信息安全研究 第7卷 第9期 2021年9月
Vol.7 No.9 Sept. 2021

开源软件供应链安全风险分析

齐 越 刘金芳 李 宁
(中国网络安全审查技术与认证中心 北京 100020)
(qiy@isccc.gov.cn)

The Analysis of Security Risk in Open Source Software Supply Chain

Qi Yue, Liu Jinfang, and Li Ning
(*China Cybersecurity Review Technology and Certification Center*, *Beijing* 100020)

Abstract Currently, open source software is widely used in network products and has become an important part of the software supply chain. However, its security and controllability issues have become increasingly prominent. Western countries' dominant advantages in open source organizations and open source project policies have a great impact on the security of china's corresponding network product supply chains. Starting from the cybersecurity, this article combines the analysis results of the open source software code components to study and analyze the security risks in the open source software supply chain, and proposes suggestions for improving the safety management of open source software supply chain.

Key words security risk; cybersecurity; open source software; supply chain; network product

摘 要 当前,网络产品中大量应用了开源软件,开源已成为软件供应链中的重要一环,其安全性和可控性问题日渐突出.西方国家对开源组织及开源项目政策上的主导优势,对我国相应网络产品供应链安全产生了极大影响.从网络安全工作出发,结合软件开源代码成分分析结果,对开源软件供应链存在的安全风险进行了研究和分析,提出完善开源软件供应链安全管理的建议.

关键词 安全风险;网络安全;开源软件;供应链;网络产品

中图法分类号 TP319

近年来,随着我国互联网的蓬勃发展,电子产品和网络设备逐渐深入人民群众的日常生活,成千上万的网络产品和服务构建起了我们日常使用的通信网络和信息系统.为保障国家网络安全,2017年6月1日《中华人民共和国网络安全法》正式实施,第31条提出,通信、能源、交通、水利、金融、公共服务等重要行业和领域的信息系统一旦遭到破坏、丧失功能或者发生数据泄露,将会严重危害国家安全、国计民生和社会公共利益.在此前提下,重点行业信息系统使用的产品和服务面临的网络安全问题,应引起我们足够的重视.为了防止信息系统遭受到不法侵害,防范可能存在的网络安全风险,以网络产品和服务供应链安全作为切入点,着眼于加强供应链各环节的安全保障能力,提升网络产品和服务供应链安全管理水平,成为目前最有效、最务实的安全策略.

收稿日期:2021-03-04

网络产品和服务供应链包括了产品的核心部件、软件代码及生产制造运维过程中涉及的相关环节，其中，软件是供应链极其重要的组成部分.近年来，开源软件以其开放、共享、便捷等特点迅猛发展，逐渐成为信息系统软件开发的基础.作为软件供应链的重要一环，开源甚至形成了一种行业生态，开源软件在网络产品供应链安全中的重要位置也日益显现.

1 开源软件应用现状

随着开源软件在软件研发过程中的应用范围不断扩大，开源正进入生活的方方面面，包括我们日常使用的手机、平板等电子产品，以及大型计算机、服务器等组成的系统中都有开源软件的身影.开源软件的重要性主要体现在：一方面市场上包含开源组件的软件逐渐增多，据美国弗雷斯特研究公司(Forrester Research)统计，全球 80%以上的应用软件使用了开源组件[1]，在能源、通信、金融、互联网等行业内这一比例甚至高达 95%；另一方面软件中开源代码的比例不断升高，2019 年新思科技公司(Synopsys)通过对全球 1 200 个商业代码库的分析发现，在包含开源成分的软件中，开源代码占代码总量的平均比例由 2018 年的 57%提高到了 60%[2].从不同行业领域来看，移动互联网行业这一比例为 74%，网络安全行业为 70%，能源、金融、物联网等行业开源代码比例均在平均值 60%以上.这些行业均是关系国计民生、公共利益的重点行业.

目前，国际上应用的开源代码大都掌握在知名开源组织手中.这些开源组织主要包括：

1) Apache 基金会.

Apache 基金会成立于 1999 年，注册地位于美国特拉华州.基金会主要由个人捐赠和企业赞助商资助形成，主要任务是为其管理的开源软件提供持续的技术支持.Apache 基金会目前收录了包括 HTTP Server，Hadoop，Tomcat 等知名项目在内的 350 多个开源项目，这些开源项目推动了 Web 服务和大数据技术的快速发展.作为世界最大的开源组织，Apache 基金会管理的代码达到了 2 亿多行.

