

《汽车产品召回 信息缺陷评估指南》

（征求意见稿）

编制说明

标准起草项目组

二〇二四年九月三十日

《汽车产品召回 信息缺陷评估指南》

国家标准编制说明

一、工作简况

1. 任务来源

根据《国家标准化管理委员会关于下达 2021 年第二批推荐性国家标准计划及相关标准外文版计划的通知》（国标委发[2021]23 号）要求，《汽车产品召回 信息缺陷评估指南》（计划号：20214324-T-469）由全国产品缺陷与安全管理标准化技术委员会（SAC/TC463）归口管理和组织制定，项目周期 24 个月。

2. 制定背景

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。据工业和信息化部车联网漏洞平台收录数据显示，自 2020 年以来，车联网漏洞收录量从 1200 余条增长至 3000 余条，影响规模也逐步达到了 3000 余万辆。这些漏洞可能对公众财产、人身安全造成极大威胁，甚至可造成大面积的交通事故，危害国家安全。

漏洞是必然存在的，但并不是所有漏洞都被定义为缺陷。本标准拟解决的问题是提出一种信息缺陷评估方法，用于判

定哪些漏洞将被定义为缺陷，需要通过召回方式解决。

3. 起草过程

2021 年 8 月，标准立项计划下达，国家市场监督管理总局缺陷产品召回技术中心（以下简称市场监管总局召回中心）面向行业征集起草单位和起草专家，并组建标准起草组；

2022 年 3 月，市场监管总局召回中心组织标准起草启动会，形成标准框架并组织专题研讨；

2023 年 3 月 29 日，起草组组织召开标准起草启动会，对草案中信息缺陷评估的基本要素、评估流程和评估结果处置要求等内容进行了深入研讨，确定标准草案修改思路及撰写任务分工；

2023 年 7 月，起草组组织中国汽研专家进行专题研讨，就漏洞可获取性、漏洞利用难易程度等级划分描述进行专题研讨；

2023 年 11 月，起草组组织华为技术有限公司专家进行专题研讨，就信息缺陷评估要素及漏洞可获取性、漏洞利用难易程度等级划分进行专题研讨；

2024 年 3 月 13 日，起草组组织标准闭门研讨会，参与企业深度讨论确定草案框架，确定标准草案主体架构，针对关键术语和定义、及漏洞所触发的危险事件对“人身安全”、“财产安全”的影响进行严重性等内容进行优化，完善草案内容；

2024 年 7 月，起草组组织标准专题研讨会，基于典型案例进行了信息缺陷评估方法应用，并修订评估指标权重，完善草案内容；

2024 年 9 月 13 日，市场监管总局召回中心组织标准研讨会，中汽中心、中国汽研、国汽智联、华为、比亚迪、吉利、奔驰、蔚来、理想、宇通等 10 余家单位进行专题研讨，重点核对标准内容与 GB 44495《汽车整车信息安全技术要求》的关系。

2024 年 9 月 30 日，形成征求意见稿及标准编制说明，面向社会公开征求意见。

二、国家标准编制原则、主要内容及其确定依据

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。本文件主要包括范围、规范性引用文件、术语和定义、评估流程、5 评估与缺陷认定、评估结果处置、附录 A，共 7 个章节，其中：

1. 范围

本文件给出了汽车产品信息缺陷评估的评估流程、评估与缺陷认定及评估结果处置等内容。

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

本文件引用了 GB/T 25069-2022《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 40914-2021《汽车产品召回 预警规则》、GB/T 43387《产品召回 术语》和 GB 44495《汽车整车信息安全技术要求》等国家标准。

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。

本文件增加了信息缺陷、云-管-端-外部链接系统、信息缺陷评估、可获取性、利用难易程度等配套定义。

4. 评估流程

本条款规定了信息缺陷评估的流程如图 1 所示，主要包括：

- 确定开展评估的可能被利用的漏洞；
- 识别触发事件；
- 评估漏洞可获取性、漏洞利用难易程度，得到漏洞被利用的可能性；
- 评估漏洞被利用触发危险事件的严重性；
- 确定漏洞风险等级，进行缺陷认定。

