ICS 43.020
CCS T 40

中华人民共和国国家标准

GB/T 45496—2025

汽车产品召回　信息缺陷评估指南

Motor vehicle product recall—Guidelines for information defect assessment

2025-03-28 发布　　2025-03-28 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国产品缺陷与安全管理标准化技术委员会(SAC/TC 463)提出并归口。

本文件起草单位：国家市场监督管理总局缺陷产品召回技术中心、华为技术有限公司、中国汽车工程研究院股份有限公司、中国汽车工程学会、国汽(北京)智能网联汽车研究院有限公司、广州小鹏汽车科技有限公司、清华大学、浙江清华长三角研究院、北京中汽院科技有限公司、中汽数据有限公司、宇通客车股份有限公司、吉利汽车集团有限公司、北京梅赛德斯-奔驰销售服务有限公司、北京理想汽车有限公司。

本文件主要起草人：李艳、董红磊、肖凌云、谭玉函、夏国强、梁新苗、李文昭、席明、贺兴、张亚楠、陈桂华、方锐、丁旭、高永强、冯永琴、张恒、曲现国、任毅、孙英策、彭建芬、黄嵘、刘亚辉、王剑、彭亚敏、陈杰、石岩、周凡华、马超、郭振、于明明、马涛、王澎、陈宇鹏、吴胜男。

引　言

随着人工智能、信息通信与汽车技术跨界融合，汽车不再是孤立的机电单元，成为智能生态系统重要载体，汽车逐渐由信息孤岛的交通工具发展成为集出行、娱乐、服务等为一体的数字空间。车辆运行安全和信息安全风险交织叠加，安全形势更加复杂严峻。

汽车面临的信息安全风险来自“云-管-端-外部链接”，即云平台、网络传输、车辆及相关的外部设备。云平台信息安全风险如黑客对数据恶意窃取和篡改、敏感数据被非法访问等。网络传输安全风险包括但不限于：1）传输风险，发送错误信息；2）认证风险，通过身份伪造、动态劫持等方式冒充验证者的身份信息；3）协议风险，攻击者通过伪信息诱导车辆误判。车辆端信息安全风险包括但不限于：1）软硬件系统安全，如利用漏洞攻击车辆；2）密钥安全，如攻击者通过插桩调试获取控制信息并逆向分析，利用脚本通过数字钥匙控制车辆；3）架构安全，如通过控制器局域网络（CAN）控制车辆电子控制单元（ECU）。外部链接设备安全包括但不限于操控 App、充电桩等外部生态组件漏洞引发的风险。“云-管-端-外部链接”任一环节存在漏洞，都可能影响行车安全，因此汽车信息缺陷需从系统生态角度综合考虑。

汽车产品召回　信息缺陷评估指南

1　范围

本文件提供了汽车产品信息缺陷评估的建议，给出了评估流程、评估与缺陷认定及评估结果处置。

本文件适用于汽车产品整车生产者、零部件生产者、系统供应商、数据服务商、网络运营商、产品召回主管部门、产品召回技术机构等主体对在用车辆“云-管-端-外部链接”系统漏洞进行缺陷分析、缺陷判定、风险预警与应急处置。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069　信息安全技术　术语

GB/T 34402—2017　汽车产品安全　风险评估与风险控制指南

GB/T 40914　汽车产品召回　预警规则

GB/T 43387　产品召回　术语

GB 44495　汽车整车信息安全技术要求

3　术语和定义

GB/T 25069、GB/T 43387、GB 44495 界定的以及下列术语和定义适用于本文件。

3.1

信息缺陷　information defect

因云-管-端-外部链接系统（3.2）存在的漏洞（3.3）被利用，导致同一型号、批次或类别的车辆产品中普遍存在的不符合保障人身、财产安全的国家标准、行业标准的情形或者其他危及人身安全（3.5）、财产安全（3.6）的不合理的危险。

3.2

云-管-端-外部链接系统　cloud-channel-device-link system

车辆应用环境和关联信息构成的分布层体系。

注 1：“云”指网络信息服务载体，具备连接管理、能力开放、数据管理多业务支持能力的层系。

注 2：“管”指网络信息传输的层系，包括车载蜂窝网络通信、LTE-V2X 和 802.11p 直连无线通信等。

注 3：“端”指网络信息应用层系，包括车辆和路侧设施、汽车电子、车载终端及操作系统等与车辆相关的“端”层系。

注 4：“外部链接”指车辆使用所需的操控应用程序、充电桩等外部生态组件。

3.3

漏洞　vulnerability

在资产或缓解措施中，可被一个或多个威胁（3.4）利用的弱点。

[来源：GB 44495—2024，3.6]