MONTAVISTA SOFTWARE

Application

SOFTWARE BILL OF MATERIALS (SBOM): HOW MONTAVISTA IS STRENGTHENING SOFTWARE SUPPLY CHAIN SECURITY

Introduction: Transparency as the Foundation of Security

Modern software development relies heavily on open-source and third-party components. This dependency chain, while efficient, introduces significant risk: vulnerabilities in upstream libraries can silently propagate into downstream products. Recent supply chain incidents such as *SolarWinds* and *Log4Shell* have shown how deeply integrated components can become single points of failure for entire ecosystems.

A **Software Bill of Materials (SBOM)** is a formal, machine-readable inventory of all components, libraries, and dependencies that make up a software product. Conceptually similar to a parts list in manufacturing, an SBOM provides **transparency**—a detailed view of what's inside a software system, who produced it, and which versions are used.

The fundamental purpose of an SBOM is to give both developers and operators the ability to:

- Understand and document **what software is actually composed of**.
- Track **dependencies** across open-source and proprietary layers.
- Enable **rapid response** when vulnerabilities or licensing issues are discovered.

In short, the SBOM addresses a core weakness in modern cybersecurity: the lack of visibility into the digital supply chain. By exposing the full component tree, it allows organizations to assess exposure, manage updates, and build trust through verifiable transparency.

Managing Vulnerabilities and CVEs with SBOMs

The value of an SBOM becomes most apparent in **vulnerability management**, particularly when new **Common Vulnerabilities and Exposures (CVEs)** are published.

Without an SBOM, security teams must manually determine whether a product is affected by a vulnerability in a third-party library, often relying on incomplete or outdated documentation. With a complete SBOM, this task becomes straightforward:

1. Each software component is explicitly listed with version information.
2. These components can be automatically cross-referenced against vulnerability databases such as the NVD (National Vulnerability Database).
3. The results identify which CVEs are relevant to the specific software instance, enabling targeted and prioritized mitigation.

This transforms vulnerability response from reactive guesswork into a **data-driven process**. Automation can scan SBOMs at build time or during deployment to continuously evaluate risk exposure as new CVEs are announced.

Additionally, emerging formats such as the **Vulnerability Exploitability eXchange (VEX)** build upon SBOMs by clarifying *whether* a listed vulnerability actually affects the product's functionality or is mitigated by other factors. Together, SBOM and VEX can eliminate false positives and reduce patching overhead.

For example, when a CVE is published against a popular cryptographic library, a vendor can immediately query all SBOMs for products using that library, determine affected versions, and initiate updates within hours.

This capability is critical in large organizations maintaining many interdependent products, where even a single outdated dependency could lead to systemic compromise. By embedding SBOM management into the **CI/CD pipeline**, security posture becomes continuously measurable and maintainable.

SBOMs in the Context of the EU Cyber Resilience Act

The **EU Cyber Resilience Act (CRA)**, expected to take effect in 2025–2026, will redefine cybersecurity obligations for manufacturers and software providers across Europe. It introduces mandatory **Security-by-Design** principles and requires vendors to maintain detailed documentation of their software components, security updates, and vulnerability handling processes throughout the product lifecycle.

Within this framework, the **SBOM is emerging as a central compliance enabler**. While the Act does not explicitly name the SBOM as a required artifact, its principles align perfectly with CRA expectations:

- Manufacturers must **identify and document all components** included in their products.
- They must **track vulnerabilities** and ensure timely remediation.
- They must **communicate risks and updates** to users and regulators transparently.

An SBOM provides the technical foundation to meet all three obligations. It creates the traceability that the CRA demands — allowing authorities or customers to verify that a vendor understands its software composition and manages vulnerabilities responsibly.

Moreover, as supply chains cross borders, **SBOM standardization** becomes crucial for interoperability. The most widely adopted formats today are:

- **SPDX (Software Package Data Exchange)** — an ISO standard (ISO/IEC 5962:2021).
- **CycloneDX**, maintained by the OWASP Foundation, designed for security automation and integration with vulnerability data.

Adopting these formats early prepares organizations for both EU and international compliance landscapes. Companies that establish automated SBOM generation and maintenance now will face fewer disruptions when the CRA enforcement begins.

Beyond compliance, SBOM adoption signals **maturity and trustworthiness**. Customers, regulators, and supply-chain partners are increasingly demanding verifiable insight into the provenance of digital products. An accurate SBOM transforms software from a “black box” into a transparent, auditable asset—essential for both regulatory readiness and competitive advantage.

Using SBOMs with MontaVista MVShield, CGX and MVSecure

MontaVista offers a comprehensive suite of solutions for SBOM management through our core products, Carrier Grade eXpress (**CGX**) Linux and **MVShield**. Both platforms feature **SBOM generation** capabilities using industry-standard tools and formats, primarily **SPDX**, to ensure compliance and transparency across the customer's software supply chain. Conversion tools are available to support interoperability between various SBOM formats and simplify integration into the customer's workflows. Leveraging the built-in **trust scorecard component validation**, **CVE management with OVAL metadata**, and support for **industry-standard scanning tools** such as Tenable Nessus, CIS-CAT, and OpenSCAP, customers gain deep, automated insight into their security posture.

With **MVSecure** productized security services, MontaVista extends SBOM capabilities beyond generation to deliver **customized, intelligence-driven supply chain security** for each customer program. MVSecure enables tailored creation and processing of SBOMs that reflect the unique package composition and configuration of every embedded project. By correlating SBOM data with **continuous CVE fix feeds** from CGX and MVShield, MVSecure streamlines **vulnerability identification and prioritization**, empowering teams to proactively manage risks and maintain compliance with frameworks like NIST ZTA and the EU CRA.

MontaVista actively contributes to the evolving **SBOM-related standards**, including SPDX and VEX, ensuring alignment with the latest industry practices for software transparency and supply chain security. By closely following market trends and participating in standardization efforts, MontaVista delivers **field-proven, standards-compliant SBOM workflows** that integrate seamlessly with our products. This commitment allows customers to adopt trusted, interoperable SBOM processes that enhance vulnerability management, compliance, and long-term lifecycle security across embedded Linux deployments.

Summary

Comprehensive SBOM management is key to MontaVista's security-first strategy and approach to strengthening software supply chain security.

With over two decades of deep Linux and cybersecurity expertise supporting mission-critical applications, MontaVista delivers an integrated ecosystem through CGX, MVShield, and MVSecure, combining Secure-by-Design principles, Zero Trust architectures, and continuous vulnerability management. MontaVista's next-generation solutions ensure that customers deploying open source software to the field benefit from enhanced visibility, faster CVE response, and stronger protection against evolving software supply chain threats.

Please visit www.mvista.com and/or contact us at sales@mvista.com or leave a request for more information on our solutions.

MontaVista Software, LLC, is a leader in embedded Linux commercialization.

For over 20 years, MontaVista has been helping Linux developers get the most out of open source by adding commercial quality, integration, hardware enablement, expert support, and the expert resources of the MontaVista development community. Because MontaVista customers enjoy faster time-to-market, more competitive device functionality, and lower total cost, more devices have been deployed with MontaVista than with any other Linux.

For more information about MontaVista, visit http://www.mvista.com
Media Contact:
MontaVista Software LLC | E: pr-contact@mvista.com | T: +1 (669) 777-6841