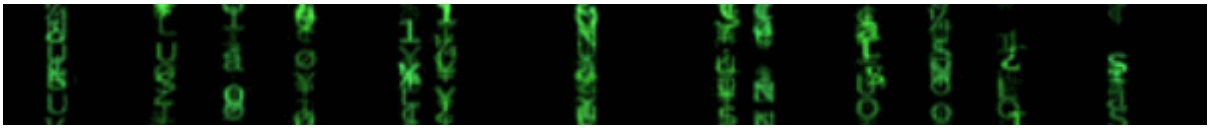
开源安全的利器：八个顶级SBOM工具

黑白之道 2022-08-01 10:45 发表于山东



到2025年，60%的开发或采购关键基础设施软件的组织将强制执行和标准化SBOM。今天，SBOM普及率不到20%。

软件安全（尤其是开源软件安全）的基本前提是你需要知道软件中都有哪些代码组件，或者说代码的可见性。这也是软件物料清单（SBOM）越来越受到业界重视的原因。从某种意义上来说，SBOM相当于食品安全领域的“添加剂成分表”。

软件行业，甚至毫不夸张地说，整个数字经济的基础设施，都正在被（开源）软件的“安全债”问题反噬。近年来，一个接一个的安全耳光接踵而至：SolarWinds软件供应链攻击，旷日持久不见天日的Log4j漏洞，以及开源工具npm维护者的“投毒”事件，都清楚地表明全球的软件供应链安全问题已经到了必须悬崖勒马的危险地步。

2022年4月Synopsis的的一项行业研究发现，97%的软件包含开源代码，其中计算机硬件和半导体、网络安全、能源和清洁技术、“物联网”设备以及互联网和移动应用软件相关系统中，100%都发现了开源代码。而且开源代码的数量也不容忽视——受调查的代码中有78%都是开源的。最令人担忧的是，包含开源代码的代码库中有81%至少存在一个漏洞，每个应用程序平均有五个高风险或严重漏洞仍未修补。

如今，开源软件已经是无处不在的“软件添加剂”，但用户却没有“成分表”可用，其危险性不言而喻。

源于制造业的物料清单这个概念对于闭源的专有软件是无效的，但是对于开源程序，SBOM不仅是有用的，而且是必须的。因为即使是实力最雄厚的科技巨头也需要花费数周时间才能找到软件漏洞，修补时间往往更长。SBOM则能帮助企业快速锁定漏洞在软件中的位置，因而大大提高软件漏洞的修复和缓解速度。

根据Linux基金会、开源安全基金会(OpenSSF)和OpenChain的说法，提高（开源）软件安全性的答案是SBOM。Linux基金会研究副总裁Stephen Hendrick将SBOM定义为“唯一标识软件包及其内容的正式且机器可读的元数据，它可能包括有关其内容的信息，包括版权和许可数据。SBOM旨在跨组织共享，特别有助于提高软件供应链参与者交付的组件的透明度。”

最佳SBOM实践

SBOM应包括：

- 应用程序的开源库
- 程序的插件、扩展和其他附加组件
- 开发人员内部编写的自定义源代码
- 有关这些组件的版本、许可状态和补丁状态的信息
- 自动组件加密签名和验证
- 自动扫描以生成SBOM，作为持续集成/持续部署(CI/CD)管道的一部分

SBOM应该使用一致的格式。流行的SBOM格式包括软件包数据交换(SPDX)、软件标识(SWID)标记和OWASP CycloneDX。虽然这些都是标准，但2021年的白宫行政命令并未强制规定特定的SBOM格式。到目前为止，这三者都没有成为事实上的行业标准。

为了使SBOM发挥效力，不仅要自动创建SBOM，还要使其成为CI/CD管道的一部分。正如美国国家电信和信息管理局(NTIA)所说，最终目标是以“机器速度”生成SBOM。

SBOM三大用例

SBOM有三种不同的用例：

- 软件生产商使用SBOM来协助构建和维护他们提供的软件。
- 软件采购商使用SBOM通知预购保证、协商折扣和计划实施策略。

- 软件运营商使用SBOM为漏洞管理和资产管理提供信息，管理许可和合规性，并快速识别软件和组件依赖关系以及供应链风险。

上述用例对SBOM的需求是完全不同的。开发人员需要能够在CircleCI、Jenkins或Travis CI等CI/CD管道上运行的工具。而运营商或客户可能甚至不知道CI/CD管道是什么，但可能非常关心资产管理和安全补丁更新。

Gartner估计，到2025年，60%的开发或采购关键基础设施软件的组织将强制执行和标准化SBOM。今天，SBOM普及率不到20%。

如何选择SBOM工具

市场上许多SBOM工具、捆绑代码安全扫描程序和其他类似程序，用户选择起来比较困难，Gartner建议使用提供以下功能的工具：

- 在构建过程中创建SBOM。
- 分析源代码和二进制文件（如容器图像）。
- 为这些工件生成SBOM。
- 编辑SBOM。
- 以人类可读的格式查看、比较、导入和验证SBOM。
- 将SBOM内容从一种格式或文件类型合并和翻译成另一种格式或文件类型。
- 支持通过API和库在其他工具中使用SBOM操作。

