451 Research

Mission Possible: securing the open source software supply chain with Sonatype

Analyst: Wendy Nather

24 Apr, 2013

Everyone's a critic. In the world of application security, this is particularly so, with plenty of scanners, fuzzers, analyzers and testers. Given the number of vulnerabilities that routinely show up in code, it's easy to report on what's wrong. It's another thing entirely to try to fix it.

As steward of the Central Repository for Java open source components, Sonatype has a bird's-eye view of just how many open source components are being downloaded every day, and by whom. This vantage point helps inform the company's other offerings, but it also presents a rare opportunity to do something concrete in the application security world. Sonatype recently announced the general availability of its Component Lifecycle Management (CLM) product line to help organizations get better visibility into and control of their open source use. But its potential usefulness isn't limited to the enterprise.

The 451 Take

The purpose of Sonatype's CLM platform is to get out of the way of agile developers and let them do their thing, while at the same time keeping track of the versions, vulnerabilities and licensing of the open source components they're using. If enterprises are looking to secure their software supply chain, this is a great start – especially if their code is not written, but rather assembled from open source components. IDE integration and easy migration to newer versions can help with this work.

But the implications go beyond the individual enterprise level. Since so much open source software is in use, with or without the knowledge of management, enterprises may be more vulnerable than they know. This is one of the first tools we've seen that comes close to providing remediation support, not just scan results and recommendations. This could be a step toward making software more secure across the industry, especially if it's supported by enough partners.

Context

Sonatype was founded in 2008 by Jason van Zyl, its CTO, who also founded the Apache Maven project, among other open source initiatives. The company most recently brought in a new chief security officer, Ryan Berg, who was cofounder and chief scientist at Ounce Labs (now part of IBM's AppScan suite). CEO Wayne Jackson formerly held the same position at Sourcefire, as well as at Riverbed Technology, which he founded.

Based in Silver Spring, Maryland, Sonatype built on an initial $5m investment with $11.6m in 2010 from Accel Partners, Hummer Winblad Venture Partners, Morgenthaler Ventures and Bay Partners. In 2012, a $25m series C round added New Enterprise Associates as another investor.

Products

Nexus is Sonatype's repository manager, used to proxy and cache frequently used artifacts from remote code repositories (such as the Central Repository). It is available as open source and as a paid version, Nexus Professional. One recently announced update to Nexus Professional in version 2.3 is support for Yum repositories so that customers can manage their RPM packages and NuGet support for .NET components. Another added feature is SSL support for secure connectivity to the Central Repository, which is available not only for Nexus, but also – for a small donation – for other repository managers as well. (We do confess to being a bit puzzled as to why SSL wasn't already a given, but this just shows again that even in the open source world, security is not necessarily the top priority.)

Sonatype's Application Health Check is the quality management functionality that identifies licensing issues, known security vulnerabilities in particular versions, and shows how popular a particular component is (that is, how often it's been downloaded).

As keeper of the Central Repository, Sonatype stands watch over more than 400,000 open source components. The company says that it enforces minimum criteria for code submissions (for example, all source code must be included along with documentation, and all JAR files must be signed). Its validation, which is performed in a 'white room environment' isolated from both producers and consumers, includes ensuring that submitted fixes actually take effect. Validated components are signed with two different keys, and these signatures can be revoked and reissued if needed. In this way, Sonatype vouches for the provenance of the open source code – something that many enterprises have been relying on, as they don't always have resources to vet the open source code themselves.

From this vantage point, Sonatype can see just how heavily these components are being used, and in how many organizations. The company points out that complexity is a big problem, as one component can have dependencies on hundreds of others, and enterprises typically consume thousands of components every month. Add to that the fact that open source components can be updated four or more times a year, and it's clear that only automation will allow an enterprise to keep tight control over everything it's using.

This automation comes in the form of Sonatype's newly announced Component Lifecycle Management suite, which pulls all of its offerings together in one platform. Integrating with the IDE, the CLM platform allows developers to browse the repository and see detailed information on all of the components: which versions are available, which ones are most often used, and which versions have known vulnerabilities. It can also suggest component updates and allow the developers to compare versions side by side to determine the ramifications and impact on dependencies. The migration can be carried out automatically if the developer chooses, with a click that launches the refactoring within the IDE tool.

On the management side, customers can discover and inventory the component versions in their software and see risk levels for each; they can also set policies to govern their use. An organization can prohibit the use of particular versions that are older than two years, or issue warnings when a component in production applications has a highly critical security vulnerability that is fixed in a newer version. Equally important, users can see which types of licenses appear in their components, so that they can make sure they don't conflict with the intended purposes of the software (so that GPL code isn't shipped with commercial products, for example).

