

开源软件安全评估模型和指标体系在交通运输行业客票系统中的应用

程娜¹, 李杨², 单新茹², 李子强¹, 林星辰¹, 张伟^{1,2}

(1. 国家计算机网络应急技术处理协调中心, 北京 100029; 2. 铁旅科技有限公司, 北京 100055)

摘要: 在开源生态蓬勃发展的当下, 开源软件安全问题凸显, 国内交通行业交易量最大的某个客票发售系统(简称:客票系统)对开源软件依赖程度加深, 其安全稳定运行面临挑战。通过聚焦开源软件安全, 参考国内外相关标准, 构建了包含评估建议、指标核查和技术检测三个维度的安全评估模型。在此基础上, 提出具有3个层级的开源软件安全评估指标体系, 涵盖安全管理、安全建设、安全质量、安全合规和持续性管控等一级指标。相较国内外相关标准, 该指标体系更加完善。将该指标体系应用于此客票系统, 通过收集相关数据、指标评分、综合评估与分析, 客票系统开源软件评估得分为82分, 处于持续改进级, 系统稳定性和可靠性显著增强, 验证了指标体系的有效性和实用性, 为交通行业其他业务系统开源软件安全管理提供了借鉴。

关键词: 供应链安全; 开源软件安全; 安全评估模型; 安全评估指标体系

DOI: 10.11907/rjdk.251397

扫描二维码阅读全文:



中图分类号: C93

文献标识码: A

文章编号: 1672-7800(XXXX)0XX-0001-08

Application of Open Source Software Security Assessment Model and Indicator System in Passenger Ticket System of Transportation Industry

CHENG Na¹, LI Yang², SHAN Xinru², LI Ziqiang¹, LIN Xingchen¹, ZHANG Wei^{1,2}

(1. National Computer Network Emergency Technology Coordination Center, Beijing 100029, China;
2. Tielv Technology Co., Ltd., Beijing 100055, China)

Abstract: In the current booming development of the open source ecosystem, the security issues of open source software have become prominent. The largest ticket sales system in the domestic transportation industry (referred to as the "ticket system") has deepened its dependence on open source software, and its safe and stable operation is facing challenges. This article focuses on open source software security and refers to relevant domestic and foreign standards to construct a security assessment model that includes three dimensions: evaluation recommendations, indicator verification, and technical testing. On this basis, a three-level open source software security evaluation index system is proposed, covering first level indicators such as security management, security construction, security quality, security compliance, and continuity control. The indicator system was applied to this ticket system, and through collecting relevant data, indicator scoring, comprehensive evaluation and analysis, the open source software evaluation score of the ticket system was 82 points, which is in the continuous improvement level. The system stability and reliability were significantly enhanced, verifying the effectiveness and practicality of the indicator system, and providing reference for the security management of open source software in other business systems in the transportation industry.

Key Words: supply chain security; open source software security; security assessment model; safety assessment index system

收稿日期: 2025-06-24

基金项目: 中国国家铁路集团有限公司科技研究开发计划课题(K2023W008)

作者简介: 程娜(1977-), 女, 硕士, 国家计算机网络应急技术处理协调中心高级工程师, 研究方向为网络信息安全; 李杨(1984-), 男, 铁旅科技有限公司助理研究员, 研究方向为铁路信息化; 单新茹(1995-), 女, 铁旅科技有限公司助理研究员, 研究方向为铁路数据共享与数据传输技术; 李子强(1981-), 男, 国家计算机网络应急技术处理协调中心工程师, 研究方向为 IOT 固件逆向, 源代码漏洞; 林星辰(1986-), 男, 硕士, 国家计算机网络应急技术处理协调中心高级工程师, 研究方向为网络和数据安全、ICT 供应链安全; 张伟(1985-), 男, 博士, 国家计算机网络应急技术处理协调中心高级工程师, 研究方向为网络信息安全。本文通讯作者: 张伟。

0 引言

开源生态繁荣发展背后,风险隐患备受关注。不管是直接使用开源技术,还是购买基于开源技术的商业软件,都需要考虑开源技术带来的风险^[1-2]。不同的是,规避开源技术风险的责任主体有所不同。企业在使用或引入开源软件或代码时,需要考虑开源风险、违约风险、知识产权风险、开源许可证兼容性风险,以及数据安全及隐私风险^[3-4]。开源代码安全问题凸显,影响较为严重。2022年发布的开源安全调查报告显示,一个应用程序开发项目平均有49个漏洞和80个直接依赖项。此外,修复开源项目漏洞所需的时间也在同步增加。根据国家互联网应急中心发布的《2021年开源软件供应链安全风险研究报告调查结果》显示,2020年新增漏洞中,高危漏洞占比最高,数量为1 826个^[5]。使用过时的、存在漏洞的开源组件仍然是软件开发过程中的常态。美国新思科技(Synopsys)发布的《2022开源安全与风险分析报告》围绕5个指标对代码库中的开源项目维护情况进行了统计^[6]。结果显示,包含两年无任何开发活动的组件在代码库中的占比为88%,包含过时四年多的开源代码在代码库中的占比为85%。《2023开源安全与风险分析报告》显示,在经过分析的全球17个行业超过1 700个代码库中,96%的代码库包含开源代码,代码库中76%的代码是开源的^[7]。《2024开源安全与风险分析报告》对16个行业950多个代码库中的漏洞和许可证冲突进行了分析^[8]。在这种情势下,各国各行业纷纷布局开源软件治理、安全评估等工作^[9-10]。