值得注意的是，即便是当今最好的一些SBOM工具，也未能覆盖Gartner的建议功能清单，因此我们建议用户多尝试一些工具，来寻找最适合自己的，或者向供应商和开发人员提供反馈。对于很多企业来说，能够在2025年之前完成这项任务并制订出最佳实践计划就很不错。

八个值得关注的SBOM工具

Anchore

Anchore从事SBOM业务已有六年，主要基于两个开源项目。一个是Syft，一个用于从容器映像和文件系统生成SBOM的命令行界面(CLI)工具和库。另一个是Grype，一个用于容器映像和文件系统的易于集成的漏洞扫描工具。

上述两个工具可以一起使用，在开发流程的每个阶段生成SBOM（从源代码存储库和CI/CD管道到容器注册表和运行时）。这些SBOM保存在一个集中的存储库中，以实现完

整的可见性和持续监控，甚至覆盖部署后。它支持CycloneDX、SPDX和Syft自己的SBOM格式。

Anchore将其SBOM功能捆绑到Anchore Enterprise 4.0软件SCM（供应链管理）平台中。Anchore的目标是成为一体化软件供应链和SBOM安全公司。

FOSSA

FOSSA的旗舰程序是开源许可证合规管理器和开源漏洞扫描程序。

在FOSSA的方法中，用户可以将其SBOM工具与版本控制系统（例如GitHub、BitBucket或GitLab）集成。或者，用户也可以使用它的CLI并在本地运行它，或者将其集成为CI/CD管道的一部分。

无论哪种方式，当扫描项目时，FOSSA都会自动识别目标代码库的直接依赖关系和深度依赖关系。一些深度嵌入的代码问题，例如调用Log4j的间接依赖关系，会隐藏在程序中，仍然可被黑客利用来造成严重破坏。

Mend

Mend曾经的名字是WhiteSource，提供了多种软件组合分析(SCA)工具。SBOM包含在其Mend SCA工具中。因此，Mend与其说是开发者程序或CI/CD工具，不如说是程序员的开源许可和安全机制。

因此，Mend可用于跟踪每个组件，包括直接和传递依赖关系、识别漏洞、提供修复路径以及在组件更改时自动更新SBOM记录。该公司声称其获得专利的可达性路径分析可向用户展示哪些漏洞可以安全地忽略。

Rezilion

DevSecOps公司Rezilion使用SBOM作为其整体软件安全和漏洞系统的一部分。它的动态SBOM使用动态运行时分析来跟踪代码更改时的软件攻击面。因此，它会不断查找代码组件的已知弱点。

除了提供CI/CD、导入和生产环境中所有软件组件的实时清单之外，它还会不断更新SBOM。用户可以将SBOM导出为CycloneDX和Excel电子表格。

SPDX SBOM Generator

作为一个独立的开源工具，SPDX SBOM Generator可在用户当前的包管理器或开发系统中创建SPDX SBOM。用户可以使用它的CLI从代码中生成SBOM数据。它报告代码的组件、许可证、版权和安全参考。此数据以SPDX v2.2规范导出。如果你只需要基础的SBOM功能，那么SPDX SBOM Generator是个不错的选择。

Tern

Tern也是一个开源SBOM项目，可与SPDX SBOM Generator很好地匹配使用。这个SCA工具和Python库不使用包管理器或构建系统，而是为容器映像和Dockerfile生成一个SBOM。它还能在SPDX中生成SBOM。

TauruSeer

该SBOM工具以软件即服务(SaaS)的方式提供。TauruSeer依靠获得专利的以应用程序为中心的集成方法，将其Cognition Engine安全扫描与其SBOM相结合。该软件包能保护和跟踪您的开发人员和客户的代码。

Vigilant Ops

Vigilant Ops是一家医疗设备网络安全公司，凭借其InSight平台，已将注意力转向SBOM。其SaaS平台生成、维护和经过认证的SBOM共享。它使用持续的漏洞监控和警报来整合安全性。其SBOM认证使用专利算法来确保所有组件都经过验证，并与漏洞相关联。

Vigilant Ops的安全功能也可以与其他程序生成的SBOM一起使用。相关数据在静态和传输中都是加密的。

> **文章来源：GoUpSec**

END

多一个点在看　　多一条小鱼干

喜欢此内容的人还喜欢

3 个令人惊艳的 ChatGPT 项目，开源了！

GitHubDaily

时隔 2 年更新！Motrix - 清爽开源免费的全能下载加速工具

异次元软件世界

一个非常牛逼的开源中后台模版项目

Java知音