【公开】

软件供应链安全能力评估总结报告

--软件产品开源代码安全评价能力部分

编制单位：中国网络安全审查认证和市场监管大数据中心

信息安全基准实验室

发布日期：2026 年 9 月 9 日

中国网络安全审查认证和市场监管大数据中心

信息安全基准实验室

报告签发人：陈鑫

审核人：郑刚、辛建峰

编制人：杨莉、陈淑娟

联系人：辛建峰

联系地址/邮政编码：北京市西城区三里河东路 8 号　100037

联系电话/传真：010-88650273

联系邮箱：pe@isccc.gov.cn

目 录

一、前言

《**中华人民共和国国民经济和社会发展第十五个五年规划纲要**》提出“滚动实施制造业重点产业链高质量发展行动，建立健全产业链供应链安全风险评估和应对机制”。《**国务院关于产业链供应链安全的规定**》（国务院第 834 号令）提出“国家引导产业链供应链合理有序布局，推进产业链供应链数字化、智能化，提升产业链供应链安全可控水平，促进产业链供应链高质量发展”。市场监管总局、国家发展改革委、科技部、农业农村部、商务部于 2024 年联合发布《**关于质量基础设施助力产业链供应链质量联动提升的指导意见**》（国市监质发[2024]6 号）提出“以专业高效的检验检测保障产业链供应链可靠性。支持建设一批服务高新技术产业、战略性新兴产业发展的国家和省级质检中心，加强检验检测高技术服务业集聚区和检验检测认证公共服务平台示范区建设，推动整合、提升一批检验检测共性技术平台，为产业链上下游提供一体化服务”。当前，提高产业链供应链韧性和安全水平是我国统筹发展和安全的重要战略部署，提升产业链供应链安全的技术方法和服务能力成为一些重要行业和领域的迫切需求。

中国网络安全审查认证和市场监管大数据中心（以下简称 CCRC）为国家市场监督管理总局直属正司局级事业单位，依据《网络安全法》《数据安全法》《个人信息保护法》《网络安全审查办法》及国家有关强制性产品认证法律法规，承担网络安全审查技术与方法研究、网络安全审查技术支撑工作；在批准范围内开展与网络安全相关的产品、管理体系、服务、人员认证和培训、检验检测等工作。2026 年 3 月 CCRC 在软件供应链领域组织了首次安全能力评估活动。通过本次活动，参加机构加深了对相关国家标准的理解和运用，提升了软件供应链安全的认识和技术服务能力，CCRC 为通过能力评估的机构颁发了“软件供应链安全能力”证书。

本报告针对本次评估的“软件产品开源代码安全评价能力”方向的整体结果进行分析总结。

二、概况

2.1. 参加机构的范围

来自全国的 56 家机构报名参加软件产品开源代码安全评价能力评估，参加机构的地域覆盖了 18 个省、自治区、直辖市，主要集中于北京、广东、上海、内蒙、江苏等地区。参加机构地域分布详见图 1。

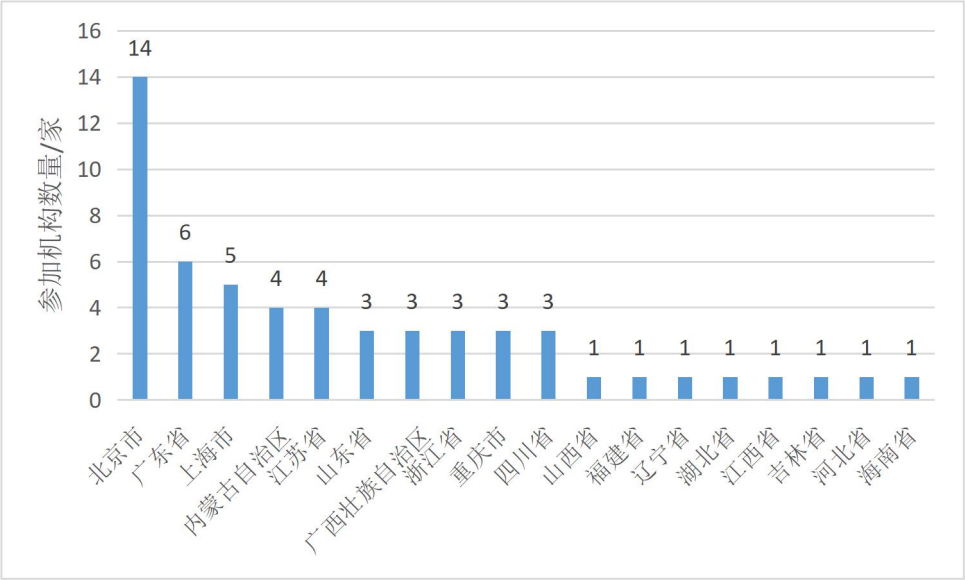

图 1 参加机构地域分布

2.2. 评估的方式及依据

本次软件产品开源代码安全评价能力评估的主要依据国家标准GB/T 43848-2024《网络安全技术 软件产品开源代码安全评价方法》，参加机构需根据GB/T 43848-2024和作业指导书的要求，对CCRC统一发放的软件包（已预设缺陷）进行检测分析，并向CCRC反馈结果报告。

检测分析条款主要来自GB/T 43848-2024的关键指标，详见下表1。

表 1　检测分析项目

序号	作业指导书 章节号/名称	检测要求
1	2.2.1.开源代码规模与占比	统计软件产品包含的各开源代码模块字节数规模及其在软件产品代码中所占比例。
2	2.2.2.开源代码编码语言	统计软件产品包含的开源代码模块所使用的编码语言种类及其所开发代码占软件产品的比例。
3	2.2.3.开源代码托管平台	统计软件产品包含的开源代码托管平台运营方基本信息。
4	2.2.4.开源代码下载平台	统计开源代码下载平台对开源代码完整性的保障情况。
5	2.2.5.开源代码漏洞严重性	参考 GB/T 30279—2020 中 6.3.3 统计软件产品包含的开源代码模块原始漏洞严重性。
6	2.2.6.开源许可证规范性	统计软件产品包含的开源代码对应许可证编写规范性情况,评价内容涉及授权范围、授权条件、违约与授权终止、免责声明等。
7	2.2.7.开源许可证兼容性	统计软件产品包含的开源代码所使用的各开源许可证之间兼容性情况,以判断软件产品对开源许可证合规使用情况。
8	2.2.8.开源代码物料清单	评价软件产品包含的开源代码物料清单的完备性,包括建立和维护可追溯性的策略和程序,记录和保留开源代码的原始供应方、开源社区或开发贡献者等相关信息。

2.3. 实施过程

本次软件产品开源代码安全评价能力评估共收到56家机构报名。2026年3月31日组织实施，全部报名机构均提交有效结果报告。2026年4月至6月期间，CCRC对结果报告进行了评分与统计分析，并于6月完成了结果公示和证书发放。

