OMRON's Approach to SBOMs:

Enhancing Software Supply Chain Transparency Through Continuous Product Security Management

Controller Div., Systems Business Div. HQ, Industrial Automation Company, OMRON Corporation

Software transparency has become an essential element of modern product security. As industrial automation products increasingly rely on open-source and third-party software, organizations increasingly require greater visibility into the software components that comprise their systems.

To address this need, OMRON develops and maintains Software Bills of Materials (SBOMs) as part of its product security program. SBOMs provide valuable visibility into software composition and support effective vulnerability management throughout the product lifecycle.

At the same time, effective product security management requires more than software inventory information alone. Understanding the potential impact of vulnerabilities, assessing exploitability in real-world environments, and providing timely mitigation guidance are equally important.

For this reason, OMRON combines SBOM management with continuous vulnerability monitoring, product-specific impact assessments, security advisory disclosures, and lifecycle-oriented security practices. These integrated activities help customers maintain secure, reliable, and resilient industrial automation systems.

1. Introduction

Software plays a critical role in today's industrial automation systems, delivering functionality, performance, and flexibility across a wide range of applications.

As the adoption of open-source software (OSS) and third-party software continues to grow, software supply chain security has become an increasingly important consideration for both product manufacturers and system operators.

Industry regulations, customer expectations, and evolving security standards are driving organizations to enhance transparency into software composition. In this context, the Software Bill of Materials (SBOM) has emerged as an important tool for understanding software dependencies and supporting security-related decision-making.

Recognizing these industry trends, OMRON continues to strengthen its product security program by incorporating SBOM management as part of a broader approach to continuous product security management.

2. Understanding SBOMs

A Software Bill of Materials (SBOM) is a structured inventory of software components contained within a product.

Industrial automation products frequently incorporate software developed by multiple organizations, including open-source and commercial software suppliers. Maintaining visibility into these components supports effective software lifecycle management, vulnerability management, and broader security activities.

SBOMs help organizations:

- Improve configuration management
- Accelerate vulnerability impact analysis
- Support incident response activities
- Address regulatory and compliance requirements

By providing transparency into software composition, SBOMs enable organizations to better understand the software assets that support their operations.

However, software composition information represents only one aspect of product security. Product risk assessments also require an understanding of vulnerability characteristics, product architecture, deployment environments, and security controls.

3. Maximizing the Value of SBOMs

SBOMs provide important software transparency benefits. To realize their full value, however, they should be considered within the broader context of product security management.

3.1 Configuration Management Matters

Industrial automation products often remain in service for many years. During their lifecycle, software and firmware versions may change due to updates, maintenance activities, and product revisions.

As a result, accurate configuration management is essential for ensuring that the appropriate software inventory information can be associated with a particular product instance.

Examples of information that may influence software composition include:

- Product model information
- Firmware versions
- Applied software updates

Combining SBOM information with accurate configuration management enables organizations to better understand their deployed assets and their associated software components.

3.2 Product Context Is Critical

While an SBOM identifies software components, it does not by itself determine whether a disclosed vulnerability poses a practical risk to a specific product.

The actual security impact of a vulnerability may depend on factors such as:

- Whether the affected functionality is used
- Product architecture and interfaces
- Available attack paths
- Existing security controls and mitigations

Consequently, product-specific analysis is often required to understand the real-world impact of newly disclosed vulnerabilities.

At OMRON, vulnerability management activities extend beyond software inventory analysis and include exploitability assessments, impact analysis, and determination of appropriate mitigation actions.

3.3 Supporting Efficient Security Operations

Organizations that integrate SBOM information into vulnerability management processes may identify numerous vulnerabilities associated with software components.

To effectively prioritize response activities, additional context is often needed, including:

- Product impact assessments
- Exploitability evaluations
- Available mitigations
- Recommended remediation actions

OMRON helps customers reduce the effort required to interpret vulnerability information by combining SBOM management with ongoing vulnerability analysis and product-specific security assessments.

4. OMRON Product Security Management Process

OMRON incorporates SBOM management into a comprehensive product security framework.

Our Product Security Incident Response Team (PSIRT) continuously monitors publicly disclosed vulnerabilities and reviews vulnerability reports received from researchers and external stakeholders.

When a newly identified vulnerability may affect an OMRON product, we perform:

- Software component correlation analysis
- Product impact assessment
- Exploitability evaluation
- Mitigation planning

Based on the results of these activities, OMRON may provide:

- Software updates
- Mitigation guidance
- Security advisories

This process supports continuous product security management throughout the product lifecycle.

5. Helping Customers Focus on What Matters

For customers, the most important security question is not merely whether a vulnerability exists, but whether that vulnerability is relevant to their environment and how it should be addressed.

OMRON's product security activities are designed to help customers make informed decisions by providing meaningful information rather than software inventory data alone.

Through continuous vulnerability monitoring, impact analysis, and security advisory communications, OMRON helps customers:

- Understand product-specific security implications
- Prioritize remediation efforts
- Reduce investigation time
- Improve overall security operations

This approach enables customers to focus resources on the issues that matter most to their environments.

6 . OMRON's Approach to Providing SBOM Information

OMRON recognizes the value of SBOMs in supporting customer security programs and software supply chain transparency initiatives.

At the same time, software composition information delivers the greatest value when accompanied by sufficient context to support meaningful risk-based decision-making.

SBOMs provide visibility into software composition, but they do not capture product-specific security assessments such as vulnerability impact analysis, exploitability evaluations, or triage decisions. Therefore, SBOM information is most effective when used together with additional context that supports accurate risk-

based decision-making.

Accordingly, OMRON works with customers to understand their security objectives and provides security-related information appropriate to those objectives that may include:

- Software composition information
- Product-specific security information
- Vulnerability impact assessments
- Security advisory information

Our goal is to ensure that customers receive information that supports practical and effective security management.

7. Conclusion

Software supply chain transparency and continuous product security management are becoming increasingly important across the industrial automation industry.

SBOMs play a valuable role by providing visibility into software composition and supporting vulnerability management activities. At OMRON, SBOMs are an integral part of our product security program.

However, effective product security management extends beyond software inventories. Continuous vulnerability monitoring, product-specific impact analysis, security advisories, and lifecycle-oriented security practices are all essential elements of a comprehensive security strategy.

By combining these capabilities, OMRON helps customers better understand product security risks, prioritize their response activities, and maintain secure and reliable industrial automation systems.

Together with our customers, partners, and suppliers, OMRON remains committed to fostering a safer, more secure, and more resilient industrial automation ecosystem.

8. Link

Product Security | OMRON Industrial Automation
https://www.fa.omron.co.jp/product/security/en/