EINPRESSWIRE

CycloneDX v1.6 Released, Advances Software Supply Chain Security with Cryptographic Bill of Materials and Attestations

CycloneDX builds upon a legacy of innovation, empowering organizations to reduce risk and enhance software and system transparency.

WILMINGTON, DE, USA, April 9, 2024 /EINPresswire.com/ -- The OWASP Foundation today announced the availability of CycloneDX v1.6. This significant release strengthens software supply chain security with the introduction of two innovative capabilities: Cryptographic Bill of Materials (CBOM), developed by IBM Research, and CycloneDX Attestations (CDXA).

CycloneDX v1.6 builds upon the existing strengths of the CycloneDX standard, which provides a machine-readable format for capturing the components that comprise software (SBOM), hardware (HBOM), services (SaaSBOM), and AI/ML models (AI/ML-BOM). CycloneDX builds upon a legacy of innovation, empowering organizations to reduce risk and enhance software and system transparency.

Cryptographic Bill of Materials (CBOM)
As quantum computer performance improves, at some point in the future they are expected to break many currently used cryptographic algorithms, such as RSA. To address the issue, companies and organisations can migrate their cryptographic assets to new post-quantum cryptographic algorithms that have been selected by NIST for standardization.

The Cryptographic Bill of Materials (CBOM), developed by researchers and software engineers at IBM, serves as a structured framework for inventorying cryptographic assets. This approach is detailed in OMB M-23-02 and is particularly focused on preparing for the transition to post-quantum cryptography (PQC). This preparation is underlined by the issuance of National Security Memorandum 10 from the White House. CycloneDX v1.6 simplifies the discovery, management, and reporting of cryptographic assets, laying the groundwork for migration to quantum-safe systems and applications. It facilitates the identification of weak cryptographic algorithms, promotes cryptographic agility, and ensures compliance with evolving cryptographic policies and advisories like CNSA 2.0, aligning with recommendations from NIST.

OWASP and the CycloneDX community would like to thank IBM Research for developing CBOM.

"The introduction of our CBOM in CycloneDX 1.6 is a significant milestone for managing the cryptography supply chain," said Michael Osborne, CTO of IBM Quantum Safe. "CBOM is the first open standard to describe an organizations' cryptographic assets inventory, and their dependencies, giving organizations deeper visibility into the cryptography they use, enabling them to assess their quantum readiness, and to consider actionable steps towards becoming quantum safe."

CycloneDX Attestations (CDXA)

CycloneDX Attestations are a modern capability for security compliance. They enable organizations to communicate standards, claims, and evidence in support of requirements, along with attestations to the veracity and completeness of those claims.

"Modern software is tremendously complex, and ensuring compliance with the dizzying array of standards is overwhelming," said Jeff Williams, CTO of Contrast Security and the first Global Chair of OWASP. "CycloneDX Attestations (CDXA) makes "compliance as code" possible with machine-readable security standards and compliance documentation, instead of endless PDFs, spreadsheets, and paper evidence. With CDXA, you can automate production of compliance evidence, streamline communication between all compliance stakeholders, facilitate discussions about substantive security issues, handle exceptions, and manage signatures. We're hoping CDXA marks the beginning of a new era where compliance and security are not entirely different things."

Advancements to AI/ML Transparency

Numerous other improvements are included in CycloneDX v1.6 including environmental considerations which enhance CycloneDX's existing support for AI/ML model cards. The incorporation of environmental data in CycloneDX v1.6 transforms AI development, offering transparency into energy usage and CO2 emissions across all stages, from training to inference. This integration enables informed decision-making, fostering sustainable technological practices. CycloneDX seamlessly integrates environmental considerations into AI development, promoting harmony between innovation and ecological preservation.

"Manifest relies on open SBOM formats not only for our internal security, but to help customers of our SBOM-powered security platform around the world." said Daniel Bardenstein, CTO and co-founder at Manifest Cyber. "CycloneDX 1.6 is a significant step forward for the global security community, unlocking both critical attestation workflows as well as evolved transparency for machine learning. The enterprises we support have been eagerly awaiting this release, and we look forward to continued innovation and partnership from the OWASP CycloneDX community well into the future."

CycloneDX 1.6's Journey Towards International Standardization

This release underscores the commitment of the CycloneDX community to fostering a collaborative and innovative environment. The OWASP Foundation along with Ecma International have created an inclusive, community-driven ecosystem for security standards development. This collaboration empowers individuals to contribute their expertise and insights, ensuring that standards like CycloneDX reflect the collective wisdom of the global cybersecurity community. This effort is led by Ecma Technical Committee 54 (TC54).

"Well-defined, standards-based, and interoperable SBOM formats are a key building block for Bloomberg's secure use of open source software. Bloomberg is very happy to see CycloneDX v1.6 on track to become an Ecma International standard sometime in 2024, with ISO standardization happening shortly thereafter," said web standards author Daniel Ehrenberg, a software engineer with Bloomberg's JavaScript Infrastructure & Tooling team and Vice President of Ecma International. "Through deep technical review and community outreach, Ecma is working to ensure that the definition of this format is transparent, interoperable, and technically rigorous. We welcome everyone interested to join and participate in this process. Ecma and OWASP are natural collaborators due to our shared focus on engineer-led pragmatism, equality among members, and openness."

New Authoritative Guides Available
To accompany the launch of CycloneDX v1.6, the community is pleased to announce the immediate availability of three new guides to help organizations make the most out of CycloneDX.

* Authoritative Guide to CBOM
* Authoritative Guide to Attestations
* Authoritative Guide to SBOM, Second Edition

These comprehensive guides, available at https://cyclonedx.org/guides/, provide in-depth information about the new features in CycloneDX v1.6 and best practices for their implementation.

To learn more about OWASP CycloneDX, access the standard, and leverage the over 220 tools that support CycloneDX, visit https://cyclonedx.org/.

About the OWASP Foundation
The OWASP Foundation 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 nearly two decades corporations, foundations, developers, and volunteers have supported the OWASP Foundation and its work. To learn more or to become a member, visit

Steve Springett

OWASP Foundation
+1 773-998-2050
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/700694330