GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80

GB/T 33561-2017

Information Security Technology – Vulnerabilities Classification

信息安全技术　安全漏洞分类

Issued on: May 12, 2017 **Implemented on: December 1, 2017**

Issued by: General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China;
Standardization Administration of the People's Republic of China.

Table of Contents

Foreword

This Standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This Standard was proposed by and shall be under the jurisdiction of the National Information Security Standardization Technical Committee (SAC/TC 260).

The drafting organizations of this Standard: National Research Institute of Information Technology Security, China Information Technology Security Evaluation Centre, National Computer Network Intrusion Prevention Centre of China Academy of Sciences Postgraduate School, National Computer Network Emergency Response Technical Team/Coordination Center of China.

The main drafters of this Standard: Gong Yafeng, Du Lin, Wei Fangfang, Li Bing, Wang Hong, Peng Hengbin, Yuan Weiqiang, Guo Tao, Hao Yongle, Zhang Chongbin, Zhang Yuqing, Liu Qixu.

Information Security Technology – Vulnerabilities Classification

1 Application Scope

This Standard specifies the principles and categories for the classification of security vulnerabilities of computer information system.

This Standard applies to the security vulnerabilities management of the computer information system security management department and the security vulnerabilities analysis and research work of the technical research department.

2 Normative References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition dated applies to this document. For undated references, the latest edition of the referenced documents (including all amendments) applies to this Standard.

GB/T 25069-2010, *Information Security Technology – Glossary*

GB/T 28458, *Information Security Technology – Vulnerability Identification and Description Specification*

3 Terms and Definitions

Those defined in GB/T 25069-2010 and GB/T 28458-2012 and the following terms and definitions apply.

3.1

computer information system

A man-machine system which consists of computers and relevant and supporting equipment and facilities (including network) and deals with the processes of acquisition, processing, storage, transmission, retrieval and others in accordance with certain application objectives and rules.

[GB/T 25069-2010, Definition 2.1.14]

3.2

vulnerability

An intentional or unintentional flaw which occurs during the processes of computer information system, including requirement, design, realization, configuration and operation. These flaws exist on all levels and links of the computer information system in different forms; once they are used by malicious entities, they will cause harm to the security of the computer information system and influence the normal operation of the computer information system.

[GB/T 28458-2012, Definition 3.2]

4 Abbreviations

The following abbreviations apply to this document.

LDAP Lightweight Directory Access Protocol

SQL Structured Query Language

XML Extensible Markup Language

XPATH XML Path Language

XSS Cross Site Scripting

5 Classification of Security Vulnerabilities

5.1 Principles

The classification of security vulnerabilities shall be subjected to the following principles:

a) uniqueness principle: when a security vulnerability is differentiated in accordance with properties and characteristics, a vulnerability only belongs to some category but not belongs to two or more categories.

b) extensibility principle: the category in which security vulnerabilities may be extensible based on actual conditions.

5.2 Classification

5.2.1 Classification in accordance with causes

Security vulnerabilities may be classified into the following categories in accordance with the causes:

a) boundary condition errors: security vulnerabilities caused by the failure to control the operating range during the program run, such as buffer heap overflow, buffer stack overflow, buffer cross-border operation and format string processing;

systems;

c) the network layer: the vulnerabilities of the network layer mainly come from the network, such as network layer identity authentication, network resource access control, data transmission confidentiality and completeness, remote access security, domain name system security and routing system security.

5.2.3 Classification in accordance with time

5.2.3.1 Generation stage

The computer information system introduces defects or errors during analysis and design, development, and configuration, operation and maintenance; the existing problems generate security vulnerabilities during implementation; they can be classified into the following categories:

a) the analysis and design: security vulnerabilities caused by the factors, including the quotation of insecure objects, emphasis of ease of use and functions and performances to compromise security, because of the lack of risk analysis during the demand analysis and design process of the computer information system;

b) the development: security vulnerabilities caused by intentional or unintentional defects introduced by the developers in the technical realization during the development process of the computer information system;

c) the configuration, operation and maintenance: security vulnerabilities caused by the factors, including improper processing of the interrelations, configurations and structures of the computer information system by the personnel of operation and maintenance during the process of operation and maintenance of the computer information system.

5.2.3.2 Discovery stage

Security vulnerabilities are identified by the vulnerability discoverers, users or manufacturers for the first time, and may be classified into the following categories:

a) the unconfirmed: security vulnerabilities are discovered for the first time, failing to give vulnerability data and proofs for the confirmation of vulnerability causes and hazards;

b) the to-be-confirmed: security vulnerabilities are reported by their discoverer to manufacturers or vulnerabilities management organizations, having vulnerability analysis reports or scenarios in which vulnerabilities can be recurred.

c) the confirmed: security vulnerabilities confirmed or issued by vulnerability discoverers, users or manufacturers, having relevant information including identification and description.

5.2.3.3 Utilization stage

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------