VERACODE | FACT SHEET

HIGHLIGHTS

- ✔ Addresses OWASP Top 10 and PCI requirements regarding governance of components with known vulnerabilities
- ✔ Enables identification and management of threats introduced by components in your software application portfolio
- ✔ Creates "Bill of Materials" (inventory) of all components, including information on where they are used, frequency of usage, versions and licensing
- ✔ Communicates known vulnerabilities from the NIST National Vulnerability Database (NVD) and suggests alternate components to integrate into the application infrastructure
- ✔ Supports blacklisting of specific components, such as Struts2
- ✔ Delivers remediation assistance early in development by providing information about the newest versions of a given component
- ✔ Offers remediation advisory services, including prioritization, threat modeling and security architecture reviews, from world-class security experts

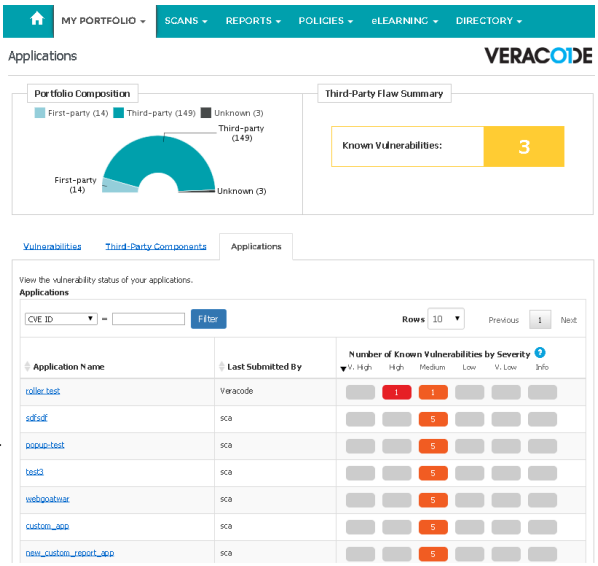
Software Composition Analysis

Reduce Risk From Third-Party and Open Source Components

To speed agile development, today's software applications are developed with the help of numerous third-party and open source components, such as frameworks, libraries and plug-ins. Up to 90 percent of an application is typically comprised of these third-party components, and many of them come from open source distribution with varying levels of security. For instance, many widely downloaded third-party components, such as the Apache Struts2 framework, contain critical vulnerabilities, which can lead to serious exploits such as DoS attacks and remote code execution.

Modern developers have grown accustomed to searching the web and downloading components — both open source and proprietary code. As a result, developers are increasingly creating software that contains code that they have not developed, and yet have not formally acknowledged its use. Also, traditional scanning tools do not typically assess third-party and open source components for vulnerabilities, resulting in increased risk and more false positives that drag down development velocity.

Other key challenges faced by developer organizations include the lack of automated and centralized ways to continuously monitor code and components in a development environment. This results in increased risk due to lack of resources and understanding of software components, and delayed product delivery through failure to keep up with the variety, complexity and release cadence of components used in an agile environment.



To help enterprises take advantage of the speed offered by component usage, Veracode offers software composition analysis, which enables developers to continuously audit all their code — including third-party and open source components — to identify vulnerabilities and offer remediation assistance and advisory services for all impacted applications. Veracode provides the only cloud-based service that combines binary static analysis (SAST), dynamic analysis (DAST) and software composition analysis via a single platform, using a single set of centralized policies, metrics, dashboards and remediation workflows across all applications and development teams.

VERACODE

FACT SHEET

HIGHLIGHTS

- ✓ Provides unified and consistent policies, metrics and reporting across all applications and their components
- ✓ Provides the same mitigation workflows as those used for SAST and DAST

KEY BENEFITS

- ✓ Automated, accelerated and secure software development by allowing developers to benefit from the time-to-market advantages associated with using third-party and open source libraries
- ✓ Reduced application risk for agile, component-based development environments without slowing down innovation
- ✓ Increased accuracy and coverage by combining software composition analysis with SAST, DAST and behavioral analysis within a unified platform to identify vulnerabilities in web, mobile and third-party applications

How It Works

Software composition analysis provides automated governance to manage third-party and open source components. It identifies components known to have security vulnerabilities or require proper licensing. Rather than scanning individual components, this capability identifies them using information (e.g., file size, file name) from external sources such as Maven (for Java) and NuGet (for .NET). Once it identifies the vulnerable components, software composition analysis provides information about intellectual property (IP) ownership, known security vulnerabilities, known remedies for those vulnerabilities, and references to outdated and most recent versions of components, along with their locations on the web.

In 2013, the Open Web Application Security Project (OWASP) acknowledged challenges faced by development organizations regarding component usage by adding section A-9: Using Components with Known Vulnerabilities to the OWASP Top 10. According to this section, "Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts."

Key Capabilities

Bill of Materials (Inventory): Provides an overview of all the components in the application portfolio, their versions and frequency of usage

Assessment of Known Vulnerabilities: Includes overview of known vulnerabilities in the component portfolio from the National Vulnerability Database, regular monthly updates of vulnerability information, and early warning updates for major known vulnerabilities or security concerns

Vulnerability Impact Analysis: Provides "self-service" impact analysis for known vulnerability concerns by quickly identifying components and applications affected by a specific vulnerability and isolating affected applications, their owners and download reports for the affected applications

Policy Manager Integration: Provides unified and consistent policies, metrics and reporting across all applications and their components

Remediation & Mitigation Workflow Assistance: Includes information about the newest versions of a given component as well as assistance with mitigation and management of known vulnerabilities similar to what is currently provided for flaws found through scanning

Advisory Services: Includes detailed threat modeling and security architecture reviews to safeguard your most critical applications once vulnerabilities and recommendations are identified

Unified View: Provided through consolidated reporting and dashboard views of both application- and component-level vulnerabilities within the entire portfolio

Accelerate Secure Software Development

Veracode's service accelerates secure software development by allowing developers to benefit from the time-to-market advantages associated with using third-party and open source libraries, without introducing unnecessary risk. With this service, enterprises can be confident the third-party components used to speed the software development processes are as secure as the code developed internally.

