国内外软件供应链安全现状分析与对策建议

Analysis and Countermeasures on Current Situation of Domestic and Overseas Software Supply Chain Security

苏俐竹,徐　雷,郭新海,张曼君,丁　攀(中国联通研究院,北京 100048)
Su Lizhu,Xu Lei,Guo Xinhai,Zhang Manjun,Ding Pan(China Unicom Research Institute,Beijing 100048,China)

摘　要:
近年来,全球软件供应链安全事件频发,影响面也越来越大。软件供应链安全已成为一个全球性问题。如何更全方位、更有效地保障软件供应链的安全,对于我国软件产业的发展和数字化进程的推进具有重要意义。主要分析了国内外软件供应链的安全现状,根据现状全面分析了软件供应链的安全风险,并提出了如何防范和管理。另介绍了国际软件供应链监管和标准,软件供应链管理建议,最后对软件供应链安全的发展趋势进行了分析和展望。

关键词:
软件供应链;网络与信息系统安全;供应链风险管理
doi:10.12045/j.issn.1007-3043.2022.09.006
文章编号:1007-3043(2022)09-0024-03
中图分类号:TN915.08
文献标识码:A
开放科学(资源服务)标识码(OSID):

Abstract:
In recent years, global security incidents in the software supply chain have occurred frequently, and the impact is growing. Software supply chain security has become a global issue. How to ensure the security of the software supply chain in a more comprehensive and effective way is of great significance to the development of the software industry and the advancement of the digitization process in China. It mainly analyzes the security status of the software supply chain in domestic and overseas, comprehensively analyzes the security risks of the software supply chain according to the security status, and puts forward how to prevent and manage them. In addition, the international software supply chain supervision and standards, software supply chain management recommendations are introduced. Finally, the development trend of software supply chain security is analyzed and prospected.

Keywords:
Software supply chain;Network and information system security;Supply chain risk management

引用格式:苏俐竹,徐雷,郭新海,等. 国内外软件供应链安全现状分析与对策建议[J]. 邮电设计技术,2022(9):24-26.

1 国内外软件供应链安全现状

2019年,新型冠状病毒的肆虐从根本上改变了人们的生活和工作方式,在疫情状况下,软件供应链的安全越来越引起人们的关注。虽然国际社会已经加强软件供应链的安全性管理,但为了更好地应对软件供应链的安全风险,研究者还需详细了解软件供应链的背景和发展,为更好地发展软件供应链安全做出更大的贡献。

1.1 国际软件供应链安全发展现状

自软件供应链的概念提出以来,国际社会对软件供应链的安全性给予了高度重视。

在国家层面,出于对软件供应链的安全性和脆弱性的担忧,多年前多国便开始规划国家软件供应链的安全策略,出台了一系列相关政策和重点项目,以便加强软件供应链的安全控制。

从企业层面,开源软件作为软件供应链中最重要的部分,世界上许多知名企业都在加大对软件供应链的安全风险管理,并利用开源软件的软件构件分析技术,确保第三方开源构件的安全。

1.2 国内软件供应链安全发展现状

随着网络安全形势的发展,我国高度重视软件供

收稿日期:2022-08-04

应链安全。2017年6月，中国发布并实施了《网络产品和服务安全审查办法》，确保软件产品测试、交付和技术支持过程中供应链的安全，并作为重点审查内容。2020年4月27日，国家互联网信息办公室等12个部门联合发布《网络安全审查办法》，要求重点信息基础设施运营商在购买网络产品和服务时，如若可能影响国家安全，应进行网络安全审查。该政策的发布代表明确地将软件供应链安全纳入了国内公众的视野。

在企业层面，中国领先的互联网企业和安全制造商已经开始投资软件供应链的安全建设，重点确保软件供应链的安全，并充分发挥创新技术在软件供应链网络安全保障中的作用，增加软硬件安全检测分析、攻击和反渗透、源代码安全审计、漏洞挖掘、大数据分析等技术，有效保障软件供应链的安全，构建动态安全防护体系。

