ICS 43.020
CCS T40

中华人民共和国国家标准

GB/T XXXXX—XXXX

汽车产品召回 信息缺陷评估指南

Motor vehicle product recall-Guidelines for information defect assessment

(点击此处添加与国际标准一致性程度的标识)

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 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：

本文件主要起草人：

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

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 25069-2022 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

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

云-管-端-外部链接系统（3.2）存在的漏洞（3.3）被利用而导致同一型号、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]

3.4

威胁 threat

可能导致系统、组织或个人受到损害的意外事件的潜在原因。

[来源：GB 44495-2024，3.5]

3.5

人身安全 personal safety and security

避免人的健康、生命等遭受侵害的状态。

3.6

财产安全 property safety and security

避免财务、物质、数据等遭受侵害的状态。

注：包括车辆本身的、车辆以外的和车辆运行中产生的数据资产等安全。

3.7

信息缺陷评估 information defect assessment

从漏洞被利用的可能性（3.8）及漏洞严重性（3.9）两个维度，确定云-管-端-外部链接系统可能存在的漏洞被利用引发的危险事件或情形风险（3.10）水平的过程。

3.8

可能性 probability

漏洞可获取性（3.11）和利用难易程度（3.12）的综合。

3.9

严重性 severity

漏洞被利用触发车辆的危险事件或情形对人身安全、财产安全的危害程度。

3.10

风险 risk

伤害发生概率和伤害严重程度的组合。

[来源：GB/T 43387-2023，3.11]

3.11

可获取性 accessibility

漏洞被发现的难易程度。

3.12

利用难易程度 access feasibility

漏洞可能触发、引发车辆的危险事件或情形风险发生程度的度量。

4 评估流程

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。

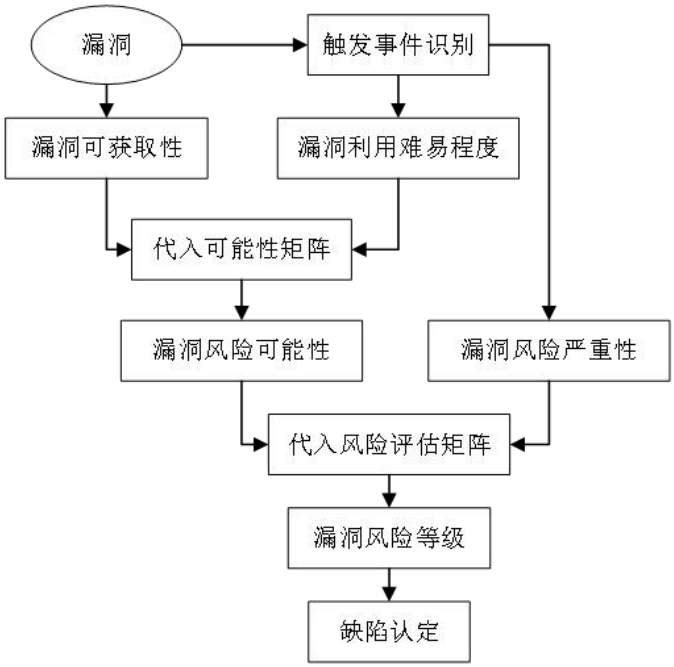

图 1　信息缺陷评估流程

5　评估与缺陷认定

5.1　概述

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。

5.2　可能性

5.2.1　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，各等级的说明见表1。

表 1　漏洞可获取性等级说明

等级	说明
容易	挖掘信息漏洞无需依靠具备信息安全知识的人员、无需掌握基础信息和业务信息、仅需要公开的漏洞利用工具，漏洞信息及相关描述可通过收集得到
中	挖掘信息漏洞需要依靠具备一般信息安全知识的人员、掌握较少基础信息和业务信息、使用通用商用工具，漏洞信息及相关描述通过较深度信息收集得到
难	挖掘信息漏洞需要依靠具备较丰富信息安全知识的人员、掌握大量的基础信息和业务信息、使用一般定制研发的专用设备及脚本，漏洞信息及相关描述需要通过较深度挖掘得到
极难	挖掘信息漏洞需要依靠具备非常丰富信息安全知识的人员、掌握足够多的基础信息和业务信息、使用多种深度定制研发的专用设备及脚本，漏洞信息及相关描述需要通过深度挖掘得到

