GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/T 30276-2020

Replacing GB/T 30276-2013

Information security technology - Specification for cybersecurity vulnerability management

信息安全技术 网络安全漏洞管理规范

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

Issued by: State Administration for Market Regulation;
Standardization Administration of the People's Republic of China.

Table of Contents

Information security technology - Specification for cybersecurity vulnerability management

1 Scope

This Standard specifies the management process, management requirements and verification methods for each stage of the cybersecurity vulnerability management process (including vulnerability discovery and report, receipt, verification, disposal, release, tracking).

This Standard applies to cybersecurity vulnerability management activities that are carried out by provider of network products and services, network operator, vulnerability repository organization, and vulnerability emergency response organization.

2 Normative references

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

GB/T 25069, Information security technology - Glossary

GB/T 28458-2020, Information security technology - Cybersecurity vulnerability identification and description specification

GB/T 30279-2020, Information security technology - Guidelines for categorization and classification of cybersecurity vulnerability

3 Terms and definitions

Terms and definitions determined by GB/T 25069, GB/T 28458-2020 and the following ones are applicable to this document.

3.1 User

Individuals or organizations that use network products and services.

3.2 Provider of network products and services

Individuals or organizations that provide network products and services.

5 Cybersecurity vulnerability management requirements

5.1 Vulnerability discovery and report

During the vulnerability discovery and report stage, the requirements are as follows:

a) Requirements for vulnerability discoverers:

-- Under the premise of following relevant national laws and regulations, use manual or automatic methods to detect and analyze the vulnerability, and verify the authenticity of the vulnerability;

-- When implementing vulnerability discovery activities, the user's system operation and data security shall not be affected or damaged; there shall be no behavior that violates the business operation and data security of other organizations in order to discover vulnerabilities;

-- When identifying potential vulnerabilities of network products or services, proactively assess possible security risks;

-- Effective measures shall be taken to prevent leakage of vulnerability information.

b) Requirements for vulnerability reporters:

-- After discovering vulnerabilities in the network or products and services, the vulnerability information shall be reported in time;

-- When reporting vulnerabilities, the vulnerabilities shall be described objectively and truthfully.

5.2 Vulnerability receipt

In the vulnerability receipt stage, the requirements are as follows:

a) Vulnerability reports shall be provided with vulnerability receiving channels, such as websites, emails or telephones; measures shall be taken to ensure the security and confidential receipt of vulnerability information;

b) A vulnerability receipt strategy shall be formulated and publicly released, to facilitate vulnerability reporters to report vulnerabilities. The receipt strategy includes but is not limited to vulnerability receipt range, vulnerability receipt channel, vulnerability receipt requirements, vulnerability receipt process;

-- If the reported vulnerability is found in a product or service that the provider or network operator does not currently provide support, the provider or network operator shall continue to complete the investigation and vulnerability verification, and confirm the impact of the vulnerability on other supported products or online services.

b) If it is the vulnerability repository organization that performs the verification:

-- After confirming that the vulnerability is received, coordinate the verification of the vulnerability information in a timely manner. The coordination method may include: inform the provider of the product or service that is related to the vulnerability to verify and confirm; jointly perform verification and confirmation with the provider or network operator who is associated with the vulnerability; work with the vulnerability reporter to jointly verify and confirm the vulnerability information;

-- Reflect the vulnerability objectively and truthfully; do not mislead the provider or network operator, vulnerability reporter who is associated with the vulnerability;

-- After verification, notify the provider or network operator who is associated with the vulnerability in time.

c) If it is the vulnerability emergency response organization that performs the verification:

-- After confirming that the vulnerability is received, coordinate the verification of the vulnerability information in a timely manner. The coordination method may include: inform the provider of the product or service who is related to the vulnerability to verify and confirm; jointly perform verification and confirmation with the provider or network operator who is associated with the vulnerability;

-- After verification, notify the provider or network operator who is associated with the vulnerability in time.

d) When the following situations occur during the vulnerability verification process, terminate the subsequent vulnerability management stage; feedback to the vulnerability reporter:

-- Repeated vulnerability: The vulnerability is a repeated vulnerability, a resolved or fixed vulnerability;

-- Unverifiable vulnerability: The vulnerability is a vulnerability that cannot be verified by the provider, network operator, vulnerability repository organization;

-- Inform the vulnerability reporters and users of the disposal measures of the vulnerability in a timely manner; report to the vulnerability emergency response organization when necessary;

-- Effective ways and convenient conditions shall be provided for users to obtain patches, upgraded versions and temporary disposal suggestions;

-- Necessary technical support shall be provided to the affected users to support them to complete the vulnerability repair;

-- The deeper reasons for the vulnerability should be investigated, to determine whether other products or services have the same or similar vulnerabilities.

b) Requirements for the vulnerability repository organization:

-- Cooperate with the vulnerability emergency response organization and relevant network product providers and network operators to carry out vulnerability disposal work;

-- Maintain an objective and accurate attitude in the process of vulnerability disposal; timely share the verified vulnerability information with providers, network operators, and vulnerability emergency response organizations who are associated with the vulnerability;

-- Provide vulnerability disposal suggestions and related technical support to providers, network operators who are associated with the vulnerability;

-- Corresponding necessary measures shall be taken to protect the security and confidentiality of the information that is related to the reported vulnerability and to prevent the information from leaking and being used by others.

c) Requirements for the vulnerability emergency response organization:

-- Coordinate and supervise the vulnerability disposal work; feedback the vulnerability attribution, vulnerability disposal and other disposal suggestions to the relevant vulnerability receivers.

-- Supervise and urge providers and network operators who are associated with the vulnerability to take timely vulnerability repair or preventive measures, so as to prevent cybersecurity threats which are caused by the large-scale use of the vulnerability;

-- Work with providers or network operators who are associated with the vulnerability to perform continuous tracking of the vulnerability disposal

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

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