ICS 35.030
CCS L80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 43741-2024

Cybersecurity technology - Requirements for crowdsourcing security test services

网络安全技术 网络安全众测服务要求

Issued on: April 25, 2024 **Implemented on: November 1, 2024**

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

Table of Contents

Foreword

This document is in accordance with the provisions of GB/T 1:1-2020 "Guidelines for standardization work Part 1: Structure and drafting rules for standardization documents" Drafting: Please note that some of the contents of this document may involve patents: The issuing organization of this document does not assume the responsibility for identifying patents: This document was proposed and coordinated by the National Cybersecurity Standardization Technical Committee (SAC/TC260): This document was drafted by: National Computer Network Emergency Response Technical Coordination Center, China Electronics Technology Standardization Institute, National Information Technology Security Research Center, Alibaba Cloud Computing Co:, Ltd:, Qi'anxin Wangshen Information Technology (Beijing) Co:, Ltd:, China Mobile Communications Group Group Co:, Ltd:, Institute of Software, Chinese Academy of Sciences, Shanghai Douxiang Information Technology Co:, Ltd:, Beijing Topsec Network Security Technology Co:, Ltd:, China Unicom Consulting and Design Institute Co:, Ltd:, Shanghai Wenyu Information Technology Co:, Ltd:, Ant Technology Group Co:, Ltd:, Hangzhou Anheng Information Technology Co:, Ltd:, Beijing Municipal Government Security Assurance Center (Beijing Information Security Evaluation Center), Beijing Eastern Network Information Technology Co:, Ltd: Company, Beijing Zhongan Tianxia Technology Co:, Ltd:, Beijing Qihoo Technology Co:, Ltd:, China Industrial Internet Research Institute, Venusstar Information Technology Group Co:, Ltd:, Beijing Digital Stargazing Technology Co:, Ltd:, and China Electronics Technology Network Information Security Co:, Ltd: The main drafters of this document are: Yun Xiaochun, Wang Wenlei, Geng Dongmei, Liu Xiangang, Zhang Dajiang, Shu Min, Sun Yan, Yang Chen, Gao Jiming, Wang Hong, Yan Hanbing, He Nengqiang, Dong Hang, Wang Huili, Deng Pingping, Yu Bin, Cui Tingting, Li Yuan, Hu Ming, Wang Junjie, Guo Liang, Yan Hongshi, Wang Yan, Qiu Qin, Zuo Min, Hu Xiaona, Zha Qiwen, Zhang Qi, Yang Wei, Li Xunan, Yan Dingyu, Wu Junyu:

Article 27 of the Cybersecurity Law of the People's Republic of China stipulates that "no individual or organization shall engage in illegal intrusion into other people's networks, Disrupting the normal function of other people's networks, stealing network data, and other

activities that endanger network security; not providing devices specifically used to invade networks, interfere with networks This document is in compliance with relevant national regulations: Based on the corresponding laws, regulations and technical standards, this paper proposes a network Network security crowd testing service requirements: Cybersecurity Technology Cybersecurity Crowd Testing Service Requirements

1 Scope

GB/T 43741-2024 sets the requirements for crowdsourced security testing services - bug bounty and public testing platforms, on which an organisation invites a body of independent testers to attack its systems. The arrangement is useful and legally delicate: in China unauthorised testing is a criminal act, so the scope, the authorisation and the conduct of the testers have to be documented precisely, and the vulnerabilities found are themselves sensitive material that must not leak while they are being fixed. The standard sets the roles and responsibilities, the service process and the security risks, then the service requirements at each stage: the preparation phase, the implementation phase and the post-processing phase, with an informative annex on the functions of a crowdsourced testing platform and a normative annex giving the code of conduct for authorised testers. It took effect on 1 November 2024.

This document describes the roles and responsibilities, service processes, and security risks of the network security crowd testing service, and specifies the service requirements: This document applies to network security crowd-testing service activities:

2 Normative references

The contents of the following documents constitute the essential clauses of this document through normative references in this document: For referenced documents without a date, only the version corresponding to that date applies to this document; for referenced documents without a date, the latest version (including all amendments) applies to This document:

GB/T 25069-2022 Information Security Technical Terminology

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

GB/T 30276-2020 Information security technology network security vulnerability management specification

GB/T 35273 Information security technology Personal information security specification

3 Terms and definitions

The terms and definitions defined in GB/T 25069-2022 and GB/T 28458-2020 and the

following apply to this document: 3:

1 Organize non-specific individuals or organizations in a crowdsourcing and voluntary manner to conduct security tests such as vulnerability discovery on network products and systems the process of:

Note 1: The network security crowd testing service complies with the relevant national vulnerability management regulations:

Note 2: The cybersecurity crowd-testing service for critical information infrastructure is carried out under the guidance of the cybersecurity authorities and protection departments: 3:

2 Organizations that need cybersecurity crowd-testing services (3:1):

Note: The crowd test demander has the ownership of the test object, signs an authorized test agreement with the crowd test organizer (3:3), and authorizes the crowd test organizer to organize the authorized test: Party (3:4) carries out network security crowd testing services (3:1): 3:

3 Under the authorization of the crowd testing demander (3:2), organize authorized testers (3:4) that meet the requirements of the crowd testing demander to carry out network security crowd testing services (3:1) organization: 3:

4 Authorized test entity authorizedtestentity A natural person or organization that has been authorized by the crowd testing organizer (3:3) to conduct security testing on the test object: 3:

5 An organization that conducts audits and oversight during the cybersecurity crowd-testing service (3:1):