本文基于开源软件安全漏洞、评测方法^[11]、评估模型^[12]及指标体系^[13-14]等方面的研究,实现了软件成分分析、漏洞分析与评估、漏洞范围影响分析等功能,进而建立了开源软件安全评估模型。在此基础上,结合国铁集团业务系统在开源软件使用与管理方面的实际情况,依据相关评测方法与评估模型,构建了适用于业务场景的开源软件安全评估指标体系。

1 开源软件安全评估模型

本文参考国内外相关标准^[15-16],包括国标《信息安全技术信息安全保障指标体系及评价方法第2部分 指标体系》(GB/T 31495.2-2015)^[17]、《信息安全技术 信息技术产品安全可控评价指标第1部分:总则》(GB/T 36630.1-2018)^[18]、《网络安全技术 关键信息基础设施安全保护能力指标体系》(报批稿)^[19]、美国的C2M2模型及指标、美国NIST的评估指标、CSA云评估、美国关基网络安全控制性能指标(CPG)等,设计了开源软件管理的安全评估模型。

开源软件安全评估模型包括3个维度:评估建议、指标核查和技术检测。其中,评估结果由低至高依次分为亟

需整改、有待改进和持续改进三个等级,分别对应不同的开源软件安全级别。开源软件安全评估模型如图1所示。

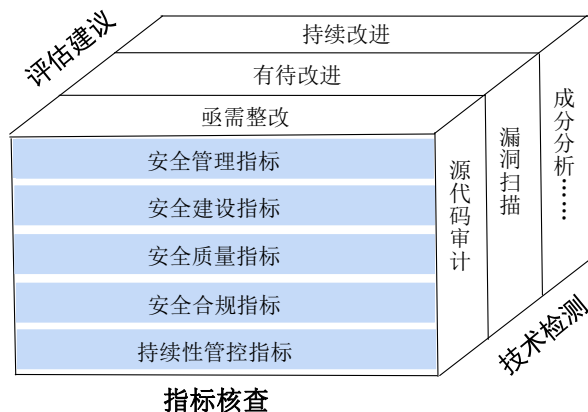


Fig. 1 Open source software security assessment model

图1 开源软件安全评估模型

技术检测通过源代码审计、漏洞扫描、软件成分分析等方法,对开源软件质量进行评估。

指标核查通过资料搜集、现状分析、技术检测等手段,对安全管理指标、建设指标、质量指标、合规指标和持续性管控指标进行逐项评分。

综合评分60分以下对应亟需整改级,61~80分对应有待改进级,81分以上对应持续改进级。

2 开源软件安全评估指标体系

针对开源软件安全需求,结合关键信息基础设施ICT供应链安全保障的迫切要求,构建了开源软件安全评估指标体系。开源软件安全评估指标体系共有3个层级,其中,一级指标和二级指标构成指标体系框架,三级指标为底层指标。

开源软件安全评估指标体系的一级指标是安全评估模型的指标核查维度,包括安全管理指标、安全建设指标、安全质量指标、安全合规指标和持续性管控指标。其中,安全管理指标评估开源软件安全组织和制度;安全建设指标评估开源软件生命周期安全管理情况;安全质量指标评估开源软件安全漏洞和版本管理情况;安全合规指标评估版权和专利管理情况;持续性管控指标评估第三方管理和连续性。开源软件安全评估指标体系的二级指标是对一级指标依据一定的准则进行分析和分解所得,开源软件安全评估指标体系框架如图2所示。

在一级指标基础上,参考《网络安全技术 软件产品开源代码安全评价方法》(GB/T 43848-2024)^[20]和信通院开源软件治理能力评价成熟度模型(T/CCSA 383.3-2023)^[21],结合开源软件安全管理需求,设计了安全评估指标体系的二级指标和三级指标,并设置了各指标所占的分值比例。开源软件安全评估指标如表1所示。

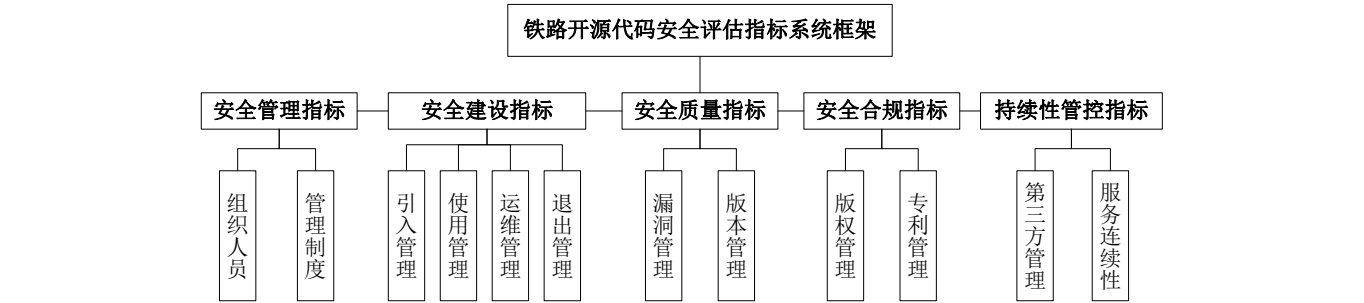


Fig. 2 Framework for open source railway software security assessment indicators

图2 开源软件安全评估指标体系框架

Table 1 Open source software security evaluation metrice

表1 开源软件安全评估指标

一级指标(5)	二级指标(12)	三级指标(26)	指标要求	评估方法
安全管理指标(20)	组织人员(10)	组织机构	建立开源代码管理团队,明确责任分工	核查管理制度,是否对开源代码组织机构有明确说明,责任划分清晰
		岗位人员	设置岗位负责开源代码管理工作,合理配备人员	核查岗位责任书,是否有开源代码管理职责,人员配备是否合理
		资源投入	规范开源代码管理的资源投入	核查管理制度,是否对开源代码管理有资金投入比例等方面的管理要求
	管理制度(10)	制度流程	建立开源代码安全管理制度,例如开源代码生命周期管理、漏洞管理、应急管理等,规范管理流程	核查管理制度,确认开源代码安全管理相关制度是否覆盖全面、内容完整、流程清晰
		技术规范	配套技术规范,例如物料清单格式规范、安全评估规范等,支撑管理流程落地	核查技术规范,是否能科学、严谨、规范指导流程控制点实施
	引入管理(10)	引入评估	对新引入的开源代码进行安全评估,包括但不限于源代码审计、漏洞扫描、成分分析等	核查开源软件引入阶段安全评估报告
		物料清单	新引入的开源软件要求有物料清单,且格式符合规范	核查开源软件是否有物料清单,其格式是否符合技术规范要求
	使用管理(10)	测试评估	进入开源代码库的软件,在使用过程中应按开发测试规范要求进行安全测试评估	核验测试环境、测试过程、测试工具、测试方法等的规范性,核查测试评估报告
		资产管理	对存量开源软件进行盘点,建立台账,开展资产动态更新管理	核查开源软件资产台账,与开源代码库比对,确认台账与开源代码库中软件是否一致
		设计与生成	在使用开源代码过程中检查开源代码设计文档完备性、兼容性、使用规范性;在编译以及链接过程中检查开源代码安全措施落地性,包括配置检查、漏洞扫描等	核验开发环境,开源代码使用过程中设计与生成是否按管理流程、技术规范执行
安全建设指标(35)	运维支持和应急处置		对开源软件建立监控、跟踪等运维机制,编制针对性的应急预案	核验开源软件监控情况,核查开源软件应急预案
		运维知识库	建立开源软件专家支持机制和运维共享知识库	核查开源软件专家库、共享知识库落实情况
	运维管理(10)		对开源代码库中正在使用的开源软件,从社区情况、安全漏洞情况、版本更新情况及开源许可证情况等方面,定期分析其信息变动情况,并及时更新,根据分析评估结果开展整改	核查定期评估报告内容完整性、及时性,以及整改情况
		定期安全评估		
	退出管理(5)	退出机制	开源代码库内确认不再使用的开源软件通过规范的退出流程和机制进行推出管理	核查管理办法,是否对开源软件退出机制、流程有明确的规定
		退出计划	根据开源软件产品替代、法律安全等情况,制定开源软件退出规划	核查开源软件退出规划
安全质量指标(30)	漏洞管理(20)	开源代码漏洞率	统计开源软件包含的代码模块的原始漏洞数量和千行漏洞率	核查漏洞监测报告,检查开源代码中每千行的已知漏洞数量,是否千行漏洞率在1.5及以下,有漏洞的开源代码中平均漏洞个数在1个及以下
		开源代码漏洞严重性	参考GB/T30279-2020《信息安全技术 网络安全漏洞分类分级指南》统计漏洞严重程度	核查漏洞分级统计清单,是否不存在中危及以上漏洞
		开源代码漏洞修复率	统计开源代码已修复漏洞在其所发现的漏洞中的占比,以及修复时间	核查漏洞修复统计清单,以及修复率,是否达到高危漏洞出现3个月内修复漏洞比例为80%及以上

续表				
一级指标(5)	二级指标(12)	三级指标(26)	指标要求	评估方法
安全合规指标(10)	版本管理(10)	开源代码版本更新	统计开源代码库中使用版本与开源社区最新发布版本的滞后情况	核查开源软件资产台账中开源代码版本记录、更新和跟踪情况,是否实现开源代码均为3年内发布较新稳定版本
	版权管理(5)	开源许可证协议	统计开源软件包含的开源代码相关许可证的规范性,例如授权范围、授权条件、违约与授权终止、免责声明等;互惠性,对自由互惠的开源许可证进行识别和风险评估,判断自研代码与开源代码之间的合规使用情况;兼容性,判断开源代码之间的许可证合规使用情况	核验开源软件的开源许可证完整性、规范性,核查开源代码成分扫描报告,确认开源代码使用的弱互惠性开源许可证是否通过弱隔离方式引入,如静态链接和动态链接等,强互惠性开源许可证是否通过强隔离方式引入,如聚合体,开源代码使用的开源许可证之间是否兼容
	专利管理(5)	开源许可证专利	统计开源软件包含的开源代码涉及专利是否得到授予,开源许可证的适用范围和出现纠纷时法律声明情况	核查开源软件资产台账中专利记录、更新、跟踪情况
		开源社区安全管理	统计开源社区安全管理情况,例如对于开源代码的安全扫描、贡献管理;签署开源贡献协议、具备代码审查机制、具备数字签名等	核查管理的开源社区声明文档是否定期发布安全问题、开源代码合并是否具备安全测试标记、贡献规则文档是否要求开源贡献者签署协议要求、是否有人进行代码审查、是否具备代码发布安全机制措施等
持续性管控指标(10)	第三方管理(5)	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及其营方基本信息	核查软件产品包含的开源代码所在的代码托管平台运营方地址是否不受国际政治、战争、贸易管制、知识产权等一种或多种国际环境影响
		开源代码下载平台	统计软件产品包含的开源代码下载平台运营方基本信息,确认开源代码下载平台对开源代码完整性具备保障情况,并据此对开源代码下载平台做出评价	核查软件产品包含的开源代码下载运营方地址是否从不受国际政治、战争、贸易管制、知识产权等一种或多种国际环境影响;开源代码官网地址的哈希值和数字签名,与软件产品使用的开源代码进行比对,验证是否被篡改
	服务连续性(5)	持续供应能力	确保引入开源代码库的开源软件版本稳定,持续跟踪版本更新情况	核验对开源代码版本的持续跟踪情况
		供应链保障能力	确保引入开源代码库的开源软件可追溯性	核验开源代码是否使用SBOM等技术确保可追溯性

3 指标体系比对

通过将本文设计的5个一级指标、12个二级指标与主流开源软件安全评价方法相比对,《网络安全技术 软件产品开源代码安全评价方法》(GB/T 43848-2024)和《开源软件治理能力评价成熟度模型》(T/CCSA 383.3-2023)指标均不如本文覆盖全面、内容翔实,说明本文开源软件安全评估模型和指标体系的科学性、完整性和实用性。指标体系对比情况如表2所示。

4 开源软件安全评估指标体系在客票系统中的应用

4.1 客票系统开源软件使用现状分析

客票系统作为核心业务系统之一,承载着海量的票务交易数据和用户信息,其稳定性与安全性至关重要。随着客票业务量的持续增长以及功能的不断拓展,客票系统通过广泛使用开源软件,有效提升了开发运维效率和降低成本。客票系统软件框架图如图3所示。

在客票系统的研发与运维过程中,使用了多种类型的

Table 2 Indicator system comparison table
表2 指标体系对比表

指标级别	本文指标内容	《网络安全技术 软件产 品开源代码安全评价方 法》(GB/T 43848-2024)	《开源软件治理能力 评价成熟度模型》 (T/CCSA 383.3- 2023)
		覆盖情况	覆盖情况
一级指标	安全管理指标	√(较简单)	√
	安全建设指标	×	√
	安全质量指标	√	×
	安全合规指标	√	×
	持续性管控指标	×	×
二级指标	组织人员	√	√
	管理制度	×	√
	引入管理	×	√
	使用管理	×	√
	运维管理	×	√
	退出管理	×	√
	漏洞管理	√	×
	版本管理	√	×
	版权管理	√	×
	专利管理	√	×
	第三方管理	×	√
	服务连续性	×	×

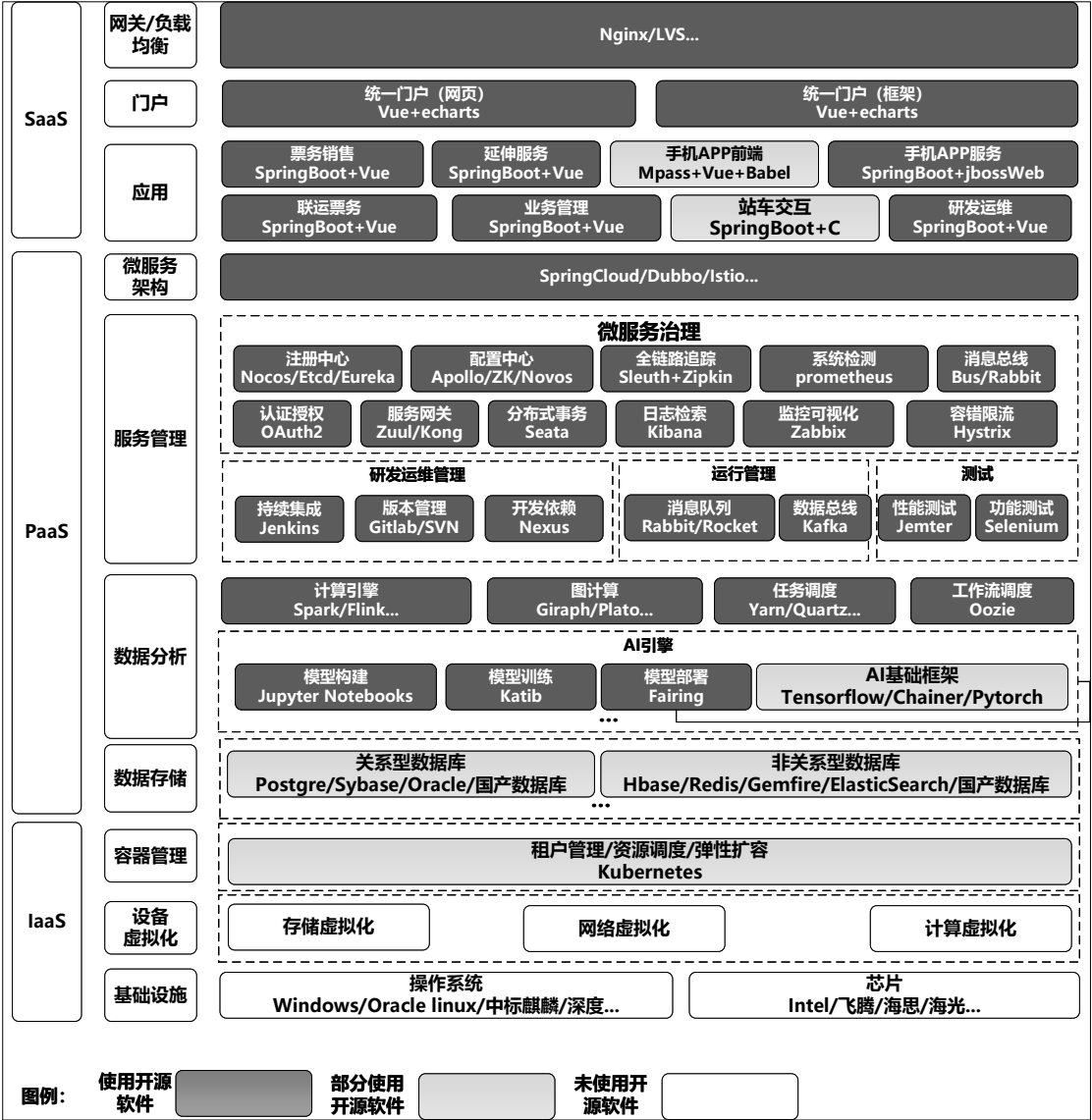


Fig. 3 Ticket system software framework diagram

图3 客票系统软件框架图

开源软件,主要包括:网关负载均衡(反向代理 Nginx 等)、门户(前端框架 Vue、echarts 等)、开源基础软件(关系数据库、容器编排工具 Kubernetes 等)、开源研发及治理框架(Java 开发框架 Spring Boot、微服务治理框架 Spring Cloud 等)、开源中间件(Java 容器 Tomcat、数据总线 Kafka 等)、开源技术组件(日志处理 Log4j、认证授权 OAuth2 等)、开源数据处理组件(数据计算 Spark、Flink 等)、开源研发工具(源代码托管 Gitlab CE、持续集成 Jenkins 等)、开源智能算法与模型(模型训练 Katib、大语言模型 DeepSeek R1 等)和开源运行监控工具(基础设施监控 Zabbix、Prometheus 等)等。近两年,客票系统针对各业务子系统的开源软件使用情况开展了针对性收敛与调整。目前,客票系统共使用开源软件 80 余个、开源组件 2 000 余个,每个开源软件版本控制在 2~3 个。

随着开源软件在客票系统中的应用日益广泛,其安全风险也随之凸显:一方面,开源漏洞频发、许可风险事件屡

有发生;另一方面,客票系统本身面临复杂多变的网络环境与安全风险。双重因素使得开源软件成为影响系统安全稳定运行的潜在风险点。在此背景下,仅依靠零散的安全评估已难以应对,对客票系统开展系统性、全流程的开源软件评估与治理,成为保障其安全运行的必然要求,具有迫切的现实意义。

4.2 指标体系应用流程与方法

根据开源软件安全评估指标体系,对客票系统中开源软件的相关数据进行全面收集。

(1)从安全管理指标角度,收集客票系统开源软件管理的组织架构信息,包括负责开源软件管理的部门设置、人员配备情况以及相应的资源投入明细;整理与开源软件相关的制度流程文件和技术规范文档。

(2)在安全建设指标方面,获取开源软件引入时的评估报告、物料清单,记录使用过程中的测试评估数据、资产管理信息,以及运维阶段的运维支持记录、应急处置预案

和实施情况、运维知识库内容更新记录、定期安全评估报告等。

(3) 针对安全质量指标,借助专业的漏洞扫描工具,收集客票系统中开源代码的漏洞率、漏洞严重性以及漏洞修复率数据,同时,掌握开源代码版本更新情况。

(4) 在安全合规指标上,梳理客票系统使用的开源软件所遵循的开源许可证协议和涉及的专利信息。

(5) 针对持续性管控指标,收集开源社区安全管理措施、开源代码托管平台和下载平台的相关信息,以及客票系统中不被支持的系统组件情况。

4.3 指标评分

根据收集到的数据,按照开源软件安全评估指标体系中设定的各指标分值比例,对客票系统中的开源软件进行逐项评分。例如,在安全管理指标的组织人员二级指标下,若客票系统设有专门的开源软件管理部门,且人员具备相