2.4. 其他说明

本次软件产品开源代码安全评价能力评估对每家参加机构赋予唯一代码，在本报告中凡说明参加机构的检测结果和评分时均以代码表示。

三、评分说明

3.1 评分方式

本次能力评估指定值由专家公议方式确定，采用定性和定量相结合的方式对参加机构提交的检测结果进行评分。

3.2 评分细则

为确保评分结果的一致性，CCRC组织技术专家制定评分细则，依据评分细则对参加机构提交的检测结果作判定。

3.3 结果判定

评审专家根据参加机构提交的检测分析结果和相关证明材料，综合考虑检测结果的准确性、过程的合理性和证据的充分性等方面，对每个检测分析结果逐项评分。

结果判定标准为：满分为100分，若机构成绩≥50分，则结果为合格，反之为不合格。

四、结果分析

参加的 56 家机构中结果为“合格”的共 47 家，占比 83.93%；结果为“不合格”的共 9 家，占比 16.07%。结果统计见表 2。

表 2 参加机构结果统计表

统计量	机构数量（个）
参加能力评估的机构数量	56
结果合格的机构数量	47
结果不合格的机构数量	9

各参加机构的得分情况详见表3。

表 3　参加机构评分结果汇总

序号	参加机构代码	分数	结论	序号	参加机构代码	分数	结论
1	01	62.55	合格	29	35	75.25	合格
2	02	44.95	不合格	30	36	70.2	合格
3	03	56.25	合格	31	37	82.55	合格
4	05	63.15	合格	32	38	74.3	合格
5	06	62.85	合格	33	40	66.8	合格
6	08	54.2	合格	34	41	40.55	不合格
7	09	69.6	合格	35	42	58.1	合格
8	11	59.4	合格	36	43	71.15	合格
9	12	53.75	合格	37	45	73.05	合格
10	13	55.45	合格	38	46	58.45	合格
11	15	46.9	不合格	39	47	59.55	合格
12	16	59.55	合格	40	48	57.6	合格
13	17	38.45	不合格	41	50	60.85	合格
14	18	59.3	合格	42	51	28.45	不合格
15	20	54.3	合格	43	52	72.25	合格
16	21	51.55	合格	44	54	79.3	合格
17	22	47.8	不合格	45	56	39.5	不合格
18	23	61.85	合格	46	57	40.3	不合格
19	24	59.65	合格	47	58	60	合格

序号	参加机构代码	分数	结论	序号	参加机构代码	分数	结论
20	26	56.75	合格	48	59	59.05	合格
21	27	56.75	合格	49	60	30.1	不合格
22	28	87.5	合格	50	62	51.45	合格
23	29	56.5	合格	51	63	68.75	合格
24	30	72.05	合格	52	64	53.15	合格
25	31	74.3	合格	53	65	65.5	合格
26	32	64.25	合格	54	66	61.15	合格
27	33	61.6	合格	55	67	66.9	合格
28	34	61.45	合格	56	68	64.2	合格

本次能力评估中各参加机构的成绩分布见图 2，平均分为 59.12 分，大部分机构得分集中在 50～70 分区间，呈现典型的近似正态分布。

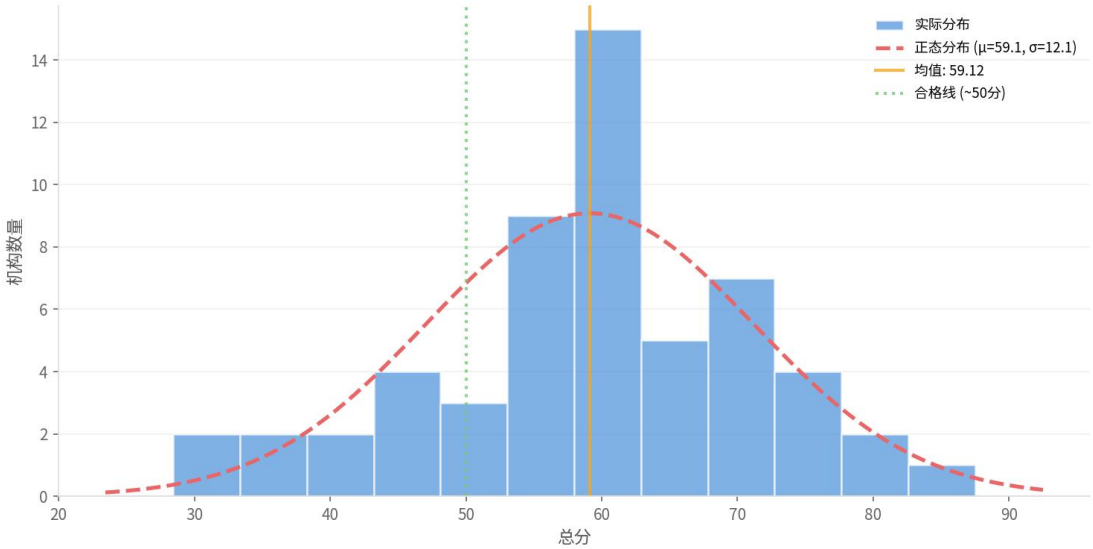

图 2 参加机构成绩分布图

本次能力评估共包含 8 个检测项，其中 2.2.1 开源代码规模与占比作为观察项不计得分。各检测项目的机构得分情况统计参见表 4，各检测项平均得分率对

比见图 3，分析可知，检测项 2.2.7 是本次评估中最薄弱项，平均得分率仅为 30.61%，且有 15 家机构（占比 26.8%）在该项得分为零；其次是 2.2.3，平均得分率 43.15%，5 家机构零分。

