OpenChain JWG Automation and SBOM SG Security Discussion 宿題3

2025/02/03 Sony Group Corporation Nobuyuki Tanaka LICENSE: CC0

課題A

Maker(最終商品提供者) Vendor(アプリA) inputs inputs ACTION 14 ACTION 15 outputs outputs BUILD BUILD BINARY **BINARY** PACKAGE SBOM PACKAGE SBOM DOCUMENT DOCUMENT inputs Componentの粒度の違い: **Component Name** Component Version Dependency Relationship **-**ACTION 21 **AGGREGATE** SBOM PACKAGES DOCUMENT

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。

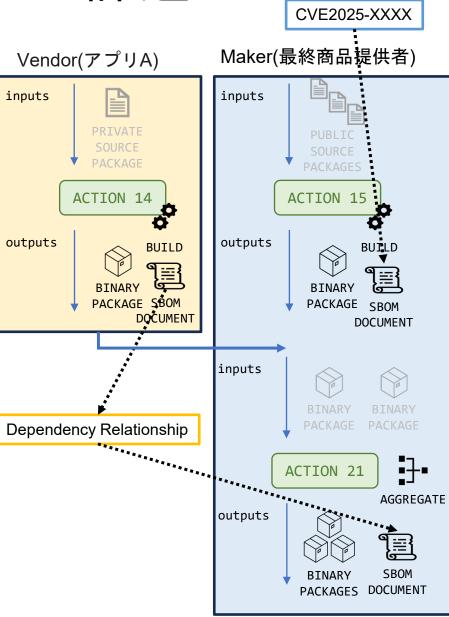
課題Aの検証:

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

	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		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
7117777170	アプリAパッケージからファイル	「ルキロ、この他はバン)」ノキロで促択
バイナリパッケージ	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。