应的专业技能和经验,资源投入充足,则可给予组织机构、岗位人员和资源投入较高的分数;若制度流程完善、技术规范明确,在管理制度二级指标下也能获得较好的评分。

在安全质量指标的漏洞管理方面,若开源代码漏洞率低、漏洞严重性低且修复率高,则在开源代码漏洞率、开源代码漏洞严重性和开源代码漏洞修复率这 3 个三级指标上就能得到较高分值;若开源代码版本更新及时,开源代码版本更新指标也可获得相应分数。以此类推,对每个一级指标下的所有二级和三级指标进行客观评分。

4.4 综合评估与分析

将各个指标的评分结果进行汇总,根据一级指标的分值权重,计算出客票系统开源软件安全评估的综合得分。通过对综合得分的分析,判断客票系统中开源软件的整体安全状况。客票系统开源软件事项整体安全状况如表 3 所示。

Table 3 Overall security status of open source software for ticket system

表 3 客票系统开源软件事项整体安全状况

二级指标	客票系统实现内容	评分
组织人员(10)	从组织架构着手,以系统安全人员为主,抽调架构研发人员、测试人员、开源课题科研人员设立了专门的开源软件安全管理部门,该部门职责清晰、分工明确,涵盖了从风险评估、漏洞监测到策略制定等多方面工作。同时,增加了专业的开源软件安全管理人员,这些人不仅具备扎实的网络安全知识,还深入了解开源软件的特性与运行机制,通过定期的内部培训和外部进修,不断提升其专业素养与实践能力,以更好地应对复杂多变的开源软件安全挑战	9
管理制度(10)	部门开源软件安全管理职责考核、人员专业素质培养等需持续改进 在制度流程和技术规范的完善上,制定了网络安全管理办法,单独篇章描述供应链安全管理,该办法对软件供应链的全生命周期管理进行了规范,涵盖开源软件从引入前的评估审核、使用过程中的监控维护,到退出时的清理流程都做出了明确规定。技术规范方面,参考国内外先进标准并结合客票系统的实际需求,制定了严格的技术准则,包括代码编写规范、安全配置标准等,确保开源软件在系统中的运行符合高安全性要求 制度覆盖度还需进一步完善,例如专门针对开源软件的漏洞管理、运维管理(应急预案)、第三方管理、物料清单规范等	7
引入管理(5)	安全建设过程中,着重加强了开源软件引入评估工作。组建了由技术专家、业务骨干和法务人员构成的评估团队,从技术可行性、安全风险、业务适配性以及法律合规性等多个维度对拟引入的开源软件进行全面评估。在引入评估环节,建立了一套科学的评估指标体系,对开源软件的功能完整性、性能表现、漏洞情况、社区活跃度等关键指标进行量化评估,只有通过严格评估的开源软件才允许进入客票系统	4
使用管理(10)	物料清单的使用需扩大使用范围,对库存开源代码物料清单进行梳理补充 在使用管理方面,强化了资产管理,对客票系统中使用的开源软件进行详细登记,记录其版本信息、使用场景、依赖关系等关键数据,实现了开源软件资产的可视化管理。同时,优化了测试评估环节,制定了全面的测试计划,涵盖功能测试、性能测试、安全测试等多个方面,确保开源软件在集成到客票系统后能够稳定运行且不引入新的安全风险。在设计生成阶段,遵循安全开发原则,将安全要求融入到软件设计和开发的每一个环节,从源头上降低安全风险	8
运维管理(10)	生成阶段编译以及链接过程中检查开源代码安全措施,包括配置检查、漏洞扫描等仍需进一步落地落细 在运维管理方面,建立了更为完善的运维支持和应急处置机制。组建了专业的运维团队,提供 7×24 小时的值班监控和技术支持,并在节假日及国家重要事件(如两会、奥运会等)期间,提供额外重点保障,确保在开源软件出现问题时能够及时响应和处理。制定了详细的应急处置预案,针对不同类型的安全事件,如漏洞暴发、恶意攻击等,明确了应急处理流程和责任分工,定期组织应急演练,提高团队的应急响应能力。此外,搭建了运维知识库,将开源软件的运维经验、常见问题及解决方案进行整理和归档,方便运维人员快速查询和学习,提升运维效率。同时,严格执行定期安全评估制度,按照既定的评估周期对客票系统中的开源软件进行全面检查和评估,及时发现潜在的安全隐患并采取相应的整改措施	7
退出管理(5)	针对开源软件的监控、跟踪等运维机制仍需进一步落实,特别是编制针对性的应急预案 在退出管理方面,建立了规范的退出机制和详细的退出计划。当开源软件不再适用于客票系统或存在严重安全风险时,按照退出机制的规定,有序地进行软件卸载、数据清理等工作,并确保相关业务不受影响。退出计划明确了每个阶段的工作任务、责任人和时间节点,保证退出过程的顺利进行	4
	退出管理需在实际应用中不断完善机制流程,持续改进	

