Product brief

HP Fortify on Demand

Open source risk analysis powered by Sonatype

Recent research reveals that 71 percent of all applications contain security flaws classified as severe or critical, and an alarming 76 percent of all organizations have no component management policies in place.

Open source risk analysis powered by Sonatype

Open source usage has exploded. Today, 90 percent of the typical enterprise application is comprised of open source or 3rd party building blocks, known as components. In 2013, application developers downloaded over 13 billion components from the Central Repository, one of the largest web repositories for open source. While these reusable components accelerate application development and innovation, without proper insight and governance they could also pose considerable security risks, quality concerns or license issues.

Recent research reveals that 71 percent of all applications contain components with known security flaws classified as severe or critical, and an alarming 76 percent of all organizations have no component management policies in place. Concerns over component vulnerabilities are now high on the priority list for standards bodies, such as the Open Web Application Security Project (OWASP), Payment Card Industry (PCI) and the Financial Services Information Sharing and Analysis (FS-ISAC) whose guidelines now mandate that open source and 3rd party components with known vulnerabilities must be avoided.

To gain deeper visibility to potential threats, companies are combining static and dynamic application security testing with open source component-level analysis.

HP Fortify on Demand's Open Source Report

HP Fortify on Demand enhances its deep level of application security testing with the integration of a new "Sonatype Open Source Report". The Sonatype report allows any organization to analyze their application's use of open source and 3rd party components, understand the application's composition including a "component bill of materials", and uncover known potential security, licensing, policy, and quality problems.

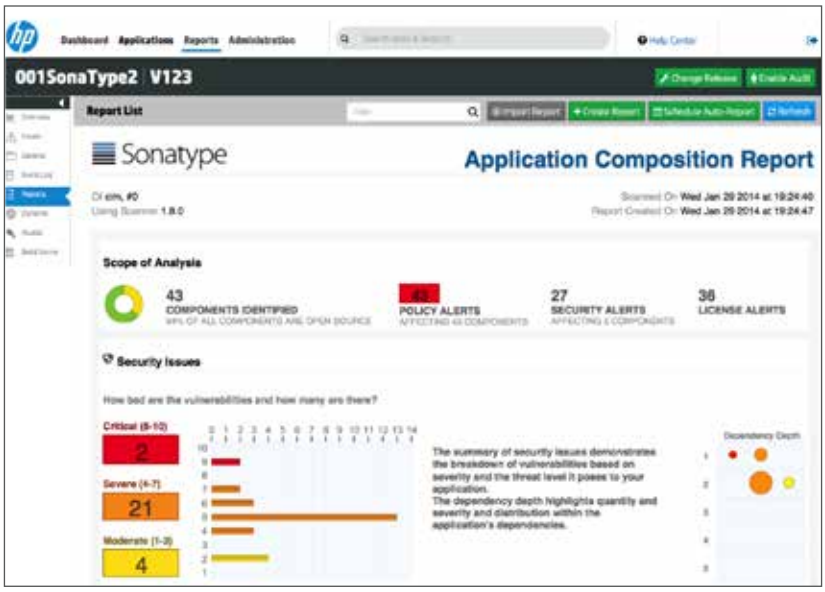
For application security and development teams, getting started with the HP Fortify on Demand open source risk analysis is easy. Simply upload an application as part of the Fortify on Demand static scan workflow. Once the analysis is complete – usually within five minutes – it is posted within Fortify on Demand reports section. Simply select the "Sonatype Open Source Report" download button and the 8-10 page report will be presented.

About Sonatype

HP Fortify on Demand's Open Source Report is powered by Sonatype. Sonatype makes it easy to create trusted applications and keep them that way over time. More than 20,000 customers rely on Sonatype to manage their open source and third party components.

Sonatype's Component Lifecycle Management (CLM) software empowers developers to select and use the best components early in the software lifecycle and easily remediate known vulnerabilities. Plus, policy automation, ongoing monitoring, and proactive alerts ensure these applications remain secure over time.

www.sonatype.com/clm



HP Fortify on Demand delivers deeper application analysis with the Sonatype Open Source Report. The sample above shows a portion of the summary for the complete 8 page report.

Each Sonatype Open Source Report provides a:

- Summary: the number of components analyzed, including key security issues and a breakdown of licenses that are in the application as well as where they are in the tree
- Bill of Materials: a complete list of the components analyzed within your application
- Security Analysis: an accurate list of known security threats sorted by vulnerability and severity level
- Quality Analysis: details of component age, fingerprint verification, and adherence to policies
- License Analysis: the license descriptors for every component and its license implication for your application

Analyze and Take Action

HP Fortify on Demand's open source report delivers quick feedback on risks that enable security and development teams to establish plans that can remediate potential vulnerabilities, advocate changes to open source policies, or confirm compliance to industry regulations.

The open source report complements Fortify on Demand's in-depth, application source code level security testing. Multiple levels of analysis and testing deliver more value through improved risk evaluation of applications, including those for mobile and web.

For more Information

http://www8.hp.com/us/en/software-solutions/fortify-on-demand-application-security

or

www.sonatype.com/fortify