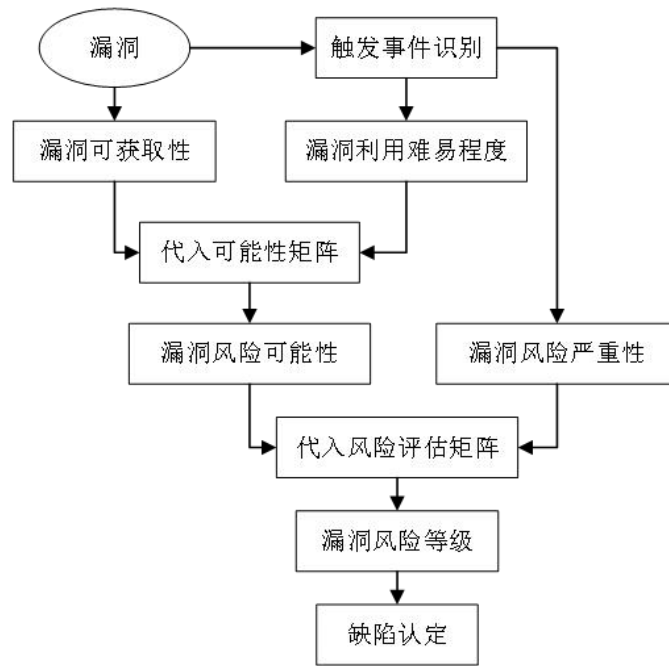


图1 信息缺陷评估流程

5. 评估与缺陷认定

本条款规定信息缺陷评估需综合考虑漏洞被利用引发危险事件或情形的可能性和严重性两个维度，两者共同决定漏洞风险等级。其中，漏洞被利用风险可能性需通过漏洞可获取性和漏洞利用难易程度共同决定。

1) 漏洞可获取性根据获取方式、专用工具、获取人员的专业水平和知识水平对漏洞可获取性进行分析与评估，漏洞可获取性分为4个等级：容易、中、难、极难。

2) 漏洞利用难易程度评估分为初步评估和结果修正两个步骤，分为4个等级：容易、中、难、极难。

3) 严重性根据由漏洞所触发的危险事件对“人身安全”、“财产安全”的影响进行严重性等级划分，分为5个等级：高、较高、中、较低、低。

4) 在漏洞被利用引发危险事件或情形的可能性和严重性等级确定的基础上, 应按照 GB/T 34402-2017 中 4.6 的要求确定漏洞风险等级。漏洞风险等级水平分为五级: 高 (第 5 级)、较高 (第 4 级)、中 (第 3 级)、较低 (第 2 级)、低 (第 1 级)

可能性 \ 严重性					
	低	较低	中	较高	高
低	1	2	2	3	3
较低	2	2	3	3	4
中	2	3	3	4	4
较高	3	3	4	4	5
高	3	3	4	5	5

图 2 风险评估矩阵

5) 缺陷认定。根据漏洞风险等级和国内外召回案例进行缺陷判定:

——综合风险水平等级为高 (第 5 级) 和较高 (第 4 级) 的漏洞, 应认定为信息缺陷;

——综合风险水平等级为中 (第 3 级) 的漏洞, 通过分析国内外相关召回案例, 若存在类似召回案例的, 应认定为缺陷; 若没有类似召回案例, 应认定为普通漏洞;

——综合风险水平等级为较低 (第 2 级) 和低 (第 1 级)

