Generating a Software Bill of Materials (SBOM) with Open Source Standards and Tooling

Every month there seems to be a new software vulnerability showing up on social media, which causes open source program offices and security teams to start querying their inventories to see how FOSS components they use may impact their organizations.

Frequently this information is not available in a consistent format within an organization for automatic querying and may result in a significant amount of email and manual effort. By exchanging software metadata in a standardized software bill of materials (SBOM) format between organizations, automation within an organization becomes simpler, accelerating the discovery process and uncovering risk so that mitigations can be considered quickly.

In the last year, we’ve also seen standards like OpenChain (ISO/IEC 5320:2020) gain adoption in the supply chain. Customers have started asking for a bill of materials from their suppliers as part of negotiation and contract discussions to conform to the standard. OpenChain has a focus on ensuring that there is sufficient information for license compliance, and as a result, expects metadata for the distributed components as well. A software bill of materials can be used to support the systematic review and approval of each component’s license terms to clarify the obligations and restrictions as it applies to the distribution of the supplied software and reduces risk.

Kate Stewart, VP, Dependable Embedded Systems, The Linux Foundation, will host a complimentary mentorship webinar entitled **Generating Software Bill Of Materials** on Thursday, March 25 at 7:30 am PST. This session will work through the minimum elements included in a software bill of materials and detail the reasoning behind why those elements are included. To register, please click here.

Register for webinar
There are many ways this software metadata can be shared. The common SBOM document format options (SPDX, SWID, and CycloneDX) will be reviewed so that the participants can better understand what is available for those just starting.

This mentorship session will work through some simple examples and then guide where to find the next level of details and further references.

At the end of this session, participants will be on a secure footing and a path towards the automated generation of SBOMs as part of their build and release processes in the future.

The post Generating a Software Bill of Materials (SBOM) with Open Source Standards and Tooling appeared first on Linux Foundation.