E33

セキュリティ工数を削減して初動対応を1時間以内にします
―「1-10-60ルール」を達成する脆弱性管理

文脈SBOMを利用した効率的な脆弱性管理技術

IOWN Evolution 持続可能なビジネスのためのデータ管理技術

背景

2020年にSolarWindsを狙ったサイバー攻撃が発生し、サプライチェーンセキュリティの重要性が再認識されました。プロダクトが安全に構築されたことの証明は社会的な要求になっており、それを実現する方法としてSBOM（ソフトウェア部品表）が利用されています。

成果の概要

SBOMは食品の成分表示のように「製品の安全」を見える化しますが、問題箇所を特定して直すには成分の情報だけでは足りません。NTTコミュニケーションズは、通常のSBOM分析で取り除かれてしまう利用状況（文脈情報）に着目し、脆弱性対応プロセスの削減に成功しました。

SBOMを利用したプロダクトの脆弱性対応

従来のSBOMによる脆弱性管理手法 - 5ステップ
デプロイ / SBOM分析 /コンテキストの手動収集 /コンテキストに基づく意思決定 /アクションの実行

提案手法 - 3ステップ（特許出願）

脆弱性対応の時間を短縮

SBOM分析
＋コンテキスト管理

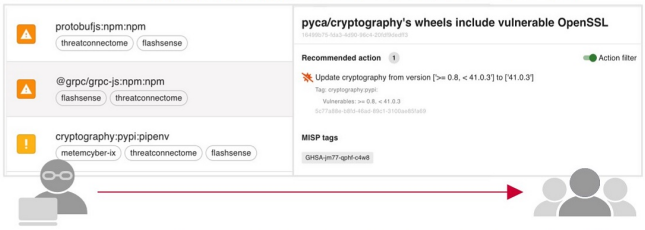
脅威発見と対策立案プロセスの高速化

最適なアクションによる
迅速なセキュリティ対応

文脈SBOMを利用したセキュリティ情報の柔軟な配布

パッケージマネージャ情報に着目してSBOMを効果的に利用

プロダクト開発者目線でのセキュリティ通知



ソフトウェア部品と利用状況（コンテキスト）が共有されるため、文脈SBOMは認識のずれを小さくできる

技術のポイント

- 文脈SBOMを利用した脅威発見とセキュリティ対策立案プロセスの高速化（特許出願中）
- 文脈SBOMを利用したセキュリティ情報の柔軟な配布（特許出願中）
- 初動対応が完了するまでの時間を大幅に削減（開発現場でSOC水準の「1-10-60ルール」を達成）

この研究がもたらす未来

既存のSBOMサービスは開発者にとって使いづらいものでした。本技術は文脈SBOMを利用して開発者が必要な情報を提供し、迅速なセキュリティ対応を実現します。

出展企業

エヌ・ティ・ティ・コミュニケーションズ株式会社

問い合わせ先

metemcyber@ntt.com