Enhanced Software Security through SBOM Management and Analysis

May 2024

Introduction

The vast majority of commercial and custom applications contain open source code. Typical vulnerability analysis tools do not inspect individual open source components within applications, although any one of these components may contain vulnerabilities or obsolete code that can put you at risk. This was clearly demonstrated with the Log4j vulnerability that enabled the massive cybersecurity attack that spread to SolarWinds customers in 2020.

In response to ongoing breaches, many of which target the global supply chain, multiple international organizations have developed mandates, directives and guidelines to minimize the threat of future attacks.

In the United States, President Biden issued Executive Order 14028 in May 2021. This order defines security measures that must be followed by any software publisher or developer that does business with the federal government. Additionally, in December 2022, the signing of Section 3305 of the Consolidated Appropriations Act of 2023 authorized the Food and Drug Administration (FDA) to establish cybersecurity standards for medical devices.

In the European Union, the Network and Information Security (NIS) Directive established EU-wide legislation on cybersecurity. The subsequent NIS2 agreement, put into force in January 2023, obligates more entities and sectors to take measures to increase the level of cybersecurity in Europe.

Specific industries are also enacting guidelines, with the banking and financial sectors taking the lead. The New York State Department of Financial Services' 23 NYCRR500 with Incorporated Second Amendment spells out requirements and compliance measures for financial institutions that are based in or doing business in the State of New York. In the EU, the Digital Operational Resilience Act (DORA) [Regulation (EU) 2022/2554] also defines uniform requirements concerning the security and risk management of network and information systems in the financial industry. These are just a few of the initiatives being developed and enacted.

The Software Bill of Materials (SBOM)

These guidelines and mandates have at least one common element: they each require all software developers to provide a Software Bill of Materials – or SBOM - a complete inventory list of components and libraries that make up a software application.

The National Telecommunications and Information Administration (NTIA) defines an SBOM as *"a…complete, formally structured list of components, libraries, and modules that are required to build (i.e. compile and link) a given piece of software and the supply chain relationships between them. These components can be open source or proprietary, free or paid, and widely available or restricted access."*

The NTIA also compiled and published initial guidelines for the minimum content that should be included in an SBOM.

SBOMs also follow National Institute of Standards and Technology (NIST) guidelines that encourage consistent content and promote the development of approved human- and machine-readable file formats including SPDX (Microsoft) and CycloneDX (OWASP).

Another SBOM standard is the ISO International Standard for Open Source license compliance. The ISO/IEC 5230:2020 Information Technology – OpenChain Specification defines a process for managing a bill of materials for supplied software. This standard aligns with NTIA guidelines and pushes for SBOMs that include all components, not just the open source ones.

SBOMs typically contain the following information about applications:

- Open source code
- Proprietary code
- Associated licenses
- Versions in use
- Download locations for components
- Dependencies and sub-dependencies

