GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/T 30279-2020

Replacing GB/T 30279-2013; GB/T 33561-2017

Information security technology - Guidelines for categorization and classification of cybersecurity vulnerability

信息安全技术 网络安全漏洞分类分级指南

Issued on: November 19, 2020 **Implemented on: June 01, 2021**

Issued by: State Administration for Market Regulation;
Standardization Administration of PRC.

Table of Contents

Information security technology - Guidelines for categorization and classification of cybersecurity vulnerability

1 Scope

This standard provides categorization methods and classification indicators for network security vulnerabilities (hereinafter referred to as "vulnerabilities"); gives suggestions for classification methods.

This standard applies to the categorization of vulnerability and evaluation of hazard level, which are carried out by the network product and service providers, network operators, vulnerability collection organizations, vulnerability emergency organizations, in the process of relevant activities, such as vulnerability management, product production, technology research and development, network operations, etc.

2 Normative references

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) is applicable to this standard.

GB/T 20984 Information security technology - Risk assessment specification for information security

GB/T 25069 Information security technology - Glossary

GB/T 28458 Information security technology - Cybersecurity vulnerability identification and description specification

GB/T 30276 Information security technology - Specification for cybersecurity vulnerability management

3 Terms and definitions

The terms and definitions, as defined in GB/T 25069, GB/T 20984, GB/T 28458, GB/T 30276, as well as the following terms and definitions, apply to this document.

3.1

implementation, during the code development process of network products and services.

5.2.2 Resource management errors

This type of vulnerability refers to a vulnerability, which is resulting from the mismanagement of system resources (such as memory, disk space, files, CPU usage, etc.).

5.2.3 Input validation errors

5.2.3.1 Overview

This type of vulnerability refers to a vulnerability, which is caused by the lack of proper validation of the input data.

5.2.3.2 Buffer area errors

This type of vulnerability refers to the lack of correct boundary data validation, when performing operations on memory, resulting in incorrect read and write operations to other associated memory locations, such as buffer overflow, heap overflow, etc.

5.2.3.3 Injection

5.2.3.3.1 Overview

This type of vulnerability refers to the error in parsing or interpretation, which is caused by the lack of correct validation of user input data, during the operation of constructing commands, data structures, or records through user input, resulting in unfiltered or incorrectly filtered out special elements.

5.2.3.3.2 Formatted string errors

This type of vulnerability refers to the vulnerability, which is caused by the lax filtering of parameter type and quantity, when receiving an external formatted string as a parameter.

5.2.3.3.3 Cross-site scripting

This type of vulnerability refers to a vulnerability in WEB applications, that provides incorrect code execution to other clients, due to the lack of correct validation of client data.

5.2.3.3.4 Command Injection

This kind of vulnerability means that in the process of constructing executable commands, the wrong executable commands are generated, due to improper filtering of special elements in them.

5.2.3.3.5 Code injection

This kind of vulnerability means that in the process of constructing code segments through external input data, the special elements in them are not correctly filtered, resulting in the generation of wrong code segments and modifying the expected execution control flow of network products and services.

5.2.3.3.6 SQL injection

This type of vulnerability refers to the lack of validation of the external input data, that constitutes the SQL statement, in database-based applications, resulting in the generation and execution of wrong SQL statements.

5.2.3.4 Path traversal

This type of vulnerability refers to failure to properly filter resources or special elements in file paths, resulting in access to locations outside of restricted directories.

5.2.3.5 Backlinks

This type of vulnerability means that when accessing a file using a file name, the wrong file path is accessed, because the file name of a link or a shortcut representing an unexpected resource is not properly filtered.

5.2.3.6 Cross-site request forgery

This kind of vulnerability refers to that -- in WEB applications, due to insufficient validation of whether the request comes from a trusted user, the deceived client sends an unexpected request to the server.

5.2.4 Numeric errors

This type of vulnerability refers to the integer overflow, sign error and other vulnerabilities, which are caused by incorrect calculation or conversion of the generated numbers.

5.2.5 Competition condition problems

This kind of vulnerability refers to the security problem, which is caused by another piece of code that can concurrently modify the shared resource in the same time window, when a piece of concurrent code needs to access the shared resource mutually exclusive in the concurrent running environment.

5.2.6 Processing logic errors

Such vulnerabilities are caused by problems in processing logic implementation or incomplete branch coverage during the design and implementation process.

5.4.2.1 Overview

This type of vulnerability refers to the vulnerability in which the information of the affected components is obtained without authorization, due to configuration errors during operation.

5.4.2.2 Log information disclosure

This type of vulnerability refers to information disclosure, which is caused by abnormal output of log files.

