路径	利用复杂度	影响程度	安全漏洞等级
1	远程	简单	完全	超危
2	远程	简单	部分	高危
3	远程	复杂	完全	高危
4	邻接	简单	完全	高危
5	邻接	复杂	完全	高危
6	本地	简单	完全	高危
7	远程	简单	轻微	中危
8	远程	复杂	部分	中危
9	邻接	简单	部分	中危
10	本地	简单	部分	中危
11	本地	复杂	完全	中危

表 6（续）

序　号	访问路径	利用复杂度	影响程度	安全漏洞等级
12	远程	复杂	轻微	低危
13	邻接	简单	轻微	低危
14	邻接	复杂	部分	低危
15	邻接	复杂	轻微	低危
16	本地	简单	轻微	低危
17	本地	复杂	部分	低危
18	本地	复杂	轻微	低危

安全漏洞等级划分步骤及示例参见附录 A。

附 录 A
（资料性附录）
安全漏洞等级划分步骤及示例

A.1 安全漏洞等级划分步骤

安全漏洞等级划分步骤包括：

a) 参照表 1，确定访问路径的赋值；
b) 参照表 2，确定利用复杂度的赋值；
c) 参照表 4，分别确定保密性、完整性和可用性的影响赋值；
确定影响的步骤包括：
1) 确定保密性的赋值；
2) 确定完整性的赋值；
3) 确定可用性的赋值。
d) 参照表 5，确定影响程度赋值；
e) 参照表 6，根据访问路径、利用复杂度和影响程度的赋值，确定安全漏洞等级。

A.2 安全漏洞等级划分举例

微软 Windows RPC 缓冲区溢出漏洞(CNNVD-200810-406)，其安全漏洞等级划分步骤如下：

a) 参照表 1，确定访问路径的赋值为“远程”；
b) 参照表 2，确定利用复杂度的赋值为“简单”；
c) 参照表 4，分别确定保密性、完整性和可用性的影响赋值；
确定影响的步骤包括：
1) 确定保密性赋值为“完全”；
2) 确定完整性赋值为“完全”；
3) 确定可用性赋值为“完全”。
d) 参照表 5，确定影响程度赋值符合表 5 序号 1 的组合，为“完全”；
e) 参照表 6，根据访问路径、利用复杂度和影响程度的赋值，确定安全漏洞等级符合表 6 序号 1 的组合，为“超危”，见表 A.1。

表 A.1 安全漏洞等级划分示例

漏洞编号	访问路径	利用复杂度	影响程度			安全漏洞等级
			保密性	完整性	可用性	
			完全	完全	完全	超危
CNNVD-200810-406	远程	简单	完全			

参 考 文 献

[1] GB/T 28458—2012 信息安全技术 安全漏洞标识与描述规范
[2] GB/T 20984—2007 信息安全技术 信息安全风险评估规范