オムロンの SBOM への取り組み

-ソフトウェアサプライチェーンの透明性向上と継続的な製品セキュリティ管理の実現に向けて

オムロン株式会社　インダストリアルオートメーションビジネスカンパニー

システム事業本部 コントローラ事業部

オムロンは、製品に含まれるソフトウェアの透明性向上とサプライチェーンセキュリティ強化のため、SBOM（Software Bill of Materials）の整備および運用を進めています。

一方で、SBOM は製品に含まれるソフトウェア構成を可視化するための基盤情報であり、それ単独では製品への実際の影響や対策優先度を判断することはできません。

オムロンは、SBOM の整備に加え、PSIRT 活動による継続的な脆弱性監視、製品固有の影響評価、対策実施およびセキュリティアドバイザリ公開を一体的に推進し、製品ライフサイクル全体を通じた継続的な製品セキュリティ管理の実現に取り組んでいます。

1．まえがき

産業用オートメーションシステムにおいて、ソフトウェアは製品価値を支える重要な構成要素となっています。一方で、OSS（Open Source Software）やサードパーティ製ソフトウェアの活用拡大に伴い、ソフトウェアサプライチェーンに起因するセキュリティリスクへの対応が求められています。

近年では、EU CRA（Cyber Resilience Act）をはじめとする法規制や標準において、製品に含まれるソフトウェア構成の可視化と管理が求められており、その手段として SBOM（Software Bill of Materials）が注目されています。オムロンはこうした動向を踏まえ、安全・安心な製品の提供と継続的な製品セキュリティ管理の実現に向けて、SBOM の整備と活用を進めています。

2．SBOM とは

SBOM は製品に含まれるソフトウェアコンポーネントが階層化されたリストです。

近年の産業用機器では、多数の OSS やサードパーティ製ソフトウェアが利用されており、どのコンポーネントが製品に含まれているかを把握することは製品セキュリティ管理において重要となっています。

SBOM により、

- 構成管理
- 脆弱性影響調査
- インシデント対応
- 規制対応

を効率的に実施できます。

なお、SBOM はソフトウェアの構成情報を示すものであり、脆弱性の有無や製品への影響を示すものではありません。製品のリスクを適切に評価するためには、SBOM に加えて脆弱性情報や製品固有の影響評価を組み合わせて活用することが重要です。

3．装置メーカーの立場から見た SBOM の課題

SBOM は、ソフトウェアサプライチェーンの透明性向上や脆弱性管理を支える重要な基盤情報です。一方で、産業用オートメーション機器のような長期運用製品においては、SBOM を整備するだけでは十分な製品セキュリティ管理を実現できない場合があります。

3.1 SBOM を有効に活用するためには製品構成管理が不可欠

産業用機器では、同一製品であっても製造時期やロットによって搭載されるファームウェアバージョンが異なる場合があります。

例えば PLC では、製造ロットによって搭載されるファームウェアバージョンが異なり、それに伴って製品に含まれるソフトウェアコンポーネントの構成も変化することがあります。

このため、装置 1 台ごとに搭載されている

- PLC の型式
- ファームウェアバージョン
- 適用されたソフトウェア更新

を適切に管理していなければ、SBOM を保有していても実際にどの SBOM が対象となるのか特定できません。

つまり、SBOM は単独で存在しても十分な価値を発揮するものではなく、構成管理情報と組み合わせて運用されて初めて製品セキュリティ管理に活用することができます。

3.2 SBOM だけでは実際のリスクは判断できない

SBOM からは、製品にどのようなソフトウェアコンポーネントが含まれているかを把握できます。しかし、ソフトウェアコンポーネントに脆弱性が存在することと、その脆弱性が実際に製品で悪用可能であることは必ずしも同じではありません。例えば、

- 当該機能が製品内で使用されていない
- 攻撃対象となるインタフェースが無効化されている
- 対象機能へ到達できる経路が存在しない
- 製品のセキュリティ機能により悪用が防止されている

場合には、コンポーネントに脆弱性が存在していても実際の製品リスクは限定的となることがあります。

PLC を例にすると、ある OSS ライブラリに脆弱性があることが公表され、そのライブラリが PLC の SBOM 上に存在していたとしても、その脆弱な機能をその PLC が利用していなければ、実際には攻撃が成立しない可能性があります。そのため、装置メーカーには PLC の SBOM との照合だけでなく、

- 製品での利用状況
- 攻撃経路の有無
- 製品固有の影響評価
- 対策要否の判定

等の確認及び対応が求められます。

3.3 SBOM だけでは実際の運用負荷が増加する可能性もある

前述のとおり、お客様がサプライヤーから提供された SBOM を脆弱性情報管理ツールへ取り込んだ場合、多数の脆弱性候補が検出されることがあります。

しかし、その結果だけでは、

- 実際に製品へ影響するのか
- 対策が必要なのか
- どの脆弱性を優先的に対応すべきか

等を判断することは困難です。

例えば、その SBOM から 100 件の脆弱性候補が検出された場合でも、それらすべてが実際に対象製品へ影響するとは限りません。

実際には、製品で利用していない機能に関する脆弱性や、製品構成上攻撃が成立しない脆弱性が含まれる場合があります。

このため、検出された脆弱性候補について個別の影響評価を実施しなければならなくなり、結果として、お客様自身が膨大な脆弱性情報を調査・評価する必要が生じ、運用負荷が大きくなる可能性があります。

