ICS 43.020
CCS T40

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 44774-2024

Specifications of emergency response management for vehicle cybersecurity

汽车信息安全应急响应管理规范

Issued on: October 26, 2024 **Implemented on: October 26, 2024**

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

Table of Contents

1 Scope

GB/T 44774-2024 sets the management process for vehicle cybersecurity emergency response. A vulnerability in a car is unlike one in a server: the fleet is in the hands of the public, a fix must be delivered over the air or through workshops to vehicles that may be moving, and a mistaken patch can be as dangerous as the flaw. Chinese regulation now requires manufacturers to have this capability, and the standard describes what it consists of. It sets the overall architecture and then the phases: preparation, verification, response, remediation and post-incident handling, with the roles, decisions and records belonging to each, and informative annexes giving an example of the emergency response process with its associated documents and the grading of both the response and the incident. It took effect on 26 October 2024.

This document establishes the management process for the emergency response for vehicle cybersecurity and describes the relevant management methods. This document applies to vehicle cybersecurity emergency response management conducted by relevant organizations, including all phases of preparation, verification, response, remediation and post-incident handling.

2 Normative References

This document does not have normative references.

3 Terms and Definitions

The following terms and definitions are applicable to this document.

3.1 vehicle cybersecurity A state in which a vehicle's electronic and electrical systems, assemblies and functions, so that its assets are protected from threats. [Source: GB/T 40861-2021, 3.1]

3.2 vehicle cybersecurity incident A single or multiple identified vehicle cybersecurity states in a vehicle that may compromise an organization's assets or operations. NOTE. a cybersecurity state indicates a potential cybersecurity breach or the occurrence of a certain control failure.

3.3 emergency response plan An organization's policies and procedures for maintaining or recovering business operations, including information system operations, in response to emergent / significant cybersecurity incidents. [Source: GB/T 24363-2009, 3.5]

3.4 emergency response for vehicle cybersecurity Preparatory work undertaken by organizations, such as vehicle manufacturers, suppliers and other stakeholders, to respond to emergent vehicle cybersecurity incidents; measures taken after the occurrence of an incident (excluding unrelated work and measures within the suppliers and other stakeholders); and post-incident assessment, tracking and summary.

3.5 stakeholder Individuals or organizations that may be affected or aware of potential impacts due to adverse consequences or unfavorable outcomes resulting from a violation of one or multiple cybersecurity attributes (such as confidentiality, integrity and availability, etc.) of one or a group of assets.

3.6 organization Individuals or collectivities with their own responsibilities, authority, and relationships to achieve their objectives. NOTE. the concept of organization includes, but is not limited to, sole proprietors, companies, legal persons, commercial firms, enterprises, institutions, partnerships, charities or academies, or any part or combination thereof, whether incorporated or unincorporated, public or private. [Source: GB/T 20984-2022, 3.1.3]

4 Overall Architecture Diagram

The overall architecture of each phase of this document is shown in Figure 1.A complete example of the emergency response process is shown in A.1 of Appendix A.

5 Preparation Phase

5.1 Overview Organize and complete the preparation and revision of emergency response plans during this phase, including formulating emergency response plans, establishing roles and responsibilities, completing training, drills, management and updates of emergency response plans, formulating cybersecurity incident classification and grading specifications, and formulating and distributing cybersecurity emergency response operation manuals. Furthermore, a coordination and cooperation mechanism with relevant external organizations is established during this phase. NOTE. the cybersecurity emergency response operation manuals are independently formulated by the organization to guide specific technical operations within and outside the organization during the emergency response process.

5.2 Formulation of Emergency Response Plan

5.2.1 The emergency response plan shall clearly specify at least the following contents.

a) Roles and responsibilities;

b) Emergency response process;

c) Timelines for each process in the verification phase, response phase, remediation phase, and post-incident handling phase. In accordance with different emergency response levels, formulate different timelines. For the classification of emergency response levels, see B.1 in Appendix B;

d) Other relevant forms and attachments, etc.

5.2.2 The emergency response plan shall be based on the organization's specific circumstances and business characteristics and shall be operable.

5.2.3 When formulating emergency response plans, participants shall adhere to the following principles.

a) Confidentiality. emergency response information shall not be provided or disclosed to unauthorized individuals, entities or process.

b) Standardization. when formulating emergency response plans, adhere to the organization's relevant cybersecurity management system.

c) Minimum impact. the emergency response plan covers the minimum set of tasks required to complete the objective of emergency response.

5.3 Establishment of Roles and Responsibilities

5.3.1 Role division The organization shall establish a cybersecurity emergency response operating mechanism in conjunction with its daily organizational structure and clearly define its responsibilities. The requirements are as follows:

a) If one person assumes multiple responsibilities, or if multiple people assume a single responsibility, the emergency response plan document shall clearly define the mapping relationships between personnel and responsibilities. The order of personnel replacement for a single responsibility shall also be clearly defined.

b) The emergency response operating mechanism shall be composed of management, business, technical, and administrative support personnel, etc. Based on their roles, it can be divided into five functional groups. the emergency response leadership group, the emergency response expert group, the emergency response implementation group, the emergency response technical support group, and the emergency response daily operation group. Personnel shall be assigned to these groups based on their skills and knowledge. Personnel assigned to these groups should be responsible for the same or similar tasks in their daily work. Among these five functional groups, the organization shall at least set up emergency response leadership group, emergency response implementation group (incorporating the responsibilities of the expert group), and emergency response daily operation group (incorporating the responsibilities of the technical support group). In accordance with its own business characteristics and organizational structure, the organization may set up other groups (with self-defined names), but the relevant responsibilities shall be complete.

c) The organization may hire external experts with corresponding qualifications to assist with the emergency response or entrust an external institution with corresponding qualifications to undertake part of the work of the implementation group and the daily operation group. When hiring external experts or delegating tasks to external institutions, relevant agreements (such as confidentiality agreements, service level agreements and service continuity agreements) shall be signed with them.

d) Each functional group for emergency response shall clearly define its internal division of labor and responsibilities, and each group shall have a person in charge of overall coordination.

5.3.2 Establishment of the responsibilities of each functional group

5.3.2.1 Emergency response leadership group The emergency response leadership group serves as the leading body for cybersecurity emergency response and shall be led by a member of the organization's top management. The leadership team is responsible for leading and making decisions on major matters of cybersecurity emergency response. The requirements are as follows: