



目 录

一、概述	1
1、软件供应链安全攻击手段依然花样百出	1
2、国内企业软件供应链安全状况有所改善	4
二、国内企业自主开发源代码安全状况	6
1、编程语言分布情况	6
2、典型安全缺陷检出情况	7
三、开源软件生态发展与安全状况	8
1、开源软件生态发展状况分析	9
2、开源软件源代码安全状况分析	11
(1) 编程语言分布情况	11
(2) 典型安全缺陷检出情况	12
3、开源软件公开报告漏洞状况分析	13
(1) 大型开源项目漏洞总数及年度增长 TOP20	13
(2) 主流开源软件包生态系统漏洞总数及年度增长 TOP20	16
4、开源软件活跃度状况分析	19

(1) 68.7%的开源软件项目处于不活跃状态， 比例下降19



(2) 版本频繁更新的项目较去年增长 21.6%	20
5、关键基础开源软件分析	21
(1) 主流开源生态关键基础开源软件 TOP50	21
(2) 关键基础开源软件的漏洞披露情况未见改善	24
(3) 关键基础开源软件的整体运维风险有所改观	25
6、NPM 生态中恶意开源软件分析	26
(1) 超 95%的恶意开源组件以窃取敏感信息为目标	26
(2) 典型恶意开源组件及恶意行为剖析	27
四、国内企业软件开发中开源软件应用状况	29
1、开源软件总体使用情况分析	30
(1) 平均每个软件项目使用 166 个开源软件，再创新高	30
(2) 最流行的开源软件被 37.2%的软件项目使用	31
2、开源软件漏洞风险分析	32
(1) 存在容易利用的开源软件漏洞的项目占比大幅下降	32
(2) 平均每个项目包含的已知开源软件漏洞数明显回落	33
(3) 影响最广的开源软件漏洞的影响范围有所减小	35
(4) 20 多年前的开源软件漏洞仍然存在于多个软件项目中 ..	36
3、开源软件许可协议风险分析	37
(1) 最流行的开源许可协议在 46.9%的项目中使用	37



(2) 超 1/5 的项目使用了含有超、高危许可协议的开源软件 .	38
4、开源软件运维风险分析	40
(1) 多个二三十年前的老旧开源软件版本仍在使用	40
(2) 开源软件各版本使用依然混乱	41
五、典型软件供应链安全风险实例分析	42
1、多款主流操作系统供应链攻击实例分析	42
2、PHP 软件供应链攻击实例分析	43
3、某国产数据库供应链攻击实例分析	45
六、总结及建议	47
附录：奇安信代码安全实验室简介	51



一、概述

当前，软件供应链安全依然是网络安全中备受关注的方向，基于自研产品的技术能力和第一手实测数据，奇安信代码安全实验室继续推出《2024 中国软件供应链安全分析报告》，即本系列年度分析报告的第四期。

软件由自主开发的代码与开源代码等第三方代码集成后，形成混源代码，然后通过编译、连接等构建过程形成软件产品，交付给用户使用。在这一软件供应链模型中，每个阶段中的代码或工件都可能引入安全问题，从而导致最终软件供应链安全事件的爆发。

本期报告仍以此模型为基础，分析各阶段的代码安全问题对软件供应链安全性的潜在威胁，分析内容分别在后续的国内企业自主开发的源代码安全状况、开源软件生态发展与安全状况、国内企业软件开发中开源软件应用状况、典型软件供应链安全风险实例分析等章节中呈现。在此基础上，本报告还总结了趋势和变化。与往年报告相比，本期报告在开源软件生态发展与安全部分新增了对 NPM 生态中恶意开源软件分析的内容；在典型软件供应链安全风险实例部分，通过实例再次验证了因软件供应链的复杂性，“外来”组件的“老漏洞”发挥“0day 漏洞”攻击作用的状况。感兴趣的读者可重点关注。

1、软件供应链安全攻击手段依然花样百出

过去的一年中，软件供应链安全攻击事件没有丝毫减少的趋势，

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。
。如要下载或阅读全文，请访问：

<https://d.book118.com/196141024153010213>