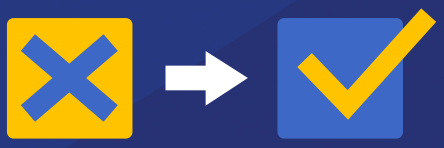
WhiteSource

WhiteSource Remediation Solution

DATASHEET



THE CHALLENGE

Manual remediation of known open source vulnerabilities requires a lot of time and effort from developers. It consists of keeping track of all of the open source components that you are using, detecting the vulnerable ones, locating its fixes, and updating the vulnerable versions.

