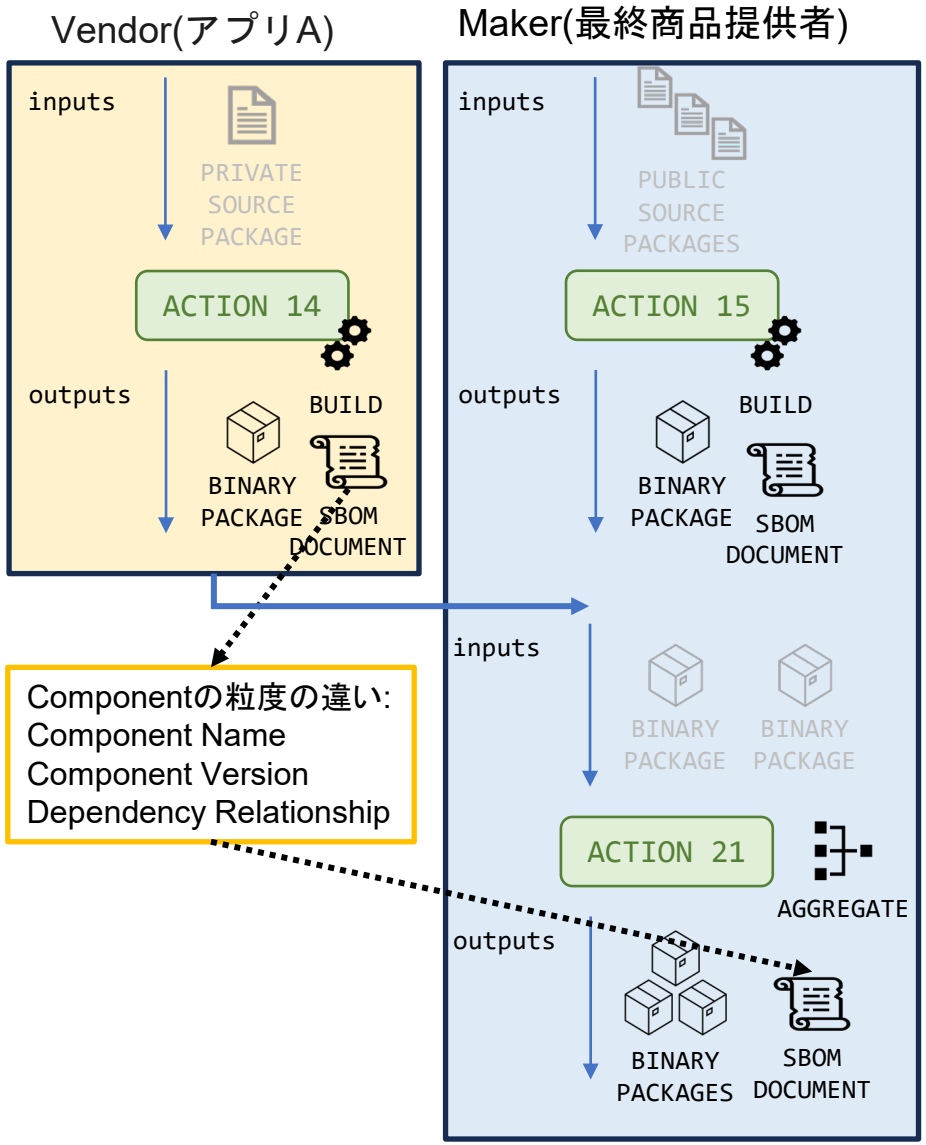
OpenChain JWG Automation and SBOM SG Security Discussion 宿題3