表 4　各检测项机构得分情况统计

检测项	满分	平均分	中位数	最高分	最低分	平均得分率
2.2.2	14	7.12	7.00	13.00	1.00	50.89%
2.2.3	15	6.47	5.00	15.00	0.00	43.15%
2.2.4	18	13.98	16.00	18.00	0.00	77.68%
2.2.5	18	9.51	10.80	16.65	0.00	52.81%
2.2.6	14	9.74	11.00	14.00	1.00	69.58%
2.2.7	7	2.14	2.00	6.00	0.00	30.61%
2.2.8	14	10.15	9.25	14.00	0.00	72.51%

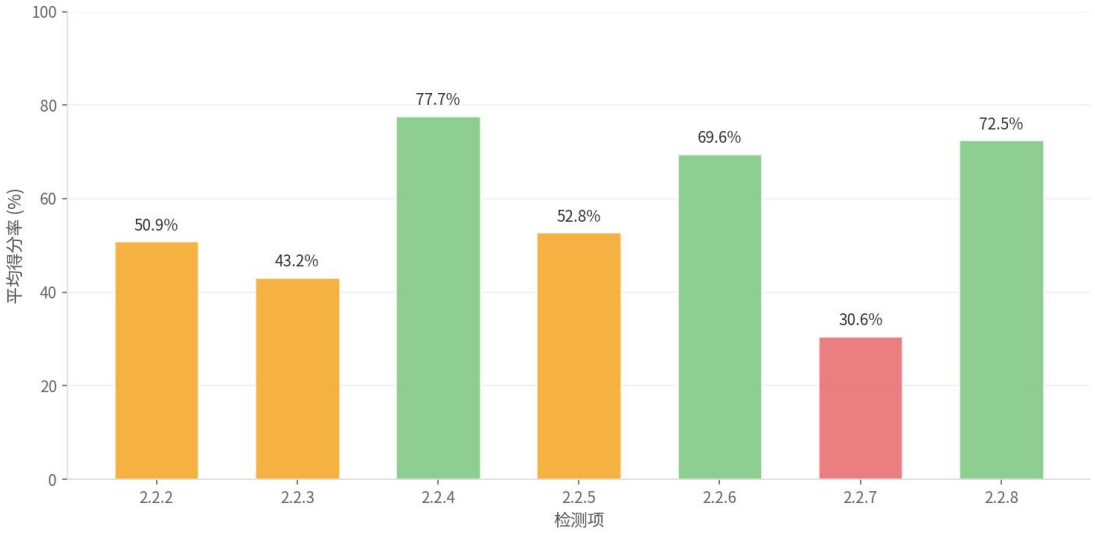

图 3：各检测项平均得分率对比

各检测项的满分机构数和零分机构数见图 4，该数据反映了检测能力的两极

分化程度。检测项 2.2.4 呈现典型的两极分化特征，近半数机构（44.6%）获得满分，但仍有 4 家机构得分为零。检测项 2.2.7 则呈现低端集中特征，无机构获得满分，且超过四分之一的机构得分为零，说明该项能力存在普遍性短板。