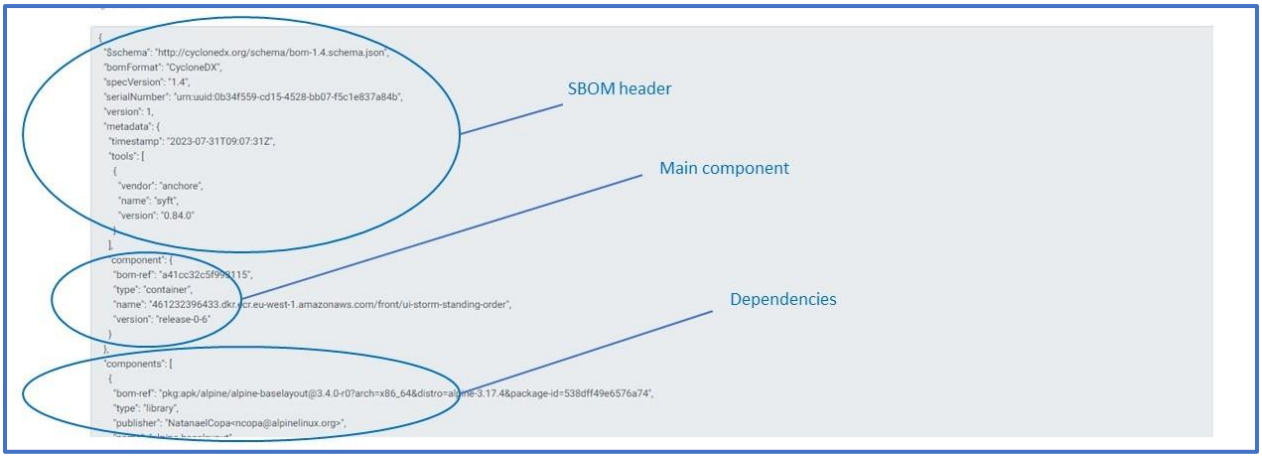

Fig. 1: A sample SBOM file with content breakdown

Uses for SBOMs

A key benefit of SBOMs is that they enable organizations to identify whether any of the components that make up a software application may have a vulnerability that can create a security risk. The Log4Shell zero-day vulnerability that was exploited in Apache Log4j2 is a perfect example. While U.S. government agencies will be mandated to adopt SBOMs, it's likely that many commercial companies will soon find this extra level of security appealing.

SBOMs organize data so that it is usable by third-party tools for:

- Vulnerability Management
- Obsolescence Management
- License Exposure Analysis

The data in SBOMs can be leveraged by Security, License Management, Operations, Legal and Procurement teams.

Who Can Benefit from using SBOMS?

If your company uses software for business purposes, it is a *Consuming Organization*. You absolutely need to understand any risk that may be present in the software provided to you from any source.

If you are a software *Publishing Organization*, whether for commercial sale or for in-house/bespoke usage, you need to understand the potential risks presented by the products and versions that you offer to Consuming Organizations. You also need to understand the open-source license types that you are utilizing (i.e., Permissive, Strong Copy Left) to avoid risks to your proprietary IP and applications.

Getting Started with SBOMs

No matter the type of organization, a significant challenge will be determining how to get started. Every organization will be receiving and managing SBOMs for every product in their portfolio, as well as the associated mitigation processes to address any vulnerabilities that may be found. Waiting to begin won't make it easier, but there are solutions that can make SBOM management and analysis much easier.

There are two key aspects that every organization will have to address when using SBOMs:

1) Having a tool that can quickly read all of the details in an SBOM, match the results to known vulnerability data, and provide heads-up reporting

2) Being able to establish an automated, proactive process to stay on top of SBOM-related activity and all of the unique mitigation options and processes for each component or software application.

As a key component of Eracent's Cybersecurity Management Suite™ (CSMS™), the cutting-edge CSMS SBOM Manager™ is unique in that it supports both of those aspects to provide an additional, critical level of protection to minimize software-based security risks. The SBOM management process is one pillar of the broader discipline of Supply Chain Risk Management (SCRM).

SBOM Content Analysis and Vulnerability Reporting

Thoroughly analyzing the content of each SBOMs is essential to realize the benefits that they can provide. The CSMS SBOM Manager automatically reads the content of SBOMs and matches each listed component to the most currently available vulnerability data, which is constantly updated in Eracent's IT-Pedia® IT Product Data Library.

IT-Pedia is a single, authoritative source for foundational information about millions of IT hardware and software products. IT-Pedia provides component-level data normalization, Lifecycle Dates and Vulnerability Data, and much more. These details are consolidated from many sources and are fully auditable.