1.3 软件供应链的安全挑战

1.3.1 国际竞争加剧，软件供应链完整性受到挑战

软件供应链的竞争与保障不仅关系到企业的生存与发展，而且成为世界各国相互制约和竞争的重要手段。一些西方国家通过实行严格的技术封锁，建立完善的出口管制法律体系，并将自己的软件、硬件和技术列入《进口管制清单》，导致国际软件供应链的竞争环境加剧，软件供应链的完整性面临严峻挑战。同时，需要制定软件供应链战略规划，确保我国软件供应链的自主性、可控性和安全性。

1.3.2 软件开源趋势增强，安全风险加剧

开源作为创新的基础，不断推动着信息技术的深度创新发展，随着开源软件的复杂性增高，其出现安全事件的概率会呈现指数级增长。一旦出现安全问题，将会产生蝴蝶效应，软件供应链会产生非常严重的影响。例如，一个开放源代码软件具有未知的安全漏洞，它将导致所有具有相关依赖关系的软件系统中存在相同的漏洞，并且漏洞攻击面将显示从点到面的爆炸性放大效应。

2021年，Sonatype发布了“2021软件供应链状况报告”。报告数据显示，开源供应、需求和安全漏洞都呈现“爆炸性”增长。其中，开源供应增加了20%，开源需求增加了73%，开源攻击激增了650%。开源安全和依赖管理在“2021软件供应链”中占据主导地位。

1.3.3 开源漏洞在流行项目中普遍存在

据统计，29%的流行开源项目至少包含一个已知的安全漏洞，只有6.5%的非热门项目未包含已知漏洞。从臭名昭著的2017年Equifax Struts事件可以看出，因为开源漏洞在发布后没有修补，导致此事件利用公开披露的开源漏洞进行攻击。在下一代软件供应链攻击行为中更为险恶的是，黑客不再用公开披露的漏洞来进行攻击。相反，他们采取主动，将新的漏洞注入到为全球供应链提供支持的开源项目中，然后利用这些漏洞进行攻击。下一代软件供应链攻击趋势如图1所示。

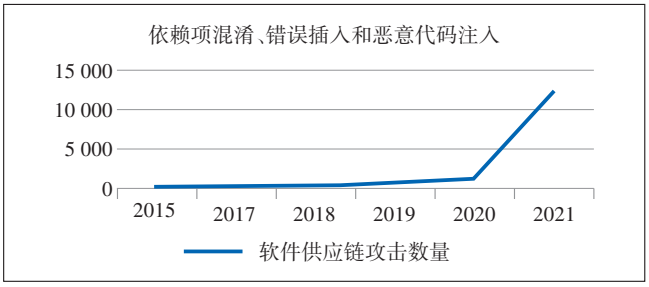

图1　下一代软件供应链攻击趋势（2015—2021）

2 国际软件供应链监管和标准

2.1 美国

在2021年，美国联邦政府针对软件供应链采取以下行动。

2021年2月，拜登总统发布行政命令（EO），列出所有供应链（包括软件）的安全条例。同年2月份，国防部首席信息官（DoD CIO）推出了零信任参考体系架构（ZTA），此架构概述了各种零信任支柱和功能，包括保护应用程序和软件供应链安全。

2021年4月，美国开始正式制定软件供应链标准（CISA），国家研究所标准和技术（NIST）发布论文《防御软件供应连锁攻击》。这2个文件强调了软件供应链攻击受损对政府、关键基础设施和私营部门软件客户的广泛影响。

2021年5月，拜登签署了第2份软件供应链行政命令，这一次是对国家网络安全态势的批判性审视。EO中“关于改善国家网络安全”的条例是美国政府关于软件供应链安全的一个里程碑。此外，EO制定了一个详细的计划，以采取措施保护联邦软件。

2021年7月，NIST发布了概述指南《关键软件使用安全措施》。同年7月份，国家电信信息管理局（NTIA）发布了SBOM的最低定义，这是一个提高软件透明度的关键步骤。

2.2 英国

2021年5月，英国政府宣布正在寻求“关于防范数

字技术的建议”，因为供应链相互关联，供应商的漏洞产品和服务逐渐增多，成为更吸引攻击者的目标。同年5月，英国数字、文化部，媒体和体育部（DCMS）开展了一项调查，并邀请行业专家和技术组织在英国各地加强供应链安全。该倡议表明英国越来越重视保护数字供应链安全。

