Ke, Jessica - Intern

From: Gauthami Polasani <gauthami@fossa.com>
Sent: Thursday, June 17, 2021 2:24 PM
To: SBOM_RFC
Subject: Comments on RIN 0660–XC05: Software Bill of Materials Elements and Considerations

All - Please find below our comments on the questions posed in the regulations published.

1. Are the elements described above, including data fields, operational considerations, and support for automation, sufficient? What other elements should be considered and why?

- *The below should be included as additional data fields in the SBOM -*
    - *Package Download URL*
    - *Licenses used*
    - *Latest version available*

The download URL helps clarify where the package came from and adds an additional layer of security and confidence to the origins of the package. Part of the risk with open source comes from licenses so the licenses used in the component should form part of a SBOM. The latest version available helps the users determine the age of the current version and if they risk using stale packages.

2. Are there additional use cases that can further inform the elements of SBOM?

Provenance of the packages

> *With malicious actors constantly increasing their attack surface, keeping track of the origin and composition of packages becomes really crucial in avoiding supply chain attacks.*

Licensing risk

> *One of the original use cases for SBOM and one that is still relevant in terms of risk mitigation.*

3. SBOM creation and use touches on a number of related areas in IT management, cybersecurity, and public policy. We seek comment on how these issues described below should be considered in defining SBOM elements today and in the future.

d. Integrity and authenticity: An SBOM consumer may be concerned about verifying the source of the SBOM data and confirming that it was not tampered with. Some existing measures for integrity and authenticity of both software and metadata can be leveraged.

Currently there are no standards on how SBOMS are built/generated. Having such a standard would help automate the process of scanning/processing SBOMs which would be essential to determining integrity of the SBOM itself

Thanks

Gauthami Polasani