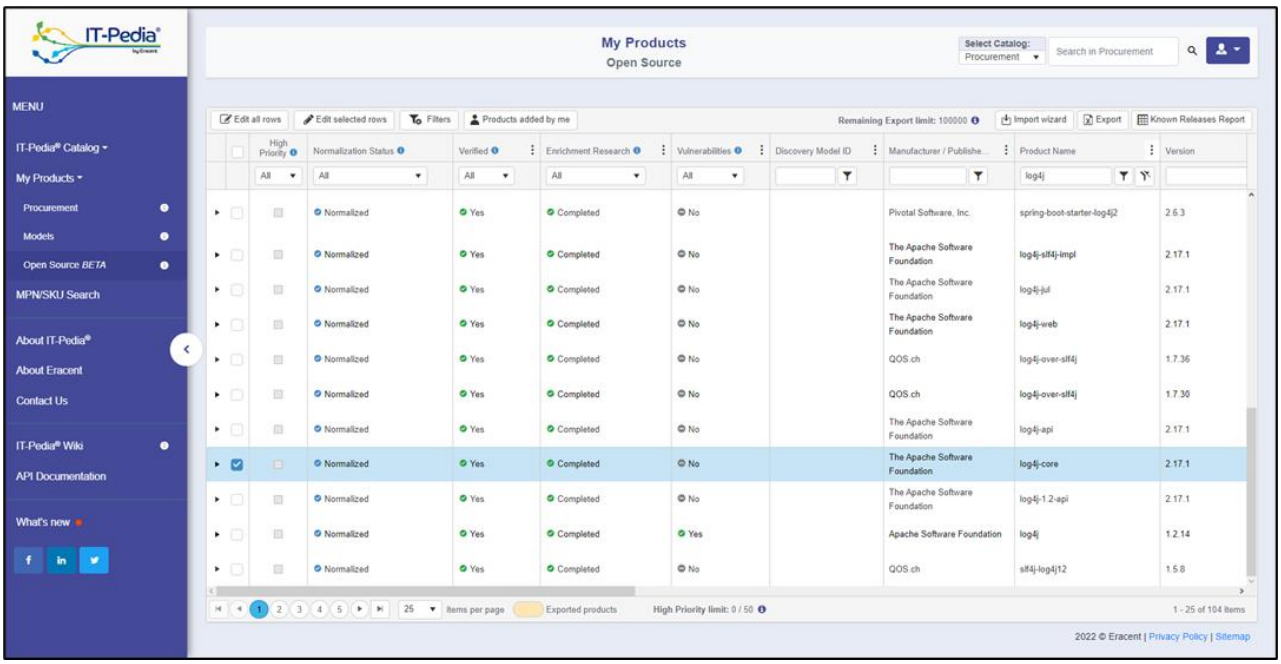

Fig. 2: IT-Pedia “My Products” Interface for Open Source Components

The Content Analysis and Vulnerability Reporting process provides instant visibility into any component-level vulnerabilities that need to be mitigated. It also identifies obsolete code that has not been updated recently and may now pose a security risk.

