VERACODE EBOOK

Addressing Your Open Source Risk

VERACODE

Challenges In Securing Open Source

When assessing the posture of your open source risk, you have to ask three key questions:

QUESTION ONE

Which libraries are we using, and do they contain any vulnerabilities?

QUESTION TWO

Does the vulnerable library actually do anything bad?

QUESTION THREE

Can I react fast enough to new vulnerabilities?

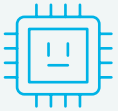
Nobody does it quite like Veracode

While we help our customers protect themselves from open source risks, there are a number of vendors that do the same basic discovery and reporting.

However, Veracode's focus is on coverage and actionable results that help development teams maintain velocity while ensuring more secure applications are delivered to production. The following are the technology aspects that set us apart from the rest of the competition.

NVD vs Veracode Proprietary Database

We've developed our own database that includes all of the open source vulnerabilities in the National Vulnerability Database (NVD), as well as our own list of vulnerabilities in open source libraries that haven't yet been disclosed to the NVD. In many cases, the vulnerabilities we find and record have either not been disclosed yet and are in the time between patching and full public disclosure or, in some cases, there was never any intent to disclose the vulnerability and its fix. There's a third category we track, which is "Reserved CVEs." We take the Reserved CVE IDs from the NVD and then find the vulnerabilities in the public repos in order to give you a jump on the fix prior to full public disclosure.



Machine Learning

The goal of our machine learning technology is to automate the identification of potential security vulnerabilities from commit messages and bug reports. In open source projects, bugs are typically tracked with issue trackers, and code changes are merged in the form of commits to source control repositories.

Our system uses natural language processing and real machine learning to identify potential vulnerabilities in open source libraries with a high level of accuracy. By analyzing the patterns found in past commit messages and bug-tracking issues using machine learning, our model can identify when new commits or bug issues resemble a silent fix of a potential vulnerability. These potential vulnerabilities are then raised to our security research team.

Security Research Team

The security research team is responsible for taking all of the data that our machine learning system sends us and reviewing each potential vulnerability to ensure that it is in fact real. If there are any false positives that return, the team adds this feedback into the system to better tune the algorithm over time.

License Database

In addition to tracking security vulnerabilities, which is the main focus of our technology, we also offer the ability to identify a limited set of open source licenses that can pose both business and financial risk to organizations.

Scanning Agent

Unlike our other scanning tools, which look at the binary of an application, the Software Composition Analysis agent scans source code in your projects, and thus we believe it's important to keep this scanning local. The agent is deployed with a single line added to your CI system, or within your CLI, by performing a CURL command and pulling the more up-to-date agent from Veracode on every build.

Call Graph

You can run the scanner interactively from a command line or automatically as part of a continuous integration process. By integrating with your build process, you always know exactly what code is being used. With each scan, it generates a call graph of your application as well as a complete and accurate dependency graph that describes with absolute precision what versions of open source libraries are being used. Using both the dependency graph and call graph, the scanner then performs control flow analysis to determine, with the best level of precision possible, if your application is actually using open source code in a vulnerable way.

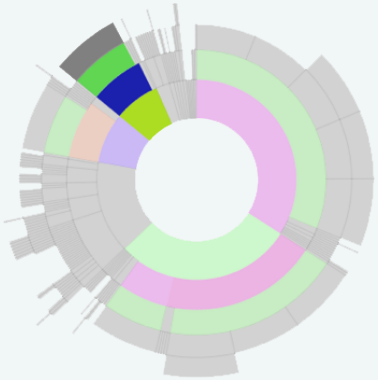
Vulnerable Methods

The call graph creation that happens by the agent (discussed in the previous section) allows us to see how data and controls flow through your application — which includes determining if that data is flowing through the vulnerable part of the open source library being used. If it is, we indicate back to the developer that this is, in fact, a vulnerable method, and it's causing your application to be vulnerable to exploits. When we scan with vulnerable methods, we find that up to 90 percent of the vulnerabilities reported aren't likely to actually impact the code. While we definitely recommend developers stay on top of the latest up-to-date version of every library they use, in reality, development and security teams have to work together to make trade-offs between security and speed. With vulnerable methods, developers can tackle the vulnerabilities that are actually likely to make their application vulnerable first, reducing their risk by the most in the shortest amount of time.

Dependency Graphs

This image is a visualization within our platform of a dependency graph. The empty circle in the middle is your application, and all of the sections around it are different direct and indirect libraries. In this specific example, all of the colored sections are libraries containing vulnerabilities that affect the application either directly or indirectly.

It's important to realize that just because your development teams may only be using a few open source libraries, they could actually be pulling in hundreds of different libraries indirectly. Our scanner identifies all of these, the versions being used, and any vulnerabilities that they contain. And for supported languages, it identifies the call stacks and traces the vulnerabilities through your application to identify those that actually impact your application and leave it open to exploits.



How you and your organization can benefit from Veracode's SaaS solution

Application security programs are only as good as the rate at which they're adopted. Veracode's Software Composition Analysis solution provides you with:

Developer adoption

We built our solutions with developers in mind to help your teams find and remediate issues. And since we're SaaS, no matter where your developers are, they can secure their code with remediation guidance for everything from vulnerable method indicators to code examples and full stack traces. You'll remediate faster with Veracode's self-serve online resources and personalized one-on-one consultation calls with your developers.

Better inventory and awareness of open source risk

Our extensive database of known and unknown/undisclosed vulnerabilities means you get the full view of your risk posture. With a full bill of materials covering your libraries, their versions, any vulnerabilities, and the licenses for them, you'll know exactly what's being used. We maintain that vulnerability database so your developers can access it no matter where they are in the world.

Steady development velocity

Developers can check their code while they're working on it thanks to CI integration, prioritization of vulnerabilities with vulnerable methods, and fix and update advisories. Lightning-fast feedback, directly in their environment, helps them get ahead of any problems and avoid unplanned work. And for applications already deployed, we notify you of new vulnerabilities we discover, without you having to rescan the code.

Ability to scale as your company grows

We're a SaaS-based company, which means you don't have expensive on-premises equipment to maintain. Our cloud scales with the needs of your business as you onboard more developers and build new applications. Whether all of your teams are in one building, or spread out across thousands of locations around the globe, they get the exact same level of service and quality of results.

Active Protection From Open Source Risk

There are a number of different places where you could start your application security program, and a lot of different paths to mature your program — but there aren't a lot of companies that can help cover your needs from end to end. When assessing your options for your AppSec partners, you need to look for a company that can cover the entire software development lifecycle (SDLC), with a strong focus not only on first- and third-party code, and also has the ability to implement a mature program. Veracode is the market leader in application security, and our years of experience have shown that those companies that evaluate their first-party code, plus open source libraries, and do so early, midway, and late in the SDLC have the best coverage. With Veracode, you can ensure a scalable, cost-effective AppSec program that helps make security part of your competitive advantage.

DOWNLOAD OUR WHITEPAPER

Learn more about your open source risk and how Veracode can help you reduce it.

VERACODE

Veracode is the leading independent AppSec partner for creating secure software, reducing the risk of security breach, and increasing security and development teams' productivity. As a result, companies using Veracode can move their business, and the world, forward. With its combination of process automation, integrations, speed, and responsiveness, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities. Veracode serves more than 2,500 customers worldwide across a wide range of industries. The Veracode solution has assessed more than 15 trillion lines of code and helped companies fix more than 51 million security flaws.

Learn more at www.veracode.com, on the Veracode blog, and on Twitter.