The new service has also been integrated with the company's cloud-based security service. The service combines multiple analysis technologies in a unified platform to identify vulnerabilities in web, mobile and third-party applications. For global enterprises,

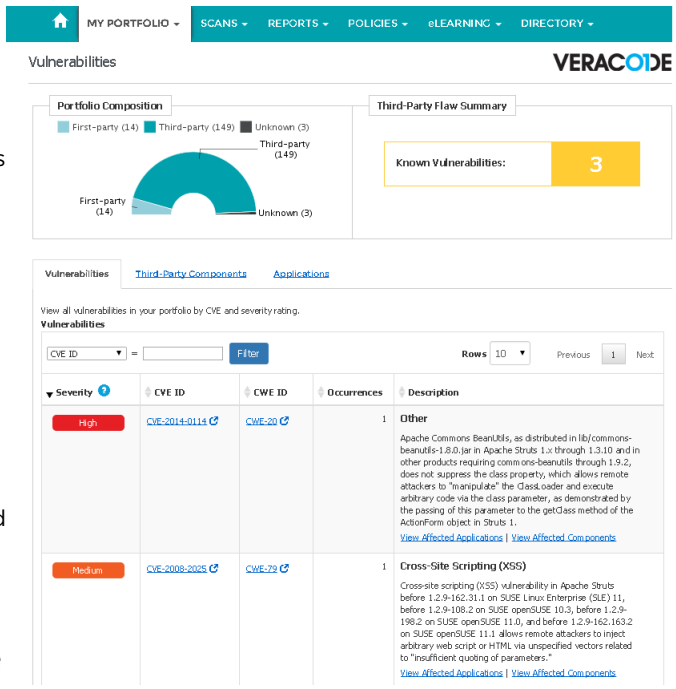
VERACODE

FACT SHEET

KEY BENEFITS

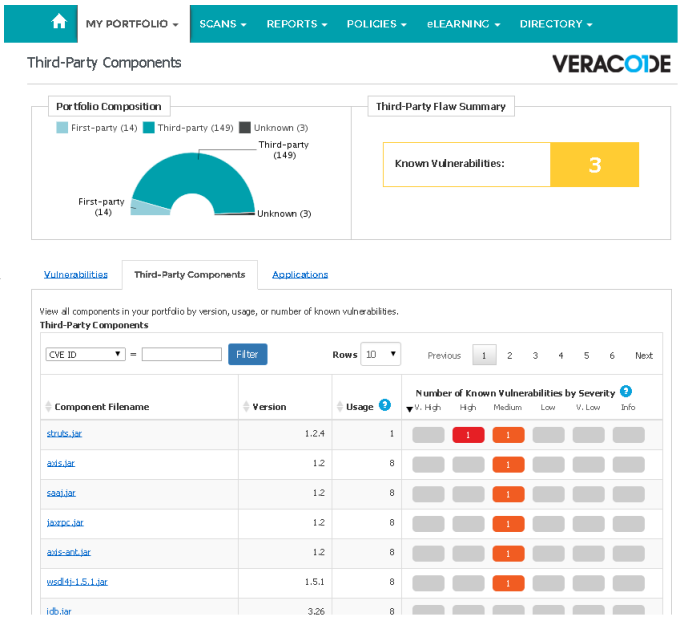
- ✔ **Ensured compliance and consistency for code used by developers**
- ✔ **Reduced complexity and risk through a single centralized platform for defining enterprise-wide policies and managing ongoing governance through Veracode's cloud-based service**
- ✔ **Continuous monitoring of complete component inventory for new vulnerabilities**
- ✔ **Improved incident response times with precise identification of components and applications to be remediated**
- ✔ **Improved code quality through increased rigor and documentation**

this approach significantly reduces complexity and risk by providing a central location for defining enterprise-wide policies and managing governance across diverse business units and development teams.



With this service, Veracode becomes the first vendor to integrate software composition analysis with binary static analysis (SAST) and dynamic analysis (DAST) in a single cloud-based service. The service provides a comprehensive inventory of third-party components used by internal developers and in third-party applications. The Veracode platform then provides vulnerability and version information for these components, so that developers can use the most up-to-date versions. Automated reporting and compliance workflows with centralized policy management are also available from the Veracode platform.

In addition, Veracode clients can use this service as the first step toward systematically addressing overall third-party risk. Through its outsourced Vendor Application Security Testing (VAST) program, Veracode helps organizations implement enterprise-wide governance programs and works directly with software vendors to ensure they comply with customers' corporate security policies.



To learn more, see: www.veracode.com/products

Veracode's cloud-based service and programmatic, policy-based approach deliver a simpler and more scalable solution for reducing global application-layer risk across web, mobileand third-party applications. Recognized as a Gartner Magic Quadrant Leader since 2010, Veracode secures hundreds of the world's largest global enterprises, including 3 of the top 4 banks in the Fortune 100 and 25+ of the world's top 100 brands.

VERACODE
The Most Powerful Application Security Platform on the Planet