2) Linux 基金会.

Linux 基金会成立于 2000 年，致力于促进 Linux 操作系统及其生态的发展.基金会为 Linux 提供了一个有利于协作和推广的开放代码平台，为解决软件开发商和用户面临的 Linux 生态系统问题提供了基础，促进并保护了 Linux 的发展.Linux 基金会内部形成了用于应用程序开发的标准服务，推动了 Linux 在全球的标准化.目前，Linux 项目的开源代码量已经超过 2 500 万行.

3) OpenStack 基金会.

OpenStack 基金会 2012 年在美国成立，其管理的最著名的开源项目为 OpenStack 云计算项目.OpenStack 项目由美国国家航空航天局和云服务商 Rackspace 共同发起，旨在推动云计算服务在全球的发展，为私有云和公有云提供可扩展的弹性服务.OpenStack 覆盖了云计算基础设施中的网络、虚拟化、操作系统、服务器等各个方面，目前已成为市场占有率最高的云计算解决方案.

开源组织管理的大量开源代码已广泛应用于日常使用的软件中，支撑了网络和信息系统的正常运行.信息系统中主流的操作系统、数据库、应用软件等产品均不同程度地嵌入了开源代码.通过对相应软件产品的安装包进行反编译及二进制代码检测，往往可以发现软件代码中的开源成分.我们通过对某款应用范围较广的办公软件进行二进制代码检测，溯源分析后发现其开源代码比例在 22%以上，在开源代码库中匹配到了 Zlib，TinyXPath，cctz，libytnef，pugixml 等 29 个开源组件，这些开源组件绝大部分出自美国的开源项目，涉及 GPL，Apache License，BSD 等开源许可证，相关代码在 GitHub，SourceForge 等代码托管平台上进行维护.

2 开源软件供应链的特点

2.1 开源代码管理具有开放性

目前，开源软件项目主要有 2 种管理模式：一种为基金会主导模式，如 Apache 软件基金会 Hadoop 项目、Linux 基金会的 Linux 项目等；另外一种为企业主导模式，如谷歌的 Android 项目、微软的 Visual Studio Code 项目等.基金会或企业

通过将软件源代码在相应社区及代码托管平台公开，供用户使用、修改和交流，以社会化协作的方式提高软件生产效率，开发者只要遵循社区的规则都可以对代码进行访问和修改.开放性促进了开源的快速发展，但也带来了代码管理的一些问题，如代码维护管理依赖开源社区、代码安全性缺乏审核、很少有特定的人员专门负责修补安全漏洞等.

2.2 开源许可证体系混乱

值得注意的是，“开源”并不代表“免费”，更不是“随便用”.开源项目在应用过程中通常需要绑定相关的许可证，开源许可证规定了开源代码的知识产权所有人对于代码使用者的限制条件，这些条件包括是否允许用于商业用途、是否允许用于某些特定领域、是否允许专利授权等，用户选择使用其开源代码相当于默认接受相关的限制条件.目前，国际上并未形成统一的开源许可证体系，已知存在的许可证就包括 Apache License，GPL，MIT，BSD 等几十种，其规定的限制条件各不相同.在企业软件开发过程中，使用多个绑定不同许可证的开源组件，会导致许可证规则冲突，面临法律风险[3].如中国某公司曾因未公开 Android 系统相关代码而被开源社区认定违反其许可证规则，原因是 Android 系统绑定了 Apache2.0 许可证，该许可证不要求公开源代码，但该公司在 Android 中加入了绑定 GPLv2 许可证的 Linux 内核代码，GPLv2 许可证则要求修改后的代码必须公开，而该公司并未公开.

2.3 大部分开源软件受美国法律管辖

20 世纪 90 年代开源概念在美国兴起，在其政策主导下产生了 Apache 基金会、Google 等开源组织和企业，以及 Hadoop，Android 等著名的开源项目.美国注册的开源组织在运营政策上基本都会遵守美国相关的法律法规.全球最大的开源基金会 Apache 软件基金会在其运营文件中就明确表示，其产品均是由在美国的服务器向外分发，须遵守美国《出口管制条例》(Export Administration Regulation，EAR).随着我国开源软件的快速发展，国内虽然产生了一批开源组织和自建的代码托管平台，但仍然难以撼动美国对开源软件的绝对主导地位，目前绝大部分开源代码事实上仍然被美国控制.