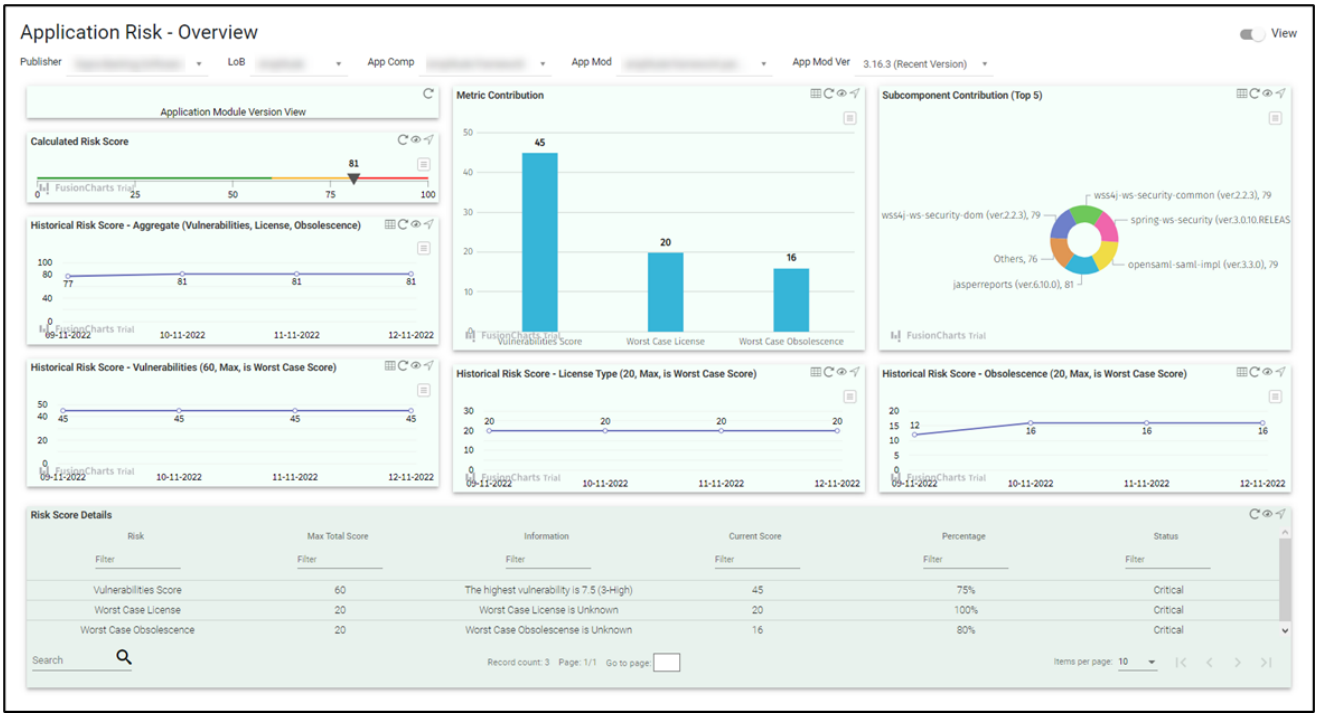

Fig. 3: CSMS SBOM Manager™ High-Level Overview Dashboard

Fig. 4: CSMS SBOM Manager™ Vulnerabilities Overview Dashboard

Proactive SBOM Process Management

In addition to analyzing the content of SBOMs, the CSMS SBOM Manager also provides a consolidated repository and centralized management point for all of an organization's SBOMs. The system provides structure, automation and reporting around all things SBOM-related. The CSMS SBOM Manager can be invaluable when initially setting up a proactive, automated SBOM program and it helps maintain a successful program moving forward.

If you know what code is embedded in the solutions that you use, you can stay ahead of issues that may be presented by the underlying components. When a zero day vulnerability is identified and published, if it relates to a component or library in one of your applications, you now have the ability to react rapidly.

The functionality of the CSMS SBOM Manager supports an evolving, iterative SBOM management process. You can focus on and prioritize SBOMs and mitigation processes based on various criteria:

- the most critical applications
- data types
- prioritizations
- classifications
- potential impact to the organization
- and more.

What benefits does the CSMS SBOM Manager process provide?

1) **A Centralized SBOM Repository** - The centralized repository in the CSMS SBOM Manager contains every SBOM from each of your suppliers. As a result, it can present the potential vulnerabilities and obsolescence of all components and libraries in real time. SBOMs are often far more current than a publisher's latest known issues list for an application, so they eliminate information lag time and customers are able to stay ahead of potential incidents.

2) **Comprehensive Process Management** – The CSMS SBOM Manager provides a single unified system that consolidates all of an organization's SBOMs, so the process can be managed as a whole. It establishes a single source of management and knowledge for all vulnerabilities corporate-wide or by business unit, team, etc. Flexible permissions enable different teams to have access to the information from different SBOMs based on platforms, system functions, software vendors and products that they utilize, and more.

3) **Automated SBOM Coverage and Monitoring** - Because permissions can be set up for each SBOM, it's possible to automate whether - and how - SBOMs are being managed and watched. It's also easy to identify any SBOMs that don't have an active manager or ownership.

4) **A Single Management Point for Publishing Organizations** - Software developers and vendors can also benefit from SBOM management tools. Taking advantage of a Context engine like the one in Eracent's Cybersecurity Management Suite, they can list all of their customers and the software that each of them has purchased. This provides visibility into:

- which offerings have the largest customer exposure
- SBOMs that have the largest customer base
- which customers have the most significant vulnerability or obsolescence exposure
- and more.