的，应认定为普通漏洞。

6. 评估结果处置

本章节规定了实施召回、发布预警和组织应急处置三种处置方式。

1) 召回处置方面，参考 GB/T 34402-2017 《》第 5 章风险控制部分，根据漏洞风险等级要求生产者采取实施召回或技术服务活动两种方式。

——对于被认定为信息缺陷的，生产者根据相应的法律法规实施召回活动，消除安全隐患。

——对于被认定为普通漏洞的，生产者可通过技术服务活动方式自行修复。

2) 发布预警方面，分为主管部门发布预警和生产者发布预警两种情形，衔接 GB/T 40914-2021 《汽车产品召回 预警规则》。

当出现以下情形之一时，汽车召回主管部门按照 GB/T 40914-2021 《汽车产品召回 预警规则》的要求向社会发布预警信息：

——漏洞风险等级为高、较高或中，生产者应实施召回活动而不实施或无法实施召回的；

——同一缺陷问题涉及多个不同生产者，部分生产者无法确认的；

——生产者不配合缺陷调查的；

——其它召回主管部门认为需要通过发布预警来控制风险的。

当出现以下情形之一时，生产者按照 GB/T 40914-2021《汽车产品召回 预警规则》的要求向社会发布预警信息并采取应急处置措施：

——漏洞风险等级为中、较低或低，同时涉及多个不同生产者或属于行业共性问题的；

——汽车产品的危险事件或情形对社会具有重大影响的；

——云平台等相关服务提供商问题导致车辆可能存在风险的；

——其它被召回主管部门认定需要启动风险预警的。

3) 应急处置方面，明确召回主管部门发布预警信息后，产品召回技术机构应联合应急机构成立调查小组，根据对应的汽车产品信息问题快速研究应急处理办法，并对外发布以帮助社会各界快速采取应急处理措施，防止问题大规模爆发。如果信息缺陷涉及到信息系统中软硬件通用漏洞的，相关应急处理机构应当在汽车产品生产者发布预警后，对事件即刻做出响应，组织对事态发展情况的跟踪研判，研究制定防范措施和应急工作方案，协调组织资源调度和部门联动的各项准备工作。

三、预期的经济效益、社会效益、生态效益

当前，汽车行业处于前所未有的转型期与变革期，智能网联以及自动驾驶技术的迅猛发展，极大地改变了传统出行方式，提升了用户驾乘体验，但同时汽车面临的网络安全挑战也更加复杂多变，数据泄露、远程控车、系统崩溃等风险场景屡见不鲜。构建一个安全、可靠的车联网生态系统，已成为全行业的共同责任与迫切需求。

汽车信息安全缺陷，将成为汽车缺陷的新形态！汽车信息安全问题不仅涉及到个人信息泄露、财产（账户）安全，还有可能遭到网络攻击，远程控制造成汽车无法正常操控，引发交通事故。本标准的编制旨在对车辆漏洞风险评估过程进行规范化和标准化，为汽车信息缺陷判定提供科学依据，为政府部门和生产者作出召回决策和其他批次性问题处理方式提供实用性指南。本标准是落实《缺陷汽车产品召回管理条例》相关要求的重要支撑标准，也是加强缺陷汽车产品召回监管的基础技术标准，还是指导生产者进一步完善汽车产品信息安全风险管理的 key 技术标准。

四、与国际、国外同类标准技术内容的对比情况

目前国际上没有可供参考、借鉴的标准，本标准未采用国际标准。

本标准与 GB 44495-2024《汽车整车信息安全技术要求》有效协同。GB 44495 明确提到车辆外部连接系统及软件升级系统不应存在由汽车行业权威漏洞平台 6 个月前公布且未经

处置的高危及以上的安全漏洞，通过此举在产品上市前尽可能规避了漏洞引起了风险。但漏洞数据是动态变化的，每天都会层出不穷的爆出新漏洞，因此在车型上市后的后市场阶段此类安全问题需引起重视，漏洞引起的安全缺陷需要及时通过召回来修复，因此本标准与强标协同，确保汽车上市后的安全缺陷被有效识别及判定，进一步通过召回降低安全风险，保障汽车安全。

五、与有关法律、行政法规及相关标准的关系

本文件与《中华人民共和国产品质量法》《缺陷汽车产品召回管理条例》等国家有关现行法律、法规和标准协调一致，无冲突和违背情况。

六、重大分歧意见的处理经过和依据

本标准在编写过程中尚未出现重大意见分歧。

七、涉及专利的有关说明

本文件不涉及专利问题。

八、实施国家标准的要求，以及组织措施、技术措施、过渡期和实施日期的建议等措施建议

本文件作为推荐性国家标准，由全国产品缺陷与安全管理体系标准化技术委员会（SAC/TC463）负责解释、组织宣贯。建议批准发布后半年内实施。

九、其他应当说明的事项

无。