3 开源软件供应链的安全风险

网络产品供应链的主要风险除了产品自身的安全性外，还包括产品使用后带来的网络和信息系统被非法控制、遭受干扰和破坏、数据泄露的风险，以及产品供应渠道可靠性及是否可能因政治、外交、贸易等原因中断供应的风险[4].我们通过对某办公软件的开源成分进行分析，同时结合其开源代码安全、开源项目、托管平台、法律政策等相关数据的收集，初步判断开源软件在供应链安全方面存在 3 大风险.

3.1 开源软件漏洞难以管理，产品安全性面临风险

开源软件因其代码的公开性，在一定程度上降低了开发成本，提高了开发效率，但同时也带来了安全风险.开源软件的安全漏洞管理与其他商业软件具有较大区别.商业软件在发现漏洞后，通常会把修复补丁自动推送给用户，开源软件则是被动的“拉取模式”，相关补丁需要人工安装.若开发人员不对使用的开源代码定期检查，则相应的安全漏洞会一直存在.随着新代码的加入，漏洞在代码库中将越积越多，漏洞平均年龄逐渐增加，修复漏洞将变得耗时耗力.在此次办公软件的开源成分分析中，通过匹配开源代码漏洞库，发现了 libytnef 等开源组件的堆溢出漏洞[5]等 14 个中高危漏洞，攻击者可利用这些漏洞构建恶意文件，入侵并瘫痪网络系统.而开源代码的开放性特点，使得代码的漏洞人人可见，这当中肯定也包括网络攻击者.在一些基础开源代码应用范围十分广泛的情况下，开源的特点导致越来越多的开源代码库正在成为网络犯罪的目标，攻击者往往倾向于利用基础开源代码发动 1 次行动造成很多攻击，而不是去攻击每一个应用.开发者甚至可以故意创建恶意代码，让企业在不知情的情况下将恶意代码纳入其代码库中，形成隐藏的风险.一旦不法分子利用开源软件的漏洞对电信、能源、交通等行业的重要信息系统发动攻击，可能造成大范围的社会基础设施出现服务中断，大量的个人信息和重要数据面临泄露的风险.

3.2 开源软件知识产权面临法律风险

企业使用开源组件相当于默认接受开源许可证的限制条件，比如办公软件中使用的 libytnef，js

等开源组件使用了 GPLv2 许可证，该许可证限制了其产品应用于特定行业领域.如果不遵守许可证规则将引起知识产权等问题上的法律纠纷，增加软件遭禁用的风险，产品提供者将承担高昂的软件替代成本.而且，注册于美国的开源组织产生的法律纠纷受美国的司法管辖.如 js 开源项目所属的 Mozilla 基金会在服务协议[6]中明确其受美国加州法律管辖，相应的索赔和纠纷应在加州圣克拉拉县法院提起诉讼.美国的属地管辖不仅增加了相关法律诉讼的成本，也令使用这些开源代码的企业和运营者在知识产权问题上面临诸多不确定性，在可能涉及域外法律管辖时，相关的法律风险大大升高.

3.3 开源代码在美国出口管制下存在断供风险

开源代码托管平台 GitHub 在官方声明[7]中明确表示，相关产品遵守美国 EAR，包括禁止受制裁的国家和团体访问其服务，禁止其企业服务出售或出口至伊朗、朝鲜、叙利亚等受美国制裁的国家.此次分析的办公软件所使用的 libytnef，pugixml，cctz 等开源组件代码就托管于 GitHub.据公开报道，2019 年就曾发生伊朗和俄罗斯克里米亚地区的 GitHub 用户个人账户遭到封禁无法取回代码的事件，这表明 GitHub 已在美国出口管制要求下展开行动.