2.3 德国

2021年5月，德国通过了《信息技术安全法案2.0》。作为第1部法案的更新，该法案影响到德国IT行业许多领域，但它明确规定，供应商，即关键组件制造商，也将承担一定的义务，以保护整个供应链安全。

3 软件供应链安全管理建议

软件供应链的安全管理是一项系统工程，需要从国家和行业2个层面入手。各级机构和企业应及时建立发现、分析、处理和保护软件供应链安全风险的能力，并从整体上改进软件供应链安全管理水平。因此，有必要对软件供应链安全检测与防御的方法和技术进行全方位地研究，确保ICT供应的完整性和ICT产品的供应链安全，防止恶意ICT扩散工具和技术以及有害隐藏功能的使用。现今，全球ICT供应链日益复杂并相互依存，其中确保完整性、稳定性和供应链安全可以从以下几方面入手。

第一，开展软件构件动态分析和开源应用缺陷智能检测技术研究，突破高效准确的开源应用安全缺陷检测状态检测技术的瓶颈，解决基于全代码遍历和代码片段级克隆技术，以提升应用程序安全检测问题，并进一步实现全球开源应用程序的全面安全检查，从源头上阻断软件供应链的安全风险。

第二，在全球范围内推广开源应用程序安全意识和预警机制，攻克软件供应链中软件源的多态跟踪技术，实现供应链各个环节中软件源的可追溯性。在国家一级实施全面、透明、客观和公正的框架和机制以保证供应链风险管理。通过软件源多态性跟踪技术监控，和开源应用的使用、传播和分布式部署，通过通信和使用渠道全面掌握有缺陷的开源应用，可以实现对全球开源应用及其安全缺陷的预测和预警。

第三，制定政策和方案。需要更多关注国家政策，并与各国和相关国家进行对话。确保所有国家都能平等竞争创新，使ICT安全与全面实现全球社会经济发展相辅相成，有助于维护国际和平与安全，同时也保障国家安全和公共利益。

第四，建立国家/行业软件供应链安全监控平台，配备系统化、规模化的软件源代码缺陷检测，和异常行为代码分析、软件漏洞分析、开源软件组件风险分析和其他关键功能。为关键基础设施和重要信息系统的用户提供日常自检服务，及时发现并处理软件供应链安全风险。

第五，严格控制软件供应链的上游，特别是开源应用程序的使用，推动区块链等新技术在软件供应链安全领域的推广应用，利用区块链的安全信任机制从根本上提高软件供应链安全的可靠保障。

4 展望

软件供应链逐渐开源化对整个软件供应链的各个环节都产生了不可避免的影响，尤其是开源应用程序的安全性，将直接影响使用。开源应用程序中的众多安全问题极大地增加了软件供应链中的安全风险，以及安全状况。

随着人工智能和自动化恶意攻击技术的不断升级，专门针对软件供应链的攻击趋势显著加强。软件供应链安全已成为网络空间攻防对抗的焦点，并且直接影响到关键基础设施和数字经济的安全。过去2年中，受疫情的影响，人们的生活和工作方式，以及商业实体和数字供应链的运作方式都发生了根本性的变化。今天，当数字创新推动经济发展时，如果企业和开发商希望避免由使用软件供应链带来的网络攻击，或者希望为软件供应链管理带来一些创新，那就要思考如何从技术创新的角度，为产业搭建一个汇集“国家、行业、机构、企业”等综合力量，且“同向、同心”的软件供应链安全保障生态体系。

参考文献：

[1] Sonatype. 2021 state of the software supply chain[R/OL]. [2022-04-25]. https://www.sonatype.com/resources/state-of-the-software-supply-chain-2021.

[2] 刘权，王超. 加强软件供应链安全保障的对策建议[J]. 中国信息安全，2018(11)：64-66.

作者简介：

苏俐竹，毕业于新西兰怀卡托大学，工程师，硕士，主要从事网络与信息安全研究工作；徐雷，毕业于北京理工大学，教授级高级工程师，博士，主要从事网络与信息安全研究工作；郭新海，毕业于北京交通大学，工程师，硕士，主要从事网络与信息安全研究工作；张曼君，毕业于西安电子科技大学，高级工程师，博士，主要从事网络与信息安全研究工作；丁攀，毕业于北京化工大学，工程师，硕士，主要从事网络与信息安全研究工作。