These issues can then be addressed as necessary. SaaS offerings can be prioritized for upgrades, on-premises installed applications with issues can be identified, and the publisher may communicate with customers in a proactive manner.

5) **Obsolescence Management** - For vendors and user organizations, SBOMs combined with the CSMS SBOM Manager provide additional value in the form of obsolescence management for components. The start- and end-of-life dates for each component included in an application can be tracked, as well as how many versions may have been released since the version utilized in an application, and more. You can avoid applications that contain outdated code that may put you at risk.

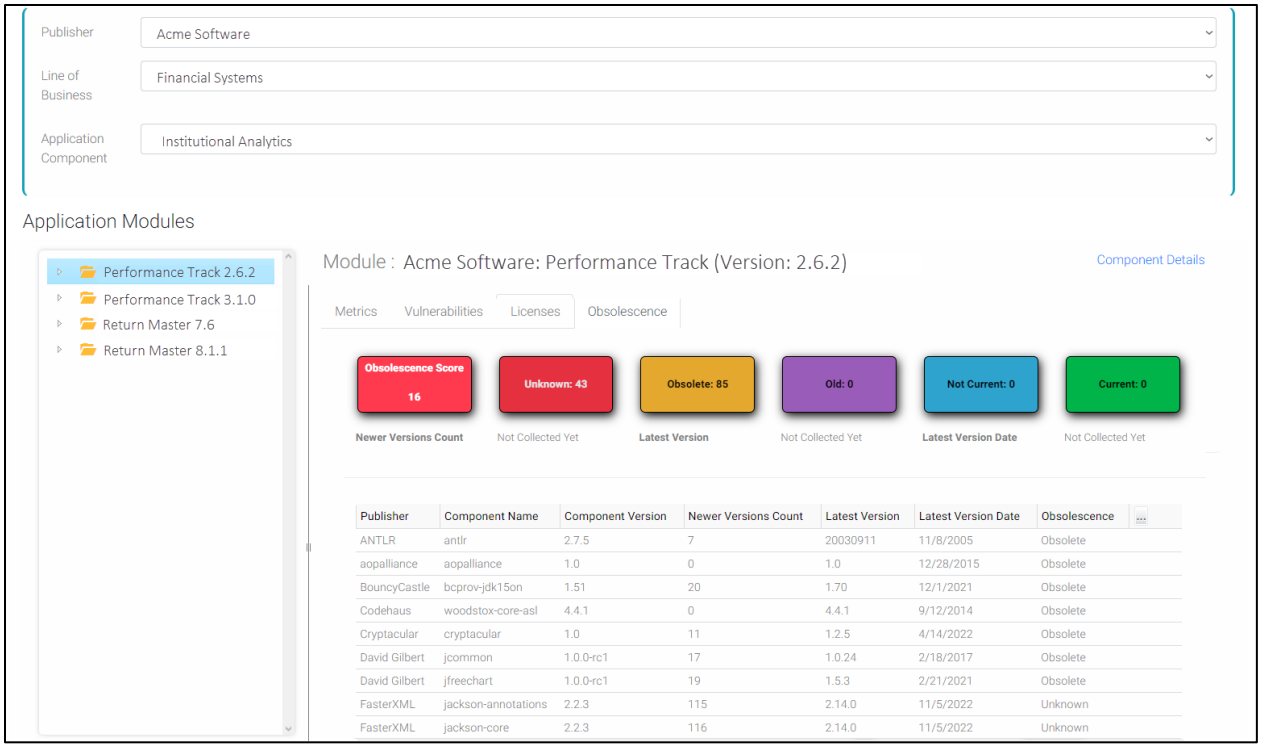

Fig. 5: Obsolescence Dashboard

6) **Score-based Reporting** – The Cybersecurity Management Suite's SBOM Manager provides detailed, actionable reporting as well as executive dashboards. Executives do not need to understand every data point or all information, so the system provides a concise summary, presents current scores, and can show a CISO specifically why a particular application may have a poor score at a particular point in time. Scores are kept in a time-series repository showing how various SBOMS (and their related applications) age. Some age better or worse than others.