美国 EAR 将开源代码的出口划分为 2 类[8]：一类是“公开可获得”(publicly available)的不带加密功能的软件源代码，不受出口管制；另一类是公开可获得的带加密功能的软件源代码(出口控制等级编号 ECCN 为 5D002)，虽不会被限制出口，但需符合备案要求.目前，知名的 Tomcat，Hadoop 等开源项目都被划定为 ECCN 5D002，相当于备案后可不受管制.总体来讲，开源软件在正常情况下属于“公开可获得”的软件，即使开源组织在政策上声明遵从美国 EAR 要求，目前尚不会被限制出口.但如果美国调整 EAR 规则，将含有开源成分的重点软件加入到管制名单，或修改目前“备案后不受管制”的条款，大量核心的开源项目将面临出口管制的限制，我国软件开发者获取相关开源代码将非常困难，相关产品的软件供应链将面临极大的断供风险.2020 年 1 月 6 日，美国商务部就通过更新 EAR 将“用于自动分析地理空间图像的软件”(出口控制等级编号 ECCN 为 0Y521)列入管制范围，智能化传感器、无人机、卫星等目标识别软件都在限制范围之内，美国企业必须得到许可后才能出口这些软件到中国等目的地.在 2019 年美国政府将华为公司列入出口管制“实体清单”后，谷歌即宣布停止向华为提供基于 Android 系统的更新服务及应用.虽然谷歌对华为的“断供”并不涉及安卓开源项目 AOSP(Android Open Source Project)，但是美国相关开源组织和平台的“集体行动”，不得不让我们开始对开源软件供应链面临的断供风险予以重视.2020 年 3 月，国际开源芯片技术组织 RISC-V 基金会就宣布将总部从美国特拉华州迁往瑞士[9].其负责人表示，虽然目前基金会的全球合作尚未受到影响，但基于对美国贸易限制的担忧及成员可能面临的地缘政治破坏，仍然决定将基金会的注册地迁出美国.在当前中美贸易摩擦尚未结束、美对我相关企业的制裁并未解除的大背景下，美国对其出口管制规定的不断调整，将导致开源软件因政治、外交、贸易等因素供应中断的风险增大.

4 对策建议

随着开源软件的广泛应用，开源安全风险日益凸显.为有效控制网络安全风险，保障重要信息系统承载的业务安全：一是网络安全检测认证机构需加强开源软件安全评价技术及方法研究，利用软件代码分析等工具准确识别网络产品中的开源成分，分析开源代码安全性，为安全评估提供重要的手段支撑.二是企业应提高开源软件供应链安全意识，充分评估开源软件许可证冲突及软件供应中断的法律风险，加大自主创新投入[10]，提高代码自主水平，推动构建国产开源生态，完善安全、可靠、多源的软件供应链安全保障体系.

参 考 文 献

[1] 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

[2] Synopsys，Inc. Open source security and risk analysis [R]. San Francisco：Synopsys，2019

[3] 刘彬彬. 开源许可协议的法律问题研究[D]. 兰州：兰州大学，2020

[4] 马宁. 我国网络安全审查法律制度的演进[J]. 保密工作，2020 (8)：52-54

[5] 曾永瑞，李喆. Linux二进制漏洞利用——突破系统防御的关键技术[J]. 信息安全研究，2018，4(9)：806-818
[6] Mozilla. Websites & communications terms of use[EB/OL]. [2021-01-27]. https://www.mozilla.org/en-US/about/legal/terms/mozilla/
[7] GitHub. GitHub and trade controls [EB/OL]. [2021-01-27]. https://docs.github.com/en/github/site-policy/github-and-trade-controls
[8] US Department of Commerce. Export administration regulations [EB/OL]. [2021-01-30]. https://bis.doc.gov/index.php/regulations/export-administration-regulations-ear
[9] RISC-V. International reports another strong year of growth with new technical milestones, educational programs, RISC-V adoption and more [EB/OL]. [2020-12-30]. https://riscv.org/announcements/2020/12/risc-v-international-reports-another-strong-year-of-growth-with-new-technical-milestones-educational-programs-risc-v-adoption-and-more/
[10] 倪光南. 坚持信创科技自立自强，建设网络强国、数字中国[J]. 信息安全研究，2021，7(1)：2-3

齐 越
工程师.主要研究方向为信息通信、网络安全.
qiy@isccc.gov.cn

刘金芳
博士，助理研究员.主要研究方向为网络安全.
liujf@isccc.gov.cn

李 宁
主要研究方向为网络安全.
lin@isccc.gov.cn