Introducing OWASP CycloneDX v1.5: Advanced Bill of Materials Standard Empowering Transparency, Security, and Compliance

Incorporates Machine Learning transparency (ML-BOM), Formulation (MBOM), and enhanced support for SBOM quality indicators including evidence and lifecycles.

WAKEFIELD, MA, USA, June 26, 2023 /EINPresswire.com/ -- OWASP, the Open Worldwide Application Security Project, is proud to announce the launch of OWASP CycloneDX version 1.5, an innovative and advanced Bill of Materials (BOM) standard that addresses transparency and compliance in the software industry. CycloneDX v1.5 sets a new benchmark by incorporating Machine Learning transparency (ML-BOM), Formulation (MBOM), and enhanced support for Software Bill of Materials (SBOM) quality indicators, including evidence and lifecycles embracing both the Software Development Lifecycle (SDLC) and enterprise Software Asset Management (SAM). With today's announcement, CycloneDX extends the BOM beyond the hardware, software, and services it supports today, allowing organizations to better identify and reduce risk in their supply chain.

ML-BOM represents a developer-friendly advancement in BOM technology. With ML-BOM, CycloneDX provides insights into the machine learning models utilized in software systems. This transparency allows stakeholders to understand and verify the training and deployment methods employed, ensuring accountability and promoting ethical artificial intelligence (AI) practices.

“With the rapid rise of generative AI models, the stakes have never been higher for AI software deployments,” said Christian Hudon, Senior Applied Research Scientist at ServiceNow. “CycloneDX’s new support for ML transparency couldn’t have come at a better time to help companies manage their AI deployments in a more secure and transparent fashion.”

Another significant new feature of CycloneDX is the inclusion of Formulation, or Manufacturing Bill of Materials (MBOM), which provides comprehensive recipes of how a particular software system was created, trained, or deployed. This formulation information helps enhance transparency by enabling stakeholders to understand the development and deployment process, empowering them to evaluate the system's reliability, security, and potential risks associated with its formulation.

“This release of the CycloneDX specification is a milestone for any cybersecurity-aware company that wants to produce mature BOMs that capture critical information to address security risk and compliance assessments, especially in the area of Continuous Integration and Delivery (CI/CD) or “manufacturing” of the BOM’s subject software, hardware or service,” said, Matt Rutkowski, IBM, OWASP Maintainer and CycloneDX Contributor.

Furthermore, CycloneDX now incorporates multiple indicators to assess SBOM quality, including expanded evidence that captures multiple methods and techniques used to identify components.

“CycloneDX is making software transparency a reality. I’m very excited about all the new capabilities in CycloneDX v1.5, particularly the ability to capture detailed evidence proving the SBOM is correct, such as methods, techniques, and call stacks,” said Jeff Williams, co-founder and CTO of Contrast Security. “SBOMs aren’t just lists of ingredients anymore. CycloneDX supports services, machine learning, low code, vulnerability disclosure, formulation, and annotations to really capture what’s important about the software you depend on”.

CycloneDX now provides the most advanced license support available, encompassing opensource licenses for OpenChain conformance and commercial license support for enterprise SAM use cases. This comprehensive license support is another industry first that minimizes legal risks and strengthens the overall software ecosystem.

“Lockheed Martin supports open standards that benefit multiple industries and the needs of our customers,” said Jerod Heck, Software Factory Deputy Chief Architect at Lockheed Martin. “As an active participant in the CycloneDX Industry Working Group, we contributed to the CycloneDX 1.5 schema to strengthen tracking of commercial license information. The updated version enables Lockheed Martin to deliver Software Bill of Materials to customers more efficiently through an existing ecosystem of tooling.”

OWASP CycloneDX is the most widely used BOM format, adopted by leaders across many industries and standardized on by multiple world governments and U.S. federal agencies. By embracing CycloneDX, these organizations demonstrate their commitment to transparency, security, and responsible software practices.

Further information on the improvements in CycloneDX v1.5 can be found at https://owasp.org/blog/2023/06/23/CycloneDX-v1.5.html

To help organizations leverage the most from SBOMs, CycloneDX has also released the first in a series of guides. The “Authoritative Guide to SBOM, Implement and Optimize Use of Software Bill of Materials” is available now. This 60 page document covers essential and advanced topics from which every organization can benefit. The guide is available at https://cyclonedx.org/guides

With today’s launch of CycloneDX v1.5, OWASP is also kicking off the development of CycloneDX v1.6 bringing Cryptography Bill of Materials (CBOM) to the standard. With today’s announcement, CycloneDX formally launched a new Feature Working Group that will take on the challenge of introducing transparency of cryptographic assets and dependencies as the first step on the migration journey to quantum-safe systems and applications. Visit https://cyclonedx.org/participate to get involved.

OWASP CycloneDX is freely available, embodying the spirit of open collaboration and knowledge sharing that OWASP champions. This accessibility helps organizations of all sizes, from startups to enterprises, can leverage CycloneDX to bolster their software transparency, compliance, and security initiatives. To learn more about OWASP CycloneDX, access the standard, and leverage the over 200 tools that support CycloneDX, visit https://cyclonedx.org/. Join the global software community in embracing this innovative BOM standard and unlock a new era of transparency and compliance in the digital landscape.

About the OWASP Foundation
The Open Worldwide Application Security Project (OWASP) is a nonprofit organization that works to improve the security of software. Through community-led open source software projects, over 260 local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web. For over two decades corporations, foundations, developers, and volunteers have supported the OWASP Foundation and its work. To learn more or to become a member, visit https://owasp.org.

OWASP and the Open Worldwide Application Security Project are trademarks of the OWASP Foundation.

Steve Springett
OWASP Foundation
+1 773-998-2050
steve.springett@owasp.org
Visit us on social media:
Twitter
LinkedIn
YouTube

in today's world. Please see our Editorial Guidelines for more information.