GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/T 28458-2020

Replacing GB/T 28458-2012

Information Security Technology - Cybersecurity Vulnerability Identification and Description Specification

信息安全技术

网络安全漏洞标识与描述规范

Issued on: November 19, 2020 **Implemented on: June 1, 2021**

Issued by: State Administration for Market Regulation;

Standardization Administration of the People's Republic of China.

Table of Contents

Information Security Technology - Cybersecurity Vulnerability Identification and Description Specification

1 Scope

This Standard specifies the identification and description information of cybersecurity vulnerability (hereinafter referred to as “vulnerability”).

This Standard is applicable to all relevant parties engaged in activities, such as: vulnerability release and management, vulnerability database construction, product production, research and development, evaluation and network operation, etc.

2 Normative References

The following documents are indispensable to the application of this document. In terms of references with a specified date, only versions with a specified date are applicable to this document. In terms of references without a specified date, the latest version (including all the modifications) is applicable to this document.

GB/T 7408-2005 Data Elements and Interchange Formats - Information Interchange - Representation of Dates and Times

GB/T 25069 Information Security Technology - Glossary

GB/T 30276-2020 Information Security Technology - Specification for Cybersecurity Vulnerability Management

GB/T 30279-2020 Information Security Technology - Guidelines for Categorization and Classification of Cybersecurity Vulnerability

3 Terms and Definitions

What is defined in GB/T 25069, GB/T 30276-2020 and GB/T 30279-2020, and the following terms and definitions are applicable to this document.

3.1 Cybersecurity Vulnerability

Cybersecurity vulnerability refers to a defect or weak point that is unintentionally or intentionally generated during the process of demand analysis, design, implementation, configuration, testing, operation and maintenance of network products and services, and may be exploited.

other than fixed fields, for example, an alternative name of the vulnerability.

Example:

GNU Bash. high risk. remote code execution vulnerability. shell break vulnerability

5.3.2 Release time

The date that the vulnerability information was released. Date writing shall adopt the extended format of complete representation in 5.2.1.1 of GB/T 7408-2005. The format is: YYYY-MM-DD, for example, 2019-01-01. Among them, YYYY signifies a calendar year; MM signifies the ordinal number of the calendar month in the calendar year; DD signifies the ordinal number of the calendar day in the calendar month.

5.3.3 Releaser

The abbreviation of "vulnerability releaser", which is an individual or organization that releases validated vulnerability information. The releaser is named after its personal identification or organization name. The "organization name" can be the official name or short name of the releaser's organization. If the vulnerability releaser is an individual, it may be named with the name of the organization, to which, it belongs. See the format below:

Personal identification of vulnerability releaser (vulnerability releaser's organization name)

Multiple releasers are allowed, which are separated by commas, for example:

Zhang San (organization A), Li Si (organization A, organization B), Wang Wu, organization C

The vulnerability release shall comply with the requirements specified in 5.5 Vulnerability Release in GB/T 30276-2020.

5.3.4 Validator

The abbreviation of "vulnerability validator", which is an individual or organization that technically validates the existence, level and category of vulnerabilities. The validator is named after its personal identification or organization name. The "organization name" can be the official name or short name of the validator's organization. If the vulnerability validator is an individual, it may be named with the name of the organization, to which, it belongs. See the format below:

Personal identification of vulnerability validator (vulnerability validator's organization name)

Multiple validators are allowed, which are separated by commas, for example:

Zhang San (organization A), Li Si (organization A, organization B), Wang Wu, organization C

The vulnerability validation shall comply with the requirements specified in 5.3 Vulnerability Validation in GB/T 30276-2020.

5.3.5 Finder

The abbreviation of "vulnerability finder", which is an individual or organization that finds the vulnerability. The finder is named after its personal identification or organization name. The "personal identification" can be the name or code of the individual finder; the "organization name" can be the official name or short name of the finder's organization. If the identity of the finder cannot be confirmed, or the vulnerability information was anonymously released, the finder can be identified as "anonymous". If the vulnerability finder is an individual, it may be named with the name of the organization, to which, it belongs. See the format below:

Personal identification of vulnerability finder (vulnerability finder's organization name)

Multiple finders are allowed, which are separated by commas, for example:

Zhang San (organization A), Li Si (organization A, organization B), Wang Wu, organization C

The vulnerability finding shall comply with the requirements of 5.1 a) in GB/T 30276-2020.

5.3.6 Category

The category, to which, the vulnerability belongs. It provides information on the attribution of vulnerability classification. The classification of categories shall comply with the requirements specified in Chapter 5 Cybersecurity Vulnerability Classification of GB/T 30279-2020.

5.3.7 Level

The vulnerability hazard level, which provides the extent of hazard that the vulnerability may cause. The classification shall comply with the requirements specified in 6.3.3 Technical Classification of Cybersecurity Vulnerabilities in GB/T 30279-2020.

5.3.8 Affected product or service

Details of the product or service, in which, the vulnerability exists. It includes supplier, name and version No., etc. For vulnerabilities with shared middleware or components, the related products or service information affected by them can all be listed.

5.3.9 Relevant number

The number of the same vulnerability in different organizations, for example, CNVD number, CNNVD number, CVE number or vulnerability number customized by other organizations, etc. If there are multiple numbers, they can be provided in sequence and separated by commas. See Appendix A for the XML representation method of relevant number.

5.3.10 Existence statement

Describe the triggering conditions, generation mechanism or conceptual proof of the vulnerability.

Appendix A

(informative)

XML Representation of an Example of Vulnerability Identification and Description Specification

This Appendix provides an example of a vulnerability (non-real vulnerability) using the vulnerability identification and description specified in this Standard. The purpose is to demonstrate the application of this Standard. In order to ensure the conciseness and readability of the example, this Appendix adopts the XML language as the representation language.

〈? xml version＝"1.0" encoding＝"UTF-8" ?〉
〈cncvd_items〉

<identification No.> CNCVD-2020-101001</identification No.>

<name> Linux Kernel. high risk. race condition vulnerability. Dirty Cow II vulnerability </name>

<release time> 2020-10-10 </release time>

<releaser> National Computer Network Emergency Response Technical Team / Coordination Center of China </releaser>

<validator>

China Information Technology Security Evaluation Center, National Research Center for Information Technology Security

</validator>

<finder> National Computer Network Intrusion Prevention Center </finder>

<category> race condition vulnerability </category>

<level> high risk </level>

<affected product or service>

<manufacturer> Debian </manufacturer>

<product or service information>

<product or service name> debian_linux </product or service name>

<version No.> 7.0 </version No.>

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

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