Mend for Bitbucket Server Integration

Automatic detection and remediation of open source vulnerabilities in your own BitBucket server

The Challenge

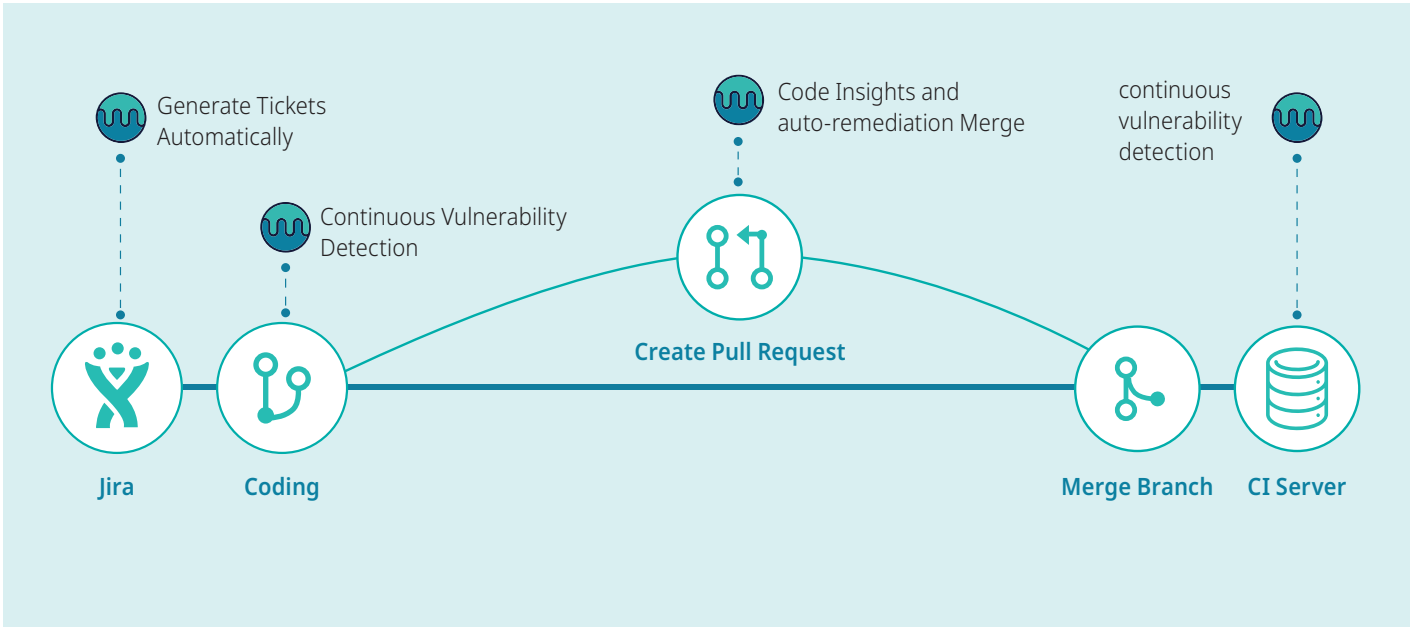
Software developers today rely heavily on opensource components, but having to ensure that each component and its dependencies are secure often delays the development process.

Integrating security tools into the software development lifecycle (SDLC) enable teams to detect vulnerabilities earlier in the development process, when it is easier and quicker to fix them. However, these security tools can add more work and slow down development.

The Mend Solution

Implement a developer-focused security tool within your developers native coding environment, so that they can use open source components without compromising on security or agility.

The Mend Bitbucket Server integration is a Bitbucket Server app that alerts developers on open source vulnerabilities while they are coding, and provides them with all the information that they need right from the Bitbucket UI. The integration can even automatically generate pull requests for vulnerable components to make the remediation process as easy as possible.



Key Benefits

1

Secure Continuously Within Bitbucket Server

Manage your open source vulnerabilities effortlessly, from your Bitbucket UI.
Track your repositories and get real-time alerts, detailed information, and actionable insights on vulnerable open source libraries and their dependencies as soon as they are added to your projects, all within the Bitbucket workflow.

2

Automate and Simplify Remediation

Remediate quickly with automatic pull requests which contain verified suggested fixes for vulnerable libraries. Get detailed information to help you make educated decisions, including the exact location of each open source security vulnerability in your repositories, with dependency trees displaying the paths to the vulnerable direct/indirect dependency, severity score, reference links and more.