このように、SBOM は製品セキュリティ管理における重要な基盤情報ですが、SBOM 単体で製品リスクを評価することはできません。

そのためオムロンは、SBOM の整備だけでなく、

- 構成管理
- 脆弱性監視
- 製品固有の影響評価
- 対策実施
- セキュリティアドバイザリ公開

を組み合わせた継続的な製品セキュリティ管理を推進しています。

オムロンが提供する価値

SBOM ＋ 製品セキュリティ管理プロセス

▼

「製品に影響があるかどうか」整理された情報の提供

4．オムロンの製品セキュリティ管理プロセス

オムロンは、SBOM の整備を入口として、継続的な製品セキュリティ管理を実施しています。公開された脆弱性情報や研究者から報告された情報について、PSIRT が継続的に監視を行っています。

新たな脆弱性が製品に関連する可能性がある場合は、

- SBOM との照合
- 製品への影響有無評価
- 攻撃可能性評価
- 対策要否判定

を実施します。さらに必要に応じて、

- ソフトウェアアップデートの提供
- 回避策提供
- アドバイザリ発行

を行います。

このプロセスにより、オムロンは製品ライフサイクル全体にわたる継続的な製品セキュリティ管理を実現しています。

5．お客様のセキュリティ運用負荷を低減するために

製品セキュリティ管理では、脆弱性の存在を把握するだけでなく、その脆弱性が実際に製品に影響するかどうかを評価することが重要です。

サプライヤーが提供する SBOM を脆弱性情報管理ツールへ取り込んだ場合、多数の脆弱性候補が検出されることがあります。

しかし、その結果だけでは、

- 製品への影響有無
- 攻撃成立可能性
- 緩和策の有無
- 修正の必要性

を判断することはできません。

結果として、お客様自身が個々の脆弱性の評価や調査を実施する必要があり、大きな運用負荷が発生する可能性があります。

オムロンは、製品開発段階において脆弱性の低減に取り組むとともに、上市後も PSIRT による継続的な脆弱性監視および影響評価を実施しています。製品への影響があると判断された脆弱性については、セキュリティアドバイザリを通じて必要な情報を提供しています。これにより、大量の脆弱性候補を個別に評価する負荷を軽減し、より効率的なセキュリティ運用の実現に寄与します。

お客様にとって重要なのは、脆弱性一覧を受け取ることではなく、自社システムへ影響する脆弱性を把握し、優先順位をつけて対応できることです。

オムロンは、SBOM の作成・維持だけでなく、製品固有の影響評価結果および対策情報を提供することにより、お客様が限られたリソースの中で効率的にリスク管理を実施できるよう支援しています。

6．お客様への SBOM 提供について

SBOM は製品セキュリティ管理に有効な情報ですが、SBOM 単独では製品への実際の影響や対策優先度を判断できない場合があります。

そのため、オムロンは SBOM の提供可否だけではなく、お客様が必要なセキュリティ判断を適切に行える情報を提供できるかという観点も重視しています。

SBOM からはオムロンが実施した製品固有の脆弱性評価やトリアージの結果を読み取ることができません。このため、SBOM を適切な目的と管理環境のもとで活用いただけるよう、提供に先立ってヒアリングをさせて頂いております。

オムロンは、SBOM を単独で提供することよりも、お客様が製品リスクを正しく理解し適切な対策判断を行えることを重視しています。そのため、お客様の利用目的に応じて、SBOM に加え、関連するセキュリティ情報や影響評価結果を含めた適切な情報提供を実施しています。

7．むすび

デジタル化が進展する中で、ソフトウェアサプライチェーンの透明性と継続的な製品セキュリティ管理は、これまで以上に重要なテーマとなっています。

SBOM は、その実現を支える重要な基盤情報であり、製品に含まれるソフトウェアコンポーネントを把握し、脆弱性への迅速な対応やライフサイクル全体にわたるセキュリティ管理を可能にします。オムロンは、製品セキュリティ活動の一環として SBOM の作成・維持を推進しています。

一方で、SBOM は製品の構成情報を示すものであり、製品固有のリスク評価結果や対策要否を示すものではありません。お客様が安全かつ効率的に製品を運用するためには、ソフトウェア構成情報だけでなく、その構成が製品に与える影響や必要な対策まで含めた情報が重要であるとオムロンは考えています。

そのためオムロンは、

- SBOM の整備・維持
- 継続的な脆弱性監視
- PSIRT による影響評価
- セキュリティアドバイザリの公開
- 製品ライフサイクル全体を通じたセキュリティ管理

を一体的に推進しています。

オムロンが目指しているのは、SBOM を作成することそのものではありません。SBOM を活用した継続的な製品セキュリティ管理を通じて、お客様の安全・安心なシステム運用を支援することです。

透明性と実効性の両立を図りながら、お客様、パートナー企業、サプライヤーとともに、より安全で信頼できる産業オートメーション環境の実現に取り組んでいきます。

8．リンク

製品セキュリティへの取り組み | オムロン制御機器
https://www.fa.omron.co.jp/product/security/