Achieving a more secure **software supply chain**

Open-source and DevOps can give agencies the power to modernize, but not without proper controls

Stephen Magill

Sonatype

Open-source software comprises 70% to 80% of a typical commercial application. And it is increasingly feeding into federal software supply chains. Free and readily available open-source components allow agencies to save time and money and, in many cases, improve quality. However, not all components are created equal.

Sonatype's research shows that within the Java ecosystem, 1 in 12 components contains a known security vulnerability. And more widely used projects are more likely to have vulnerabilities exposed; within JavaScript, 39% of the most popular components have a known vulnerability. This highlights the security challenges that agencies are up against.

Security teams often focus on updating and securing existing components. But the initial choice of which open-source library to use is equally important. A common approach is to choose the most popular option. In Sonatype's 2021 State of the Software Supply Chain Report, however, an analysis of security versus popularity found that the most popular libraries often have the most security issues.

We advocate paying attention to a project's processes and noting whether the developers have built the capacity to release quickly and respond quickly to incidents. Furthermore, pulling in one component means pulling in all the components that it depends on, so agencies should make sure the development team is following best practices for keeping dependencies up-to-date as well.

A question of national security

There is a lack of transparency in how much open-source software is being used throughout the federal government. A disconnect between developers and security teams makes it difficult to rectify this.

But in today's world, understanding what's in the supply chain is critical to national security. All government and contractor software developers need to think critically and not only ask themselves "does the code have vulnerabilities?" but "could it have vulnerabilities?" and "how do we know either way?"

Developers can't answer those questions if they don't know what code they're using, which is why software bills of materials are critical to managing any software supply chain. An SBOM is a comprehensive list of a given product's software components, open-source licenses and dependencies. It offers valuable insight into the software supply chain and potential risks.

Fortunately, many of the challenges related to the use of software components with known vulnerabilities and software supply chain mismanagement can be easily solved with education, the right tools and the right organizational policies.

Building the capacity for innovation

For agencies that want to reduce risk without negatively affecting efficiency, automation is imperative. The incredible

Luca Bravo

> “Within the Java ecosystem, **1 in 12 components contains a known security vulnerability.** And more widely used projects are more likely to have vulnerabilities exposed.”

volume of artifacts consumed by organizations today quickly outpaces the capacity provided by manual review processes. Automation allows agencies to deal with that volume and still achieve great outcomes with respect to code health, vulnerability identification and risk remediation.

Automation can also help agencies build capacity to update open-source software on a regular basis. By routinely and automatically applying patches, agencies protect themselves from known vulnerabilities while improving their ability to respond quickly to zero-day attacks.

In addition, exemplary platforms and teams along the lines of the Defense Department’s Platform One and the Air Force’s Kessel Run give agencies the opportunity to push innovation throughout the organization. Such programs provide an environment to share best practices and are an integral part of driving innovation.

By building on the successes of such programs and investing in research to develop the next wave of technology advancements, agencies can accelerate and secure software capabilities across the government. ■

Stephen Magill is vice president of product innovation at Sonatype.