供应链攻击：如何减少开源漏洞

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Supply Chain Attacks: How To Reduce Open-Source Vulnerabilities		
原文作者	珍妮弗·格雷戈里（Jennifer Gregory）	**原文发布日期**	2021 年 5 月 25 日
作者简介	珍妮弗·格雷戈里是一位专注网络安全领域的自由作家。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/articles/supply-chain-attacks-open-source-vulnerabilities/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
摘要	云很可能是未来软件的交付方式，因此在可预见的将来，供应链攻击将成为一个重大问题和挑战。企业和消费者每天都会无意间安装新的更新和应用程序。通过仔细评估用于交付软件产品的流程和工具，可以减少此类攻击的数量和影响。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

供应链攻击：如何减少开源漏洞

珍妮弗·格雷戈里

2021 年 5 月 25 日

当你读到“2021 年第一季度与 2020 年第四季度相比，软件供应链攻击增加了 42%”时，你可能会认为网络安全问题与传统供应链有关。在许多人看来，供应链就是指通过卡车和轮船运输产品。但是，软件公司早已不像几十年前那样运送其产品的 CD 了。现在，他们的供应链是互联网和云，他们通过互联网和云交付产品。如今，云就是为公司运送新应用程序和更新的“卡车”。

这意味着，攻击者可以搜寻这些系统和方法中的漏洞。通常，攻击是在管理员下载新应用或更新现有应用时开始的。届时，恶意软件会将自身嵌入到应用中。有时，员工甚至根本没有发现错误，或者发现时已经晚了。

几乎每个企业都使用多款应用来运行其业务。因此，软件供应链攻击有可能广泛传播并造成严重的破坏。接下来，我们将分析导致此类攻击增加的原因是什么，以及企业可以采取哪些措施来防御这些攻击。

开源问题和供应链网络安全

其中一个最大的问题是：许多企业依赖于开源供应链应用程序。在 2019 年至 2020 年之间，针对开源代码的攻击增加了 430%。并非所有这些攻击都与供应链有关。但是，软件公司用来交付产品的许多系统都是开源的。这意味着，与供应链相关的问题会不断增加。攻击者在攻击开源代码方面日益熟练。

要了解问题的严重性，我们可以参考《2021 年开源安全状况对比报告》。该报告指出，每个应用程序平均包含 118 个库，而只有 38%的库处于活动状态。攻击者可以将恶意软件或恶意代码插入不活动的库，而不会被检测到，这会带来严重的风险。库的平均使用期限为 2.5 年，因此应用程序的老旧库可能会存在问题，而且不会被注意到。该报告还指出，每个 Java 应用程序平均包含 50 个开源库漏洞。这意味着，每个库遭攻击的可能性为 16%。

通过红队测试抵御供应链攻击

实际经验是学习团队合作和实时使用控制措施的最佳方式。因此，越来越多的企业开始进行模拟攻击测试，以减少供应链攻击的影响。在这些测试中，“红队”使用与攻击者相同的战术、技术和程序。“蓝队”则对红队的攻击做出响应。通过对抗攻击者使用的工具，他们能够获得宝贵的经验。

这些测试的最大优势是，安全团队可以直接了解攻击，从而制定详细的流程，以最有效的方式做出响应。通过这些测试，蓝队可以减少平均检测时间和平均响应时间，减少开源代码漏洞导致的供应链破坏。在挑选进行攻击测试的合作伙伴时，应寻找可以提供团队绩效详细反馈的公司，这样，企业就可以根据这些反馈来更改其流程和工具。

减少依赖混淆问题

依赖混淆也与供应链攻击的增加有关。在应用程序中使用内部和第三方库的团队，面临因依赖混淆而遭受供应链攻击的风险——攻击者会在外部库中创建伪造的软件包。这个软件包与内部库中的软件包具有相同的名称，如果软件包管理器在内部库中找不到这一软件包，就会选择伪造的软件包。在以前的类似攻击中，攻击者依赖于开发人员拼写错误的软件包。但是，依赖混淆更加可靠，并且更具破坏性，在自动执行攻击时更是如此。

防止依赖混淆的最佳方法是提高库、软件包和依赖关系的可见性和安全性。如果安全团队对库和软件包的名称实施保护，攻击者就不太可能创建具有重复名称的假软件包了。通过使用支持命名空间模块的软件包管理器，可以减少依赖混淆攻击，因为具有相同名称的软件包不能在两个不同的地方使用。其他策略包括：仅使用信誉良好的开源库，要求开发人员在安装前验证软件包的来源等。

未来的工具

云很可能是未来软件的交付方式，因此在可预见的将来，供应链攻击将成为一个重大问题和挑战。企业和消费者每天都会无意间安装新的更新和应用程序。通过仔细评估用于交付软件产品的流程和工具，可以减少此类攻击的数量和影响。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com