The CLM platform also supports granular settings to allow policy exceptions (such as within a certain time period, or for a particular application version or environment). Additionally, it can take workflow-based actions, such as sending a request for approval to a project manager when a developer wants to include a component that isn't on the allowed list.

Sonatype CLM currently integrates with IDEs such as Eclipse; continuous integration servers such as Hudson and Jenkins; and repository managers such as Nexus; and more are planned. The idea is to keep developers from having to fire up another tool in the middle of coding (and that's the direction that many other application security products are headed, if they're not there already).

Nexus Professional subscriptions come in packs: $1,200 per year provides a 10-user license bundle, and a 100-user pack is priced at $10,200 per year. The free Nexus has a wide adoption rate – Sonatype says it sees more than 20,000 active instances out on the Internet – but Nexus Pro has its own fan base, to the tune of approximately 400 customers. The company says its Application Health Check functionality is used by roughly 370 customers.

Strategy

There's plenty of talk about the need to secure the software supply chain, and some vendors even specialize in this area by helping to identify vulnerabilities in third-party applications. This is critically important – but pointing out the problems is where nearly everyone stops, and leaves the remediation as an exercise to the reader. There may be recommendations as to what to fix and in what order, but those are also pretty academic in nature, not tailored to the messy environments that enterprises have to live in. ('Tell a vendor that just went bankrupt to fix its software? You're kidding, right?') Encouraging organizations to avoid security mistakes from the start of the systems development lifecycle through education and early testing is a great idea – and it doesn't do a thing for the billions of lines of code out there already.

But Sonatype is sitting on a golden opportunity in the form of an unprecedented amount of leverage. If more than 80% of enterprise software is indeed composed of open source components, and those can not only be sourced from a validated repository but also updated by the developer to more secure versions with a few mouse clicks – well, you do the math. Short of parachuting in crack programming SWAT teams, there will probably be no easier way for enterprises to improve the security of their existing code at something approaching both low cost and large scale.

It's by no means a silver bullet – security flaws in applications run deeper and wider than whatever open source libraries and frameworks they use. There are still plagues of cross-site scripting and SQL injection vulnerabilities that will continue to ravage the world's software, as well as other vulnerable parts of the software stack that need to be addressed at an infrastructure level. But from a systemic point of view, Sonatype's CLM platform, together with the Central Repository, could have more impact on this 'invisible plague' that enterprises may not even realize they have.

Competition

With its Nexus Professional product, Sonatype is competing with JFrog's Artifactory as well as Apache's Archiva, although the company says that based on its Central Repository server logs, it has about 70% of the market compared with the other two. Heading in the same direction as CLM, API management vendor SOA Software recently renamed its Repository Manager as Lifecycle Manager. Other vendors that check code for open source, security issues and versions via repository include Black Duck, OpenLogic, Protecode and WhiteSource Software.

On the CLM side, Sonatype might be compared with Palamida, which also checks for open source software in code, both from a licensing and security point of view. But the combination of studied lifecycle management, enterprise policy and governance support, and more or less one-click remediation makes Sonatype stand out from the crowd. The open nature of the CLM platform is intended to allow customers to integrate and act on metadata from other tools they might already have invested in (such as Black Duck, or security-oriented static analysis from Fortify Software, Veracode, Checkmarx, Coverity, Armorize Technologies, WhiteHat Security, etc.).

If you're going to save the world, though, you need sidekicks. Sonatype already partners with application security consulting firms such as Aspect Security, and we would expect similar endeavors with players like Cigital, Denim Group, Praetorian, and many others small and large (it could be Big Four-friendly).

SWOT Analysis

Strengths

Sonatype's CLM platform helps shine a light on a pervasive problem: insecure open source software in enterprise applications. Its management allows for discovery, inventory, policy enforcement, and even push-button migration of component versions.

Weaknesses

Although the front end of the CLM platform is intended to integrate with the IDE for a seamless experience for the developer, it's still a separate management tool on the back end. This could curtail adoption a bit as overworked security and project managers try to keep their entire application portfolio in order with the other tools they already have.

Opportunities

In a word: leverage. If 80% of enterprise code is really open source, then securing it with remediation and validated clean components could have a widespread impact. That won't solve the whole problem of insecure applications, but it's a big start.

Threats

There are other products with similar open source organization functionality. If the large enterprise software quality management providers take up the open source banner, it could spell trouble for Sonatype.