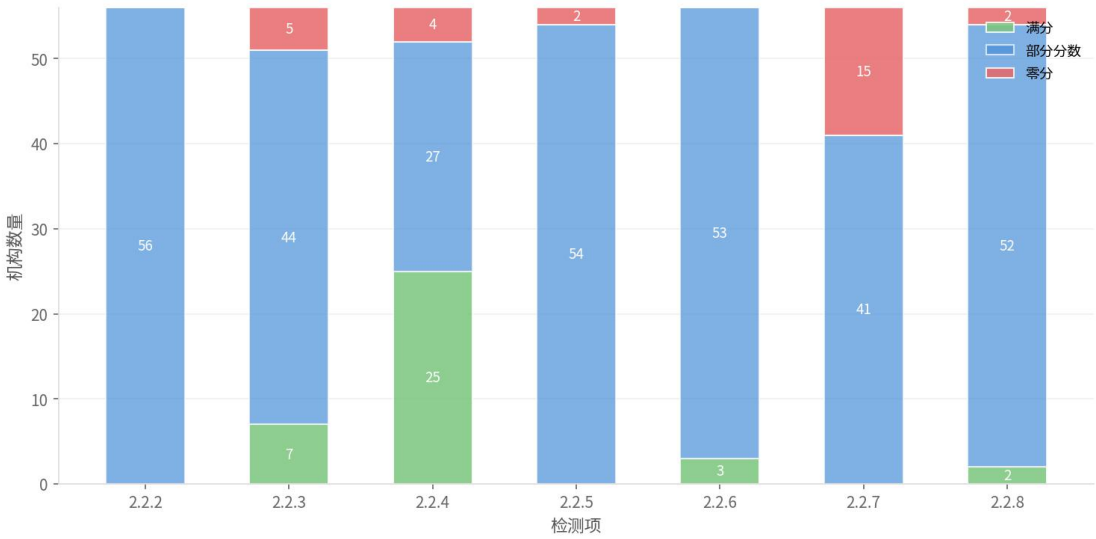

图 4 各检测项满分/零分机构数量分布

五、技术分析和建议

通过分析各参加机构提交的能力评估结果，我们发现了一些普遍存在的共性问题。为帮助各机构进一步提升软件产品开源代码安全评价能力，建议如下：

1.加强对标准要求的准确理解

准确理解标准定义与条款要求是开展软件产品开源代码安全评价的基础。分析发现，本次评估中存在部分项得分率低、各机构对考核条款理解参差不齐等突出问题，建议各机构进一步加强对标准文本的系统研究，逐条拆解各检测指标的考核要点与取证要求，针对薄弱检测项编制配套解读与标杆案例；同步建立标准与检测工具对应清单，明确各条款适配工具及输出材料，消除条款理解偏差，避免因标准把握不准造成不必要失分。

2.提升工具选型与使用能力

当前开源代码安全评价检测工具种类丰富，但由于各工具的数据库规模、分析时效，对代码的分析层次、相似代码的比对算法等技术差异，造成不同工具检测结果的差异性。结合工具选型分散、盲目堆砌工具却未提升得分等现状，建议

各机构构建开源、商用两类评价工具清单，梳理主流工具的功能定位、适用场景、数据库完善程度等，形成轻量化开源组合、商用一体化平台两套标准化检测链路；常态化开展工具实操培训，重点关注多工具联动扫描、结果交叉分析、报告解读实操，摒弃“工具越多越好”的误区，以覆盖标准检测项、具备标准符合性要求为搭配工具目标，切实发挥检测工具实际效能。

3.重视检测过程的规范性

本次能力评估中发现部分机构存在检测过程缺失、日志与佐证材料不全、操作无法追溯等过程性证明材料问题，建议各机构在后续检测和技术服务活动中，严格遵循标准和作业指导文件要求，规范技术分析记录与结果描述；在技术分析完成、材料提交前设置两级审核：一是审核工具是否覆盖全部标准维度；二是审核过程材料完整性，从源头减少流程不规范导致的失分，以确保过程完整、记录可追溯、结果准确可靠。

六、小结

本次能力评估活动受到网络安全业界广泛关注，在此感谢各参加机构、行业专家、技术支撑机构对本活动的支持！CCRC 信息安全基准实验室将进一步完善能力评估工作机制和组织形式，提升软件供应链安全领域专业技术能力，为社会提供更加规范、灵活、全面的网络安全基准和质量基础设施服务。