5.2.2　漏洞利用难易程度

5.2.2.1 漏洞利用难易程度等级说明

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。漏洞利用难易程度分为4个等级：容易、中、难、极难，各等级的说明如表2所示，漏洞利用途径等信息见附录A。

表 2 漏洞利用难易程度等级说明

等级	说明
容易	可通过远程通信利用漏洞，可以无限次实现利用漏洞触发形成危险事件或情形
中	可通过远程通信利用漏洞，实现有限次数的利用触发以形成危险事件或情形
难	可通过本地或者物理接触的方式利用漏洞，可以无限次实现利用漏洞触发形成危险事件或情形
极难	可通过本地或者物理接触的方式利用漏洞，只能实现有限次数的利用触发以形成危险事件或情形

5.2.2.2 漏洞利用难易程度初步评估

在确认了需开展评估的漏洞及识别触发事件的基础上，根据表2中漏洞利用难易程度等级说明，依据相关技术资料，组织相关专业技术人员进行漏洞利用难易程度初步评估。

5.2.2.3 评估结果修正

在进行漏洞利用难易程度初步评估后，考虑到攻击途径、触发要求、权限要求、用户交互等复杂性，需要对初步评估结果进行等级升级，修正可考虑的因素如下：

a) 可通过权限要求以及用户交互两方面对利用难易程度等级进行修正，当满足无权限或者是无用户交互条件时；
b) 可通过配置的方式或次数对利用难易程度等级进行修正，当需要手工多次配置时；
c) 可通过使用的工具对利用难易程度等级进行修正，当需要使用专业工具或者深度定制研发的专用设备时。

5.2.3 可能性初步评估

在确定了漏洞可获取性和漏洞利用难易程度的基础上，通过查询可能性评估矩阵（见表3）确定漏洞被利用风险可能性等级。漏洞被利用风险可能性等级分为5个等级：高、较高、中、较低、低。

表 3 漏洞被利用风险可能性评估矩阵

可能性		漏洞利用难易程度			
		容易	中	难	极难
漏洞可获取性	容易	高	较高	中	较低
	中	较高	中	较低	低
	难	中	较低	较低	低
	极难	低	低	低	低

5.2.4 可能性评估结果修正

考虑到汽车潜在危害对象、形式环境、漏洞场景等复杂性，可根据威胁场景对评估结果进行修正，修正可考虑的因素除参照GB/T34402-2017中4.4.3和第4.5.3的要求外，还应开展漏洞被利用风险可能性关联分析，包括但不限于：

a) 若多个漏洞（假设为漏洞 A、漏洞 B、漏洞 C）联合才能触发危险事件，此时的漏洞风险可能性指的是该危险事件或情形对应的这一组漏洞被利用的可能性；
b) 假设攻击者首先利用了漏洞 A，然后利用漏洞 B、漏洞 C，最终引发了一个危险事件或情形。此时对漏洞组（A、B、C）进行可能性评估时，应首先分别评估单个漏洞的可获取性和利用难易程度，然后再综合评判。假定可获取性和利用难易程度的容易、中、难、极难的评级分别为 1，2，3，4；
c) 若对漏洞 A 的可获取性和利用难易程度评估结果为（A1、A2）；对漏洞 B 的评估结果为（B1，B2）；对漏洞 C 的评估结果为（C1，C2）。那么这组关联漏洞的可能性结果为：（min{A1、B1、C1}，min{A2、B2、C2}）。

5.3 严重性

5.3.1 严重性初步评估

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，各等级说明如表4所示。

表 4 漏洞被利用风险严重性等级说明

等级	说明
高	不可控，可能严重危及人身、财产安全
较高	一般可控，可能危及人身、财产安全
中	造成车辆行驶性能或功能影响，但简单可控
较低	对车辆性能或功能有部分影响，但常规可控，不影响车辆行驶
低	对车辆安全性无直接影响