2025/02/03

Sony Group Corporation Nobuyuki Tanaka

課題A



①サプライチェーン上、SBOM受け渡しの課題になりそうなものを書いてください。

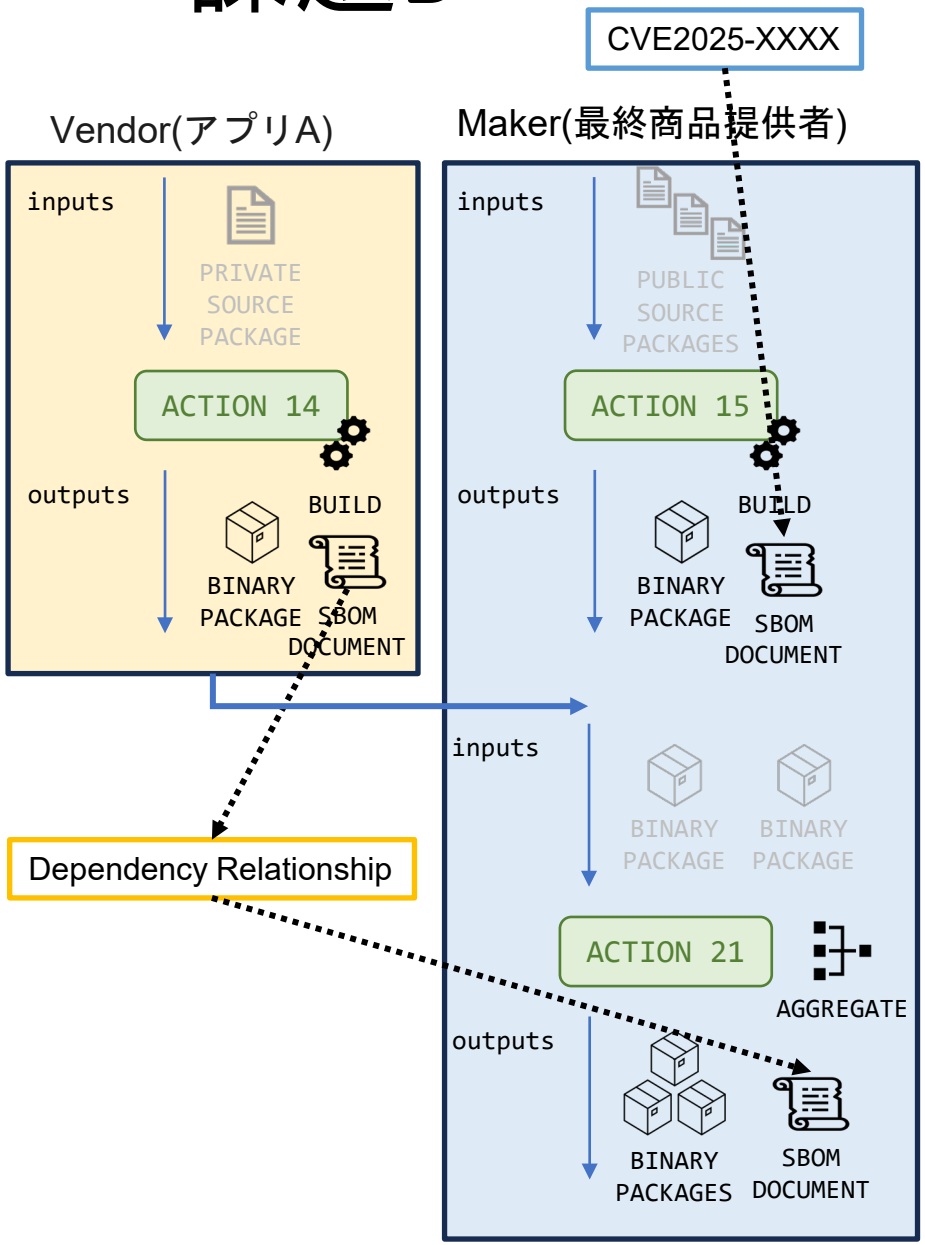
課題A:
コンポーネントの粒度が異なるSBOMをマージする(ファイルとして一つにしなくてもお互いにRelationshipをつけて矛盾なく構成する)ことはできるのか(例えば、パッケージ単位のSBOMとファイル単位のSBOM)

- コンポーネントの粒度がサプライチェーンで一貫している必要があるか
- コンポーネントの粒度を表すプロパティは必要なのか

課題Aの検証:
前提条件: VendorからアプリAがバイナリ+SBOMで提供され、アプリAがOSSに依存している前提
結論: 以下の表のとおり、どのケースでも対応できないことはない

Vendor(アプリA)のSBOMのComponentの単位	Maker(最終商品提供者)のSBOMのComponentの単位	
	バイナリファイル	バイナリパッケージ
バイナリファイル	ファイル単位で提供	アプリAが依存するOSSのファイル情報をパッケージ情報に変換してアプリAのみファイル単位、その他はパッケージ単位で提供
バイナリパッケージ	アプリAパッケージからファイルを分解してファイル単位で提供	パッケージ単位で提供

課題B



①サプライチェーン上、SBOM受け渡しの課題になりそうなものを書いてください。

課題B:
バイナリ(パッケージでもファイルでも)提供されたアプリAは、MakerのOSS Bに依存している。
OSS BにCVE2025-XXXXがあることが分かったとしても、このCVEがアプリAに影響があるかどうかはSBOMの依存関係の粒度 (パッケージでもファイルでも)ではMakerは判断できない。
アプリAがOSS Bのどの機能をどう利用しているかが分からないため。

アプリAが依存するOSSに脆弱性が見つかった場合、VendorとMaker間の契約で情報提供を求める必要があるのではないか。