ICS 43.020
CCS T 40

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 45496-2025

Motor vehicle product recall - Guidelines for information defect assessment

汽车产品召回 信息缺陷评估指南

Issued on: March 28, 2025 **Implemented on: March 28, 2025**

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 Technical Committee for Product Defects and Safety Management Standardization (SAC/TC463).

This document was drafted by: State Administration for Market Regulation Defective Product Recall Technology Center, Huawei Technologies Co., Ltd., China Automotive Industry Corporation China Automotive Engineering Research Institute Co., Ltd., China Society of Automotive Engineers, China Automotive (Beijing) Intelligent Connected Vehicle Research Institute Co., Ltd., Guangzhou Xiaopeng Motors Technology Co., Ltd., Tsinghua University, Zhejiang Tsinghua Yangtze River Delta Research Institute, Beijing China Automotive Research Institute Technology Co., Ltd., China Automotive Data Co., Ltd., Yutong Beijing Automobile Co., Ltd., Geely Automobile Group Co., Ltd., Beijing Mercedes-Benz Sales and Service Co., Ltd., Beijing Ideal Automobile Co., Ltd. company.

The main drafters of this document are: Li Yan, Dong Honglei, Xiao Lingyun, Tan Yuhan, Xia Guoqiang, Liang Xinmiao, Li Wenzhao, Xi Ming, He Xing, Zhang Yanan, Chen Guihua, Fang Rui, Ding Xu, Gao Yongqiang, Feng Yongqin, Zhang Heng, Qu Xianguo, Ren Yi, Sun Yingce, Peng Jianfen, Huang Rong, Liu Yahui, Wang Jian, Peng Yamin, Chen Jie, Shi Yan, Zhou Fanhua, Ma Chao, Guo Zhen, Yu Mingming, Ma Tao, Wang Peng, Chen Yupeng, and Wu Shengnan.

Introduction

With the cross-border integration of artificial intelligence, information communication and automotive technology, cars are no longer isolated electromechanical units, but have become an important part of the intelligent ecosystem.

As a carrier, cars have gradually evolved from information-isolated means of transportation to a digital space that integrates travel, entertainment, and services.

Security and information security risks are intertwined and superimposed, making the security situation more complex and severe.

The information security risks faced by automobiles come from "cloud-pipe-end-external links", namely cloud platforms, network transmission, vehicles and related external equipment.

Cloud platform information security risks include malicious theft and tampering of data by hackers, illegal access to sensitive data, etc. Network transmission security risks include But not limited to. 1) Transmission risk, sending wrong information; 2) Authentication risk, impersonating the identity of the verifier through identity forgery, dynamic hijacking, etc.

Information; 3) Protocol risk, attackers use false information to induce vehicle misjudgment. Vehicle-side information security risks include but are not limited to. 1) Software and hardware system

1) System security, such as exploiting vulnerabilities to attack vehicles; 2) Key security, such as attackers obtaining control information through plug-in debugging and reverse analysis, using scripts Control the vehicle through a digital key; 3) Architecture security, such as

controlling the vehicle's electronic control unit (ECU) through a controller area network (CAN).

The security of externally linked devices includes, but is not limited to, risks caused by vulnerabilities in external ecological components such as manipulating apps and charging piles.

If there is a loophole in any link of the "link", it may affect driving safety, so automobile information defects need to be considered comprehensively from the perspective of system ecology.

Guidelines for evaluating automotive product recall information defects

1 Scope

This document provides recommendations for the evaluation of automotive product information defects, and outlines the evaluation process, evaluation and defect identification, and the handling of evaluation results.

This document is applicable to automobile manufacturers, parts manufacturers, system suppliers, data service providers, network operators, product recall The recall authorities, product recall technical institutions and other entities conduct defect analysis and defect judgment on the loopholes of the "cloud-pipe-end-external link" system of in-use vehicles.

Determination, risk warning and emergency response.

2 Normative references

GB/T 25069

GB/T 34402-2017

GB/T 40914

GB/T 43387

GB 44495

3 Terms and definitions

The terms and definitions defined in GB/T 25069, GB/T 43387, GB 44495 and the following apply to this document.

3.1 Information defect informationdefect

The vulnerability (3.3) in the cloud-pipe-end-external link system (3.2) was exploited, resulting in the same model, batch or category of vehicle products being Common situations that do not meet national standards or industry standards for protecting personal

and property safety, or other situations that endanger personal safety (3.5), property Unreasonable risk to safety (3.6).

3.2 Cloud-channel-device-linksystem

A distribution layer system consisting of vehicle application environment and related information.

Note 1."Cloud" refers to a network information service carrier, a layer system with connection management, capability exposure, data management and multi-business support capabilities.

Note 2."Pipeline" refers to the layer system of network information transmission, including vehicle-mounted cellular network communication, LTE-V2X and 802.11p direct wireless communication.

Note 3."End" refers to the network information application layer system, including vehicles and roadside facilities, automotive electronics, vehicle-mounted terminals and operating systems and other vehicle-related "end" layers.

Note 4."External links" refer to external ecological components such as control applications and charging piles required for vehicle use.

3.3 Vulnerability

A weakness in an asset or mitigation measure that can be exploited by one or more threats (3.4) [Source. GB 44495-2024, 3.6]