WhiteSource

WHITESOURCE FOR GITLAB

DATASHEET

THE CHALLENGE

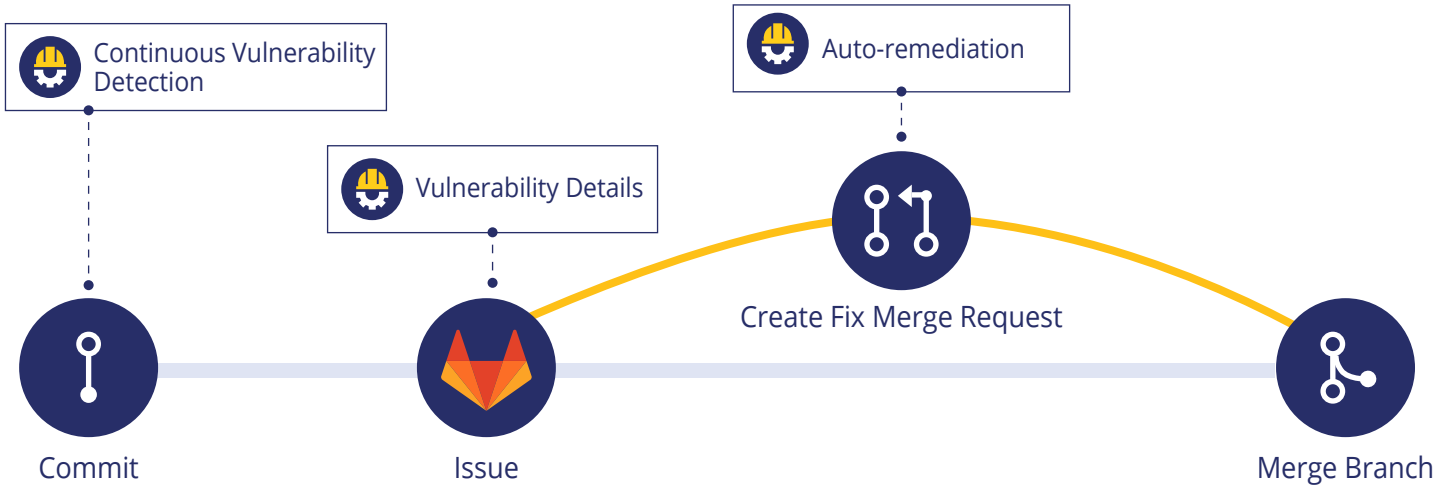
Software developers today rely heavily on open source components, but having to ensure that each component and its dependencies are secure often delays the development process.

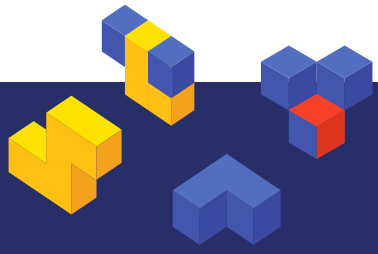
Integrating security tools into the software development lifecycle (SDLC) enables teams to detect vulnerabilities earlier in the development process when it is easier and quicker to fix them. However, these security tools can add more work and slow down development.

THE SOLUTION

Implement a developer-focused security tool within your developers' native coding environment, enabling them to use open source components without compromising on security or agility.

WhiteSource for GitLab is a native GitLab integration that alerts developers on open source vulnerabilities early in the SDLC, and provides them with all the information that they need within the GitLab UI. The integration can even automatically generate merge requests for vulnerable components to make the remediation process as easy as possible.





TOP BENEFITS

1

Secure Continuously Within GitLab

Manage your open source vulnerabilities effortlessly, from your GitLab 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, without interrupting your GitLab workflow.

2

Automate Remediation

Remediate quickly with automatic merge requests which contain verified suggested fixes for open source vulnerabilities. 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 Streamlined Workflows

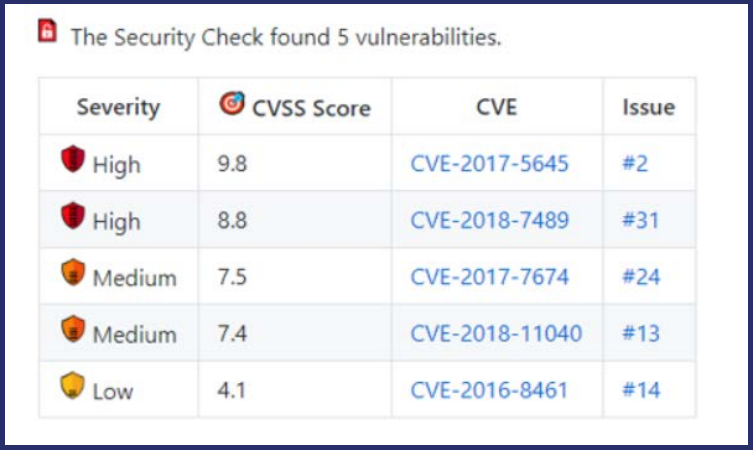
Enforce security policies automatically by triggering automated workflows to save time and speed up development. Automated workflows include tracking your repositories, opening a JIRA ticket, and remediating vulnerabilities.

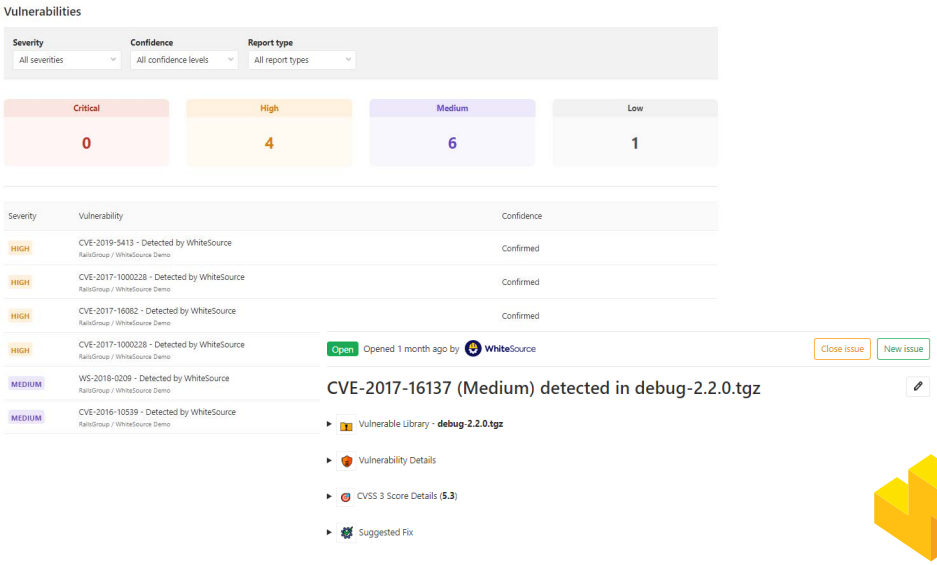
PRODUCT SPECIFICATIONS

Languages	Supports over 200 programming languages
Deployment Options	Supports both cloud-based and on-premises WhiteSource deployments.
Project Types	Supports all project Types.
Scan Triggers	A scan is automatically initiated on any push to the repository, for the new code that was added.
Merge Requests	Merge requests will automatically be opened. Data includes the vulnerability within that MR, along with the file that's vulnerable and the text diff.
Additional Integrations	Jira tickets can be opened automatically, based on WhiteSource policies.
Automated Policies	Initiate automated workflows based on your organization's open source security policies
Remediation	Merge requests will automatically be opened, with the fixed version for detected vulnerabilities in your repositories.

THE SECURITY CHECK RESULTS

An updated list is produced on every push to your repository. This is a detailed view of every open source vulnerability, with its CVSS score, link to the CVE details, and a link to a dedicated GitLab Issue opened by WhiteSource.





FULL OPEN SOURCE SECURITY REPORT

The report provides reference links, a dependency tree, vulnerability information, and suggested fixes for each detected known open source security vulnerability.
Gitlab Ultimate users can also view this data from their comprehensive Security Dashboard.

MERGE REQUESTS

Under the Merge Requests tab, see all of your dependency updates. The WhiteSource integration discovers and processes all dependency files in your repository and automatically opens merge requests with the fixed version for detected vulnerabilities.