3

Speed Up Development with Automated Workflows

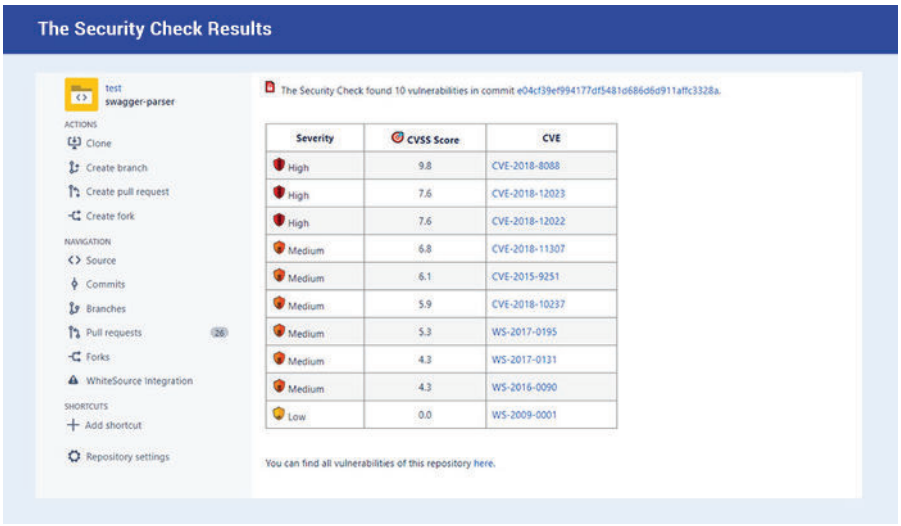
Enforce security policies automatically by triggering automated workflows to save time and speed up the remediation process. Automated workflows include tracking your repositories, opening a JIRA ticket, and remediating vulnerabilities.

Product Specifications

Languages	Supports over 200 programming languages
Deployment Options	Bitbucket Server versions 5.16 and above, supports both cloud-based andon-premises Mend deployments.
Scan triggers	A scan is automatically initiated on any push to the repository, for the new code that was added.
Pull Request	Pull requests will automatically be opened, with the fixed version for detected vulnerabilities in your repositories. Pull Request data includes the vulnerability within that PR, along with the file that's vulnerable and the text diff.
Additional Integrations	Integrates with Code Insights for enhanced PR (pull request) information. Jira tickets can be opened automatically, based on Mend policies.
Automated Policies	Initiate automated workflows based on your organization's open source security policies.

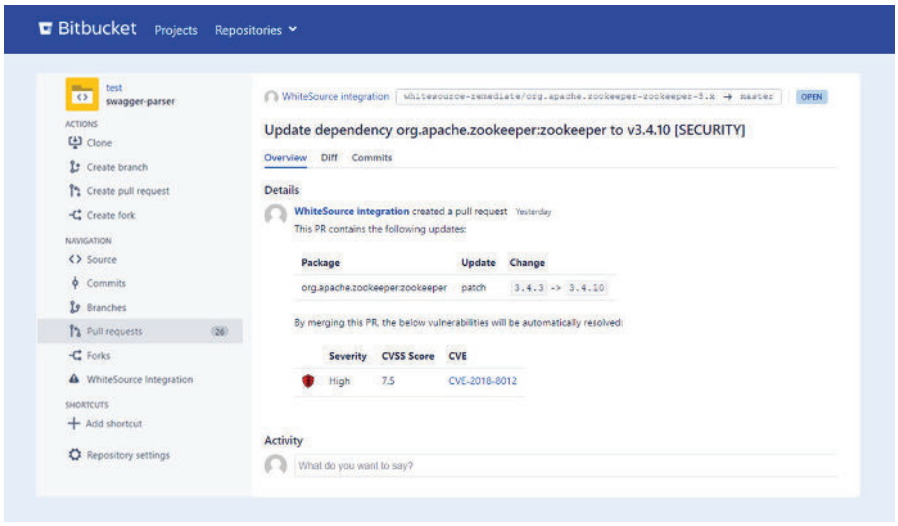
Security Check Results

An updated vulnerability list is produced on every push to your repository. This is a detailed view of every vulnerable open source library dependency with its CVSS score and a link to the CVE details.



Pull requests

Under the Pull requests tab, see all of your dependency updates.
The Mend app discovers and processes all dependency files in a repository and automatically opens pull requests with the fixed version for detected vulnerabilities.



Open Source Security Report

The report provides reference links, a dependency tree (if it exists), vulnerability information, and suggested fixes for each detected known open source security vulnerability.