Software bill of materials (SBOM)

A critical component of software supply chain security

Software bill of materials (SBOM)

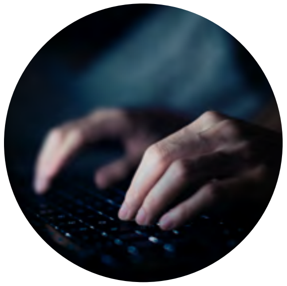
A critical component of software supply chain security

Introduction

Ensuring strong software security and integrity has never been more important because software drives the modern digital business. High-profile vulnerabilities discovered over the past few years, with the potential to lead to attacks against organizations using the software, have hammered home the need to be vigilant about vulnerability management.

Perhaps the most dramatic recent example was the zero-day vulnerability discovered in Apache's popular open-source **Log4j logging service.** The logging utility is used by millions of Java applications, and the underlying flaw — called Log4Shell — can be exploited relatively easily to enable remote code execution on a compromised machine. The impact of the vulnerability was felt worldwide, and security teams had to scramble to find and mitigate the issue.

In November 2022, open-source toolkit developers announced two high-severity vulnerabilities that affect all versions of OpenSSL 3.0.0 up to 3.0.6. OpenSSL is a toolkit supporting secure communications in web servers and applications. As such, it's a key component of the Transport Layer Security (TLS) protocol, which ensures that data sent over the internet is secure.



SBOM as a solution

One of the most effective tools for finding and addressing such vulnerabilities and keeping software secure is the software bill of materials (SBOM). SBOMs are formal, machine-readable records that contain the details and supply chain relationships and licenses of all the different components used to create a particular software product. They are designed to be shared across organizations to provide transparency of the software components provided by different players in the supply chain.

Many software providers build their applications by relying on open-source and commercial software components. An SBOM enumerates these components, creating a "recipe" for how the software was created.

For example, something like the OpenSSL toolkit includes dependencies that are difficult or, in many cases, impossible for traditional vulnerability scanners to uncover. It requires a multilayered approach to help security teams identify third-party libraries associated with a software package. This is where an SBOM can help.

The U.S. Department of Commerce has stated that SBOMs provide those who produce, purchase and operate the software with information that enhances their understanding of the supply chain. This enables multiple benefits, most notably the potential to track known newly emerged vulnerabilities and risks.

These records form a foundational data layer on which further security tools, practices, and assurances can be built, the Commerce Department says, and serve as the foundation for an evolving approach to software transparency.

A 2022 report by the Linux Foundation Research, based on a survey of 412 organizations from around the world, showed that 90% of the organizations had started their SBOM journey.

More than half of the survey participants said their organizations are addressing SBOMs in a few, some, or many areas of their business, and 23% said they are addressing them across nearly all areas of their business or have standard practices that include the use of SBOMs. Overall, 76% of organizations had a degree of SBOM readiness at the time of the survey.

The research showed that the use of open-source software is widespread, and that software security is a top organizational priority. Given the worldwide efforts to address software security, SBOMs have emerged as a key enabler, it said. Growth of SBOM production or consumption was expected to accelerate by about 66% during 2022, leading to SBOM production or consumption use by 78% of organizations.

The top-three benefits of producing SBOMs identified by survey participants were that SBOMs made it easier for developers to understand dependencies across components in an application, monitor components for vulnerabilities, and manage license compliance.

- **Understand dependencies across components in an application**
- **Monitor components for vulnerabilities**
- **Manage license compliance**

Key features to consider

SBOMs are a key to quickly finding and fixing vulnerabilities before it's too late. That's because they dig deep into the various dependencies among software components, examining the compressed files with applications to effectively manage risk. It might take a software vendor days or weeks to confirm with its developers whether its products are affected or not. That's too long a window of opportunity in which cybercriminals can exploit vulnerabilities.

Almost all SBOM solutions provide only build-time information. Build-time only gives you only details on applications during the developer phase and lacks up-to-date information on applications installed in an organization's environment.

With SBOMs, security teams can know exactly where an affected component is being used across applications in use within their organizations.

It's important for organizations to understand that not all SBOM offerings from vendors are alike. An ideal solution delivers critical, real-time visibility into an organization's software environments, enabling them to make better-informed decisions to manage risk.

SBOMs should be able to answer questions such as:

- Exactly where is a particular software package located?
- Which open-source dependencies, if any, does an application use?
- Which version of the software package is running?
- Do any other applications use the software package?

A key capability includes having the ability to understand every software component at runtime, uncover software packages and break them apart to examine all constituent components without the need to engage the software vendor.

A runtime SBOM provides the most accurate, up-to-date information because it contains details on the applications installed in your environment — not just the ones running. It's a critical feature because there may be versions of an application that a developer is changing or enhancing. With a runtime SBOM, you get information about what's happening in your environment now — not days or weeks later.

SBOMs should also be able to address any vulnerabilities or misconfigurations found in the various software components; take quick action to mitigate supply chain risk, even removing applications completely across affected endpoints; and optimize an organization's investments in third-party tools by populating them with granular, accurate and real-time SBOM data.

The takeaway

Digital businesses today rely on software to support all kinds of processes. In fact, it's difficult to imagine any company operating without applications. Keeping software secure and reliable is essential for success today.

With solutions such as SBOM, security teams at organizations can be confident that they have a good handle on all the complexities inherent in the software world, and that they are keeping up on any flaws that need to be addressed to keep applications secure.

Learn how Tanium's Converged Endpoint Management (XEM) platform can address SBOM to give your organization real-time visibility — even in the most complex software environments.

LEARN MORE

Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. More than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.

© Tanium 2023