续表		
二级指标	客票系统实现内容	评分
漏洞管理(20)	在安全质量上,通过定期的漏洞扫描和修复,开源代码漏洞率显著降低。采用多种专业的漏洞扫描工具,定期对客票系统中的开源代码进行全面扫描,及时发现并记录漏洞信息。对于发现的漏洞,根据其严重性进行分类分级,制定相应的修复策略和时间表,确保高风险漏洞能够在最短时间内得到修复。同时,持续关注开源代码漏洞修复率,通过优化修复流程、加强技术支持等方式,不断提高漏洞修复的效率和质量	16
版本管理(10)	漏洞修复需进一步落实,尽快实现千行漏洞率在1.5及以下,有漏洞的开源代码中平均漏洞个数在1个及以下 在开源代码版本更新方面,建立了版本监控机制,及时获取开源软件的新版本信息,评估新版本的稳定性和安全性,在确保不影响客票系统正常运行的前提下,及时进行版本更新,以获取更好的性能和安全特性	10
版权管理(5)	在知识产权管理方面,通过建立严格的审查机制,确保了所有开源软件使用均符合相关许可证协议和知识产权规定。在开源软件引入阶段,法务人员对开源软件的许可证协议进行详细审查,确保其使用方式符合许可证要求,避免因许可证违规使用而引发法律风险	5
专利管理(5)	对涉及的开源许可证专利进行梳理和排查,确保客票系统的使用行为不侵犯他人的知识产权。定期对开源软件的使用情况进行合规性检查,及时发现并纠正潜在的合规问题	5
第三方管理(5)	在持续性管控方面,积极与开源社区建立了更紧密的联系。安排专人负责与开源社区沟通交流,及时获取社区发布的安全公告、更新信息以及技术支持。参与开源社区的讨论和开发活动,为社区贡献力量的同时,也能更好地了解开源软件的发展趋势和潜在风险。加强了对开源代码托管平台和下载平台的监控,建立了平台风险评估机制,定期对托管平台和下载平台的安全性、稳定性进行评估,确保从这些平台获取的开源代码安全可靠。同时,密切关注不被支持的系统组件,及时制定替代方案,避免因组件停止支持而导致安全风险和业务中断	3
服务连续性(5)	开源社区、开源代码托管平台和下载平台较多、更新速度快,管理难度较大,第三方管理需在实践中不断摸索、提升 在服务连续性方面,持续跟踪产品供应情况,确保核心团队稳定、核心部件安全可控,供应链稳定可追溯 服务连续性管理需持续跟踪	4
总分(100)	客票系统在“组织人员”“引入管理”“使用管理”“退出管理”“版本管理”“版权管理”“专利管理”“第三方管理”和“服务连续性”方面管理较为规范。管理制度覆盖度还需进一步完善,运维管理中对开源软件的监控、跟踪等运维机制仍需进一步落实,漏洞修复需进一步落实,尽快提高漏洞修复率	82

由表3可知,应用开源软件安全评估指标体系后,客票系统对其使用的开源软件进行了全面梳理与评估,最终得分为82分。评估结果显示,客票系统的开源软件安全水平处于持续改进级,在“管理制度”“运维管理”“漏洞管理”“第三方管理”等指标方面仍需进一步加强改进力度。

5 结语

本文设计了开源软件安全评估模型和指标体系,并成功应用于客票系统。通过安全评估,发现并明确了客票系统在开源软件安全管理与技术措施方面存在的差距,从而指导客票系统在重点指标上进行改进与提升。结果表明,客票系统的稳定性和可靠性得到显著增强,未发生因开源软件安全问题引发的网络攻击事件,为旅客提供了更加安全且便捷的购票服务。这一实践同时也验证了该安全评估模型和指标体系的科学性、有效性和实用性,为其他业务系统的开源软件安全管理提供了有益的参考和借鉴。

参考文献:

[1] LI X B, WANG G L, SUN Z W, et al. Summary of researches on ict supply chain security evaluation technology[J]. Information Security and Communications Privacy, 2018(10): 57-64.
李祥兵,王光林,孙志伟,等. ICT供应链安全评价技术研究综述[J]. 信息安全与通信保密, 2018(10): 57-64.

[2] JI S L, WANG Q Y, CHEN A Y, et al. Survey on open-source software supply chain security[J]. Journal of Software, 2023, 34(3): 1330-1364.
纪守领,王琴应,陈安莹,等. 开源软件供应链安全研究综述[J]. 软件

学报, 2023, 34(3): 1330-1364.

[3] YUAN H J, ZHAO R, TANG G. Analysis and prevention of security risk for open source software[J]. Information Security and Communications Privacy, 2023(2): 125-134.
袁豪杰,赵冉,唐刚. 面向开源软件的安全风险分析与防范[J]. 信息安全与通信保密, 2023(2): 125-134.

[4] LUO D, WU R C. Development status and risk analysis of domestic open source software[J]. Communications World, 2022(15): 33-34.
罗丹,吴荣春. 国内开源软件的发展现状与风险分析[J]. 通信世界, 2022(15): 33-34.