7) **Licensing Exposure Analysis** – It's crucial to know what open-source licensing is in place for components and libraries that you are using. Permissive licensing enables code to be used with minimal implications, whereas the use of components under Strong CopyLeft and other license types may require you to share your IP. **Make sure your IP remains yours!**

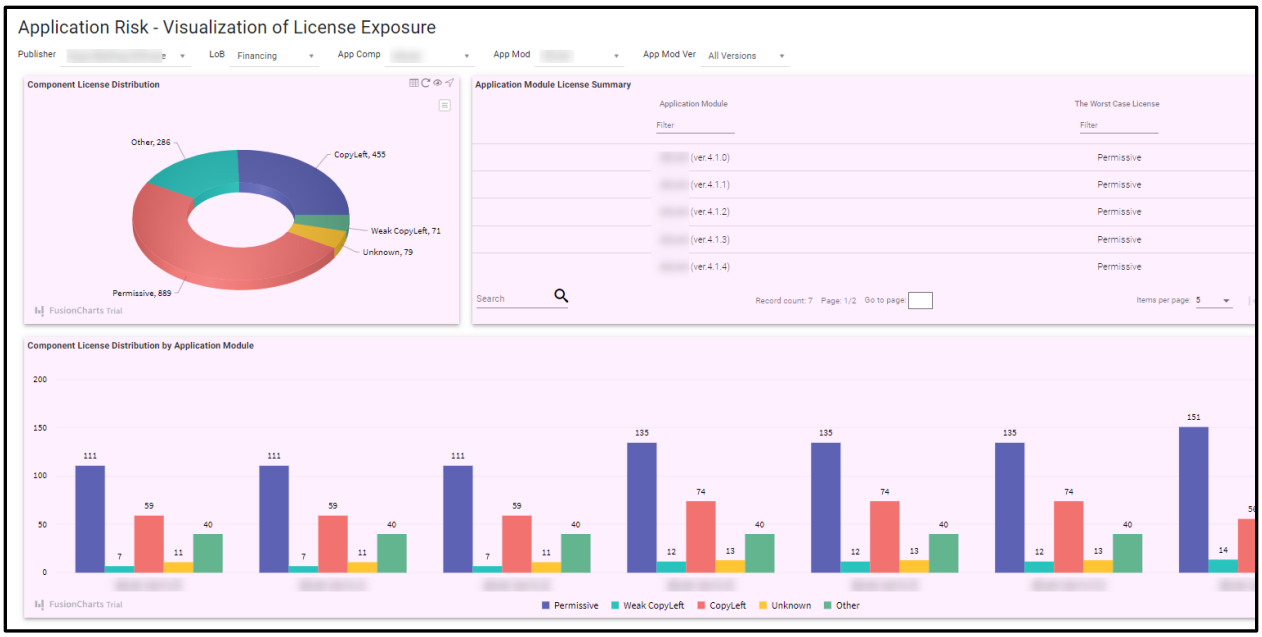

Fig. 6: License Exposure Dashboard

Summary

SBOMs will be available for any organization to use – take advantage of the information that they offer. SBOMs provides an extra layer of software-based security, and support Vulnerability Management, Obsolescence Management, and License Exposure Reporting.

A comprehensive SBOM management system will help establish and maintain an effective SBOM program.

Eracent's CSMS SBOM Manager can be used as a standalone solution, or it may be integrated as part of Eracent's broader Cybersecurity Management Suite™ and IT Management Center (ITMC) suite for IT Asset Management (ITAM) and Software Asset Management (SAM).

Fortify your organization's security with the additional level of protection provided by SBOM analysis. To learn more about the process and see a demo of the CSMS SBOM Manager, contact Eracent today.

Eracent, Inc.
519 Easton Road, P.O. Box 647
Riegelsville, PA 18077 USA

info@eracent.com
+1- 908-537-6520

eracent.com