5.4.2.3 Debug information disclosure

This type of vulnerability refers to information disclosure, which is caused by debugging information output during operation.

5.4.2.4 Side channel information disclosure

This type of vulnerability refers to information disclosure, which is caused by changes in side-channel information, such as power consumption, electromagnetic radiation, I/O characteristics, computing frequency, time consumption.

5.4.3 Fault injection

This type of vulnerability refers to a security issue, that is triggered by changing the operating environment (such as temperature, voltage, frequency, etc., or by injecting strong light), which may cause errors in code, system data, or execution.

5.5 Others

The vulnerability cannot be categorized into any of the above categories at this time, or there is insufficient information to classify it, meanwhile the details of the vulnerability are not specified.

6 Classification of network security vulnerabilities

6.1 Overview

According to the different scenarios of vulnerability classification, the classification of network security vulnerability is divided into two methods: technical classification and comprehensive classification. Each classification method includes four grades: super-risk, high-risk, medium-risk, low-risk. Among them, the technical classification reflects the degree of vulnerability hazard of a specific product or system; it is used to divide the vulnerability hazard grade from a technical point of view; it is mainly for

6.3 Classification method for network security vulnerabilities

6.3.1 Overview

The classification of network security vulnerabilities refers to the description of the degree of potential harm of network security vulnerabilities in a classification manner, including two classification methods: technical classification and comprehensive classification. Each classification method is divided into four levels: Ultra-critical, high-critical, medium-critical, low-critical, as follows:

- Ultra-critical: Vulnerabilities can easily cause particularly serious consequences to the target object;

- High-critical: Vulnerabilities can easily cause serious consequences to the target object;

- Medium-critical: Vulnerability can cause normal consequences to the target object, OR more difficult to cause serious consequences to the target object;

- Low-critical: Vulnerabilities can cause mild consequences to the target object, moderately difficult consequences to the target object, or very difficult consequences to the target object.

The vulnerability classification process mainly includes three steps: initial index assignment, intermediate index classification, final classification calculation. Among them, the index assignment is the manual assignment of each vulnerability classification index, according to the specific vulnerability. The index classification is classification of the three indexes of exploitation, influence degree, environmental factors. The classification calculation is based on the index classification calculation to generate the result of technology classification or comprehensive classification; the technology classification result is calculated by the two index categories of exploitation and influence degree; the comprehensive classification is calculated by three index categories of exploitation, influence degree, environmental factors. The vulnerability classification process is as shown in Figure 2.

where the vulnerability is located, the technical level at which the current vulnerability is exploited, that need to be considered when classifying the vulnerability. The classification of environmental factors reflects the degree of harm of vulnerabilities in the reference environment. The combination of different values of each index, in the environmental factor index group, corresponds to different environmental factor levels. The levels of different environmental factors are divided into 9 levels, which are represented by numbers from 1 to 9; the greater the value, the higher the degree of vulnerability caused by environmental factors, as shown in Appendix C.

6.3.3 Technology classification of network security vulnerabilities

The technical classification of network security vulnerabilities is divided into four levels: ultra-critical, high-critical, medium-critical, low-critical. The technology classification of network security vulnerability is determined by the two index categories of exploitability and influence degree. The higher the exploitability possibility (the higher the exploitability classification) and the more serious of the influence degree (the higher the classification of influence degree), the higher the level of vulnerability technology classification (the higher the hazard of vulnerability). The vulnerability technology classification method is as follows:

- First, assign a value to the exploitability index; calculate the vulnerability exploitability classification, according to Appendix A, based on the assignment result;

- Then, assign a value to the influence degree indicators; calculate the influence degree classification, according to Appendix B based on the assignment results;

- Finally, according to the classification results of the degree of exploitation and influence, based on Appendix D, calculate the technical classification of network security vulnerabilities.

6.3.4 Comprehensive classification of network security vulnerabilities

The comprehensive classification of network security vulnerabilities is divided into four levels: ultra-critical, high-critical, medium-critical, low-critical. The comprehensive classification of network security vulnerabilities is determined by three index categories: exploitability, influence degree, environmental factors. The higher the exploitability possibility of vulnerability (the higher the exploitability level), the higher the influence degree (the higher the classification of influence degree), the more sensitive to the influence of vulnerabilities (the higher the classification of environmental factors), the higher the level of comprehensive vulnerability classification (the greater the hazard of vulnerability). The comprehensive classification method of vulnerability is as follows:

- First, perform technical classification on the vulnerabilities; assign values to the exploitability indicators, according to the aforementioned vulnerability technical

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

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