[5] National Internet Emergency Center. 2021 open source software supply chain security risk research report[EB/OL]. <https://www.cert.org.cn/publish/main/upload/File>.
国家互联网应急中心. 2021年开源软件供应链安全风险研究报告[EB/OL]. <https://www.cert.org.cn/publish/main/upload/File>.

[6] Synopsys. 2022 open source security and risk analysis report[EB/OL]. <https://www.fxbagao.com/detail/3226120>.

[7] 2023 open source security and risk analysis report[R]. Synopsys, 2023(2): 1-19.

[8] Synopsys. 2024 safety and risk analysis report[EB/OL]. <https://www.synopsys.com/zh-cn/softwareintegrity/resources/analyst-reports/open-source-securityrisk-analysis.html>.

[9] PANG L Y. Highlights and insights of the US open source software security roadmap[J]. Network Security Technology & Application, 2025(2): 141-142.
鹿林源. 美《开源软件安全路线图》亮点与启示[J]. 网络安全技术与应用, 2025(2): 141-142.

[10] GAO H J. Research on security governance of open source software in the United States[J]. Confidentiality Science and Technology, 2024(3):

- 43-49.
- 高红静. 美国开源软件安全治理研究[J]. 保密科学技术, 2024(3): 43-49.
- [11] YUAN W. Promote open source software supply chain security and evaluation. [J]. Software and Integrated Circuit, 2024(9): 44-45.
- 袁薇. 推动开源软件供应链安全保障与测评[J]. 软件和集成电路, 2024(9): 44-45.
- [12] SU W X. Open source software supply chain security evaluation model and application[J]. Industry Information Security, 2025(2): 27-35.
- 苏文星. 开源软件供应链安全评价模型与应用[J]. 工业信息安全, 2025(2): 27-35.
- [13] WU Z H, ZHANG C, SUN H, et al. Application research of program reverse analysis in pollution detection of software supply chain: a survey [J]. Journal of Computer Applications, 2020, 40(1): 103-115.
- 武振华, 张超, 孙贺, 等. 程序逆向分析在软件供应链污染检测中的应用研究综述[J]. 计算机应用, 2020, 40(1): 103-115.
- [14] HASSIJA V, CHAMOLA V, GUPTA V, et al. A survey on supply chain security: application areas, security threats, and solution architectures[J]. IEEE Internet of Things Journal, 2021, 8(8): 6222-6246.
- [15] DONG G W. The Construction of software supply chain security standard system from the perspective of US executive orders[J]. China Information Security, 2022(2): 84-87.
- 董国伟. 从美行政令看软件供应链安全标准体系的构建[J]. 中国信息安全, 2022(2): 84-87.
- [16] CCIA Cybersecurity Industry Alliance. ICT research on supply chain security policies, regulations, and standards[EB/OL]. <https://mp.weixin.qq.com/s/REjvYcIy7wsLauAgsV23A>.
- CCIA 网安产业联盟. ICT 供应链安全政策法规和标准研究[EB/OL]. <https://mp.weixin.qq.com/s/REjvYcIy7wsLauAgsV23A>.
- [17] China Electronics Standardization Institute (CESI), National Research Center for Information Technology Security (NCFITS), et al. GB/T 31495. 2-2015. Information security technology—information security assurance indicator system and evaluation method—Part 2: Indicator system[S].
- 中国电子技术标准化研究院, 国家信息技术安全研究中心等. GB/T 31495. 2-2015. 信息安全技术 信息安全保障指标体系及评价方法 第2部分 指标体系[S].
- [18] China Electronics Standardization Institute, National Research Center for Information Technology Security, China Information Technology Security Evaluation Center, et al. GB/T 36630. 1-2018. Information security technology—security-controllable evaluation indicators for information technology products—Part 1: General[S].
- 中国电子技术标准化研究院, 国家信息技术安全研究中心, 中国信息安全测评中心等. GB/T 36630. 1-2018. 信息安全技术 信息技术产品安全可控评价指标 第1部分: 总则[S].
- [19] National Research Center for Information Technology Security, NCFITS. GB/T 39204-2022. Cybersecurity technology: key performance indicators for critical information infrastructure security protection capability[S].
- 国家信息技术安全研究中心. GB/T 39204-2022. 网络安全技术 关键信息基础设施安全保护能力指标体系[S].
- [20] China Electronics Standardization Institute, National Research Center for Information Technology Security, et al. GBT 43848-2024. Cybersecurity technology—security assessment method for open source code in software products[S].
- 中国电子技术标准化研究院, 国家信息技术安全研究中心等. GBT 43848-2024. 网络安全技术 软件产品开源代码安全评价方法[S].
- [21] China Academy of Information and Communications Technology, China Electronics Standardization Institute, et al. T/CCSA 383. 3-2023. China Academy of Information and Communications Technology (CAICT) open source software governance capability evaluation maturity model[S].
- 中国信息通信研究院, 中国电子技术标准化研究院等. T/CCSA 383. 3-2023. 信通院开源软件治理能力评价成熟度模型[S].

(责任编辑: 陈维捷)