5.3.2 严重性评估结果修正

考虑到汽车潜在危害对象、形式环境、漏洞场景等复杂性，可根据威胁场景对评估结果进行修正，修正可考虑的因素除参照GB/T34402-2017中4.4.3和第4.5.3的要求外，还应考虑漏洞被利用风险严重性关联分析、漏洞被利用场景与社会影响等因素，其中：

a) 若一个漏洞可出发多个危险事件，则以最严重的危险事件为主分析，并以最严重的危险事件的严重性等级为最终严重性评估结果；
b) 相同漏洞在不同环境下可能造成不同的后果。比如，相比于只能采用人类驾驶的车辆而言，当基于 V2X 技术进行辅助驾驶或自动驾驶时，应提高严重性的等级；
c) 社会影响指危险事件或情形发生后，对社会造成各方面的影响。由于社会影响具备不可预知的特性，因此需要根据实际案例情况，酌情提高严重性等级。

注：若漏洞对重要交通的正常运行造成了较为严重的社会影响，则应提高严重性等级。

5.4 确定漏洞风险等级

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），见图2。

严重性 / 可能性	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

5.5　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

6.1　实施召回

6.1.1　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。

6.1.2　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。

6.2　发布预警

6.2.1　召回主管部门

当出现以下情形之一时，汽车召回主管部门应按照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。

6.2.2　生产者

当出现以下情形之一时，生产者应按照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。

6.3 应急处置

6.3.1 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。

6.3.2 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。

附 录 A
（资料性）
漏洞利用途径

A.1 攻击途径

攻击途径的赋值如下：

a) 远程：攻击者可以通过互联网利用该漏洞对汽车发动攻击，比如 4G、3G 等；
b) 近距离：攻击者可以通过共享的物理或逻辑利用该漏洞对汽车发动攻击，比如蓝牙、Wi-Fi、IEEE 802.11、本地 IP 子网等；
c) 本地：攻击者通过读/写操作或运行应用程序/工具来利用该漏洞，即本地需要进行参与，该漏洞才能被利用，比如攻击者需要本地登录、需要用户去下载、接受恶意的内容；
d) 物理接触：攻击者必须物理接触汽车才能发动攻击，例如通过 OBD II 对汽车总线进行攻击。

A.2 触发要求

触发要求是指漏洞成功触发的要求，反映受影响组件在系统环境的版本、配置等因素影响下，成功触发漏洞的要求。通常触发要求低的漏洞危害程度高，触发要求的赋值如下：

a) 低：漏洞触发对受影响组件的配置参数、运行环境、版本等无特别要求，包括：默认的配置参数、普遍的运行环境；
b) 高：漏洞触发对受影响组件的配置参数、运行环境等有特别要求，包括：不常用的参数配置、特殊运行环境条件。

A.3 权限要求

权限要求是指攻击者成功利用漏洞需要具备的权限层级，即利用漏洞时是否需要拥有对该组件操作的权限，如管理员权限、访客权限等。权限要求的赋值如下:

a) 无：攻击者在发动攻击前不需要授权，执行攻击时不需要访问任何设置或文件；
b) 低：攻击者需要取得普通用户权限，该类权限对脆弱性组件有一定控制能力，具有部分（非全部）功能的使用或管理权限，通常需要口令等方式进行身份认证，例如，车载娱乐系统的普通用户权限；
c) 高：攻击者需要取得对脆弱性组件的完全控制权限。通常，该类权限对于脆弱性组件具有绝对控制能力，例如，对总线进行攻击需要对脆弱性组件的完全控制权限，普通用户权限无法攻击。

A.4 用户交互

用户交互是指成功利用漏洞是否需要用户（而不是攻击者）的参与，该指标识别攻击者是否可以根据其意愿单独利用漏洞，或者要求其他用户以某种方式参与。

a) 不需要：无需任何用户交互即可利用漏洞；
b) 需要：漏洞的成功利用需要其他用户在漏洞被利用之前执行一些操作(打开某个文件、点击某个链接、访问特定的网页等)。

注：假设某个漏洞只能在系统管理员安装应用程序期间才可能被利用。对于这种情况，用户交互是“需要”。往车机中植入木马，当用户点击特定浏览器自动执行该木马，使得车辆自动上报车辆的隐私信息。

参 考 文 献

GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求
GB/T 20272-2019 信息安全技术 操作系统安全技术要求
GB/T 28452-2012 信息安全技术 应用软件系统通用安全技术要求
GB/T 30279-2020 信息安全技术 网络安全漏洞分类分级指南