SBOM(SOFTWARE BILL OF MATERIALS) 이란 무엇인가

개요

작년 미국의 국가 사이버 보안 강화 지침(2021년 5월)이 배포된 이후, 소프트웨어 산업의 다양한 채널에서 SBOM과 관련한 자문이나 회의가 생기고 있는 상황입니다.

최근의 보안 위협은 공급망, 구축도구, 구축환경, 레파지토리등을 공격하는 추세가 많아지고 있는데 이 지침에서는 미국 연방정부가 사용하는 소프트웨어 공급망의 보안과 무결성을 개선하기 위한 조치를 지시하고 있습니다.

지침이 배포된 이후 미국 정부의 요청으로 미국의 90여개 소프트웨어 기업, 오픈소스 커뮤니티가 자문에 참여하여 의견을 제시하고, CISA, NTIA 에서는 이를 정리하여 SBOM 과 관련한 가이드라인 및 FAQ를 공개하였습니다.

- https://www.ntia.gov/SBOM

SOFTWARE BILL OF MATERIALS | National Telecommunications and Information Administration

A “Software Bill of Materials” (SBOM) is a nested inventory for software, a list of ingredients that make up software components. The following documents were drafted by stakeholders in an open and transparent process to address transparency around sof

www.ntia.gov

SBOM 이란?

SBOM 은 SOFTWARE BILL OF MATERIALS 의 약자로 소프트웨어의 구성 요소를 나타내는 메타데이터를 의미하는데 이를 보다 쉽게 설명하자면 우리가 흔히 볼 수 있는 다음과 같은 제품의 성분표기를 떠올리면 됩니다.

blocked URL

성분표기를 통해서 알러지가 있는 사람은 해당 식품을 피하기도 하고, 공급자는 제품의 우수성을 홍보하기도 하고, 크게 성분에 신경쓰지 않고 그냥 사용하는 사용자도 있을 수 있죠.

이와 유사하게, SBOM은 공급되는 소프트웨어의 구성 목록을 잘 표시해서 공급자와 사용자가 이를 기반으로 의사결정에 활용할 수 있는 환경을 조성하는 것을 목표로 하고 있습니다.

NTIA 에서 발표한 SBOM의 필수 구성요소는 다음과 같이 구성되어 있습니다.

- Supplier name
- Component name
- Version of the component
- Cryptograph hash of the component
- Any other unique identifier
- Dependency relationship
- Author of the SBOM data

이를 기반으로 작성한다면 다음과 같은 개념도로 표시할 수 있습니다.

blocked URL

National Telecommunications and Information Administration (NTIA) 에서는 오픈소스 소프트웨어나 상용 소프트웨어로 구분하지 않고 모든 공급되는 소프트웨어를 대상으로 광범위하게 적용할 수 있는 SBOM 적용을 위해 산업계의 여러 기업과 커뮤니티에 의견을 청취하고 이를 토대로 SBOM의 이해를 돕는 자료와 적용방법에 대하여 다양한 문서를 배포하고 있으니 아래 문서들을 참고하시기 바랍니다.

- SBOM at a Glance (2021)
- SBOM FAQ (2021)
- Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM) – (2021)
- SBOM Options and Decision Points (2021)
- Use Cases: Roles and Benefits for SBOM Across the Supply Chain (2019)

SPDX, OpenChain

이러한 소프트웨어 구성 목록을 기반으로 공급망의 투명성을 확보해야 한다는 필요성은 오픈소스 커뮤니티에서 10여년 전부터 논의되어 왔으며, 이를 해결하기 위해 실제 산업에서 SPDX와 OpenChain 이 많이 사용되고 있습니다.

- SPDX는 라이선스 컴플라이언스, 보안 등과 같은 문제를 다루면서 진화해서 현재는 시장에서 가장 성숙한 SBOM으로 자리잡고 있습니다. (https://www.linuxfoundation.org/blog/what-is-an-sbom/)
- 또한 오픈소스 라이선스 준수를 위한 ISO 국제표준(https://www.iso.org/standard/81039.html) 으로 오픈체인이 있으며, 이는 소프트웨어 공급망의 투명성을 강화하기 위하여 오픈소스 커뮤니티에서 고민하던 결과물입니다.

SBOM이 소프트웨어 보안의 모든 문제를 해결할 수는 없지만 보다 안전한 소프트웨어 사용에 필요한 기본을 제공하는 것은 분명히 필요한 일이며, 다양한 산업계의 의견을 토대로 만들어진 SBOM을 기반으로 소프트웨어 공급망의 투명성을 강화할 수 있는 미국의 이번 정책은 향후 IT 산업과 디지털 인프라의 소프트웨어 관리에 있어서 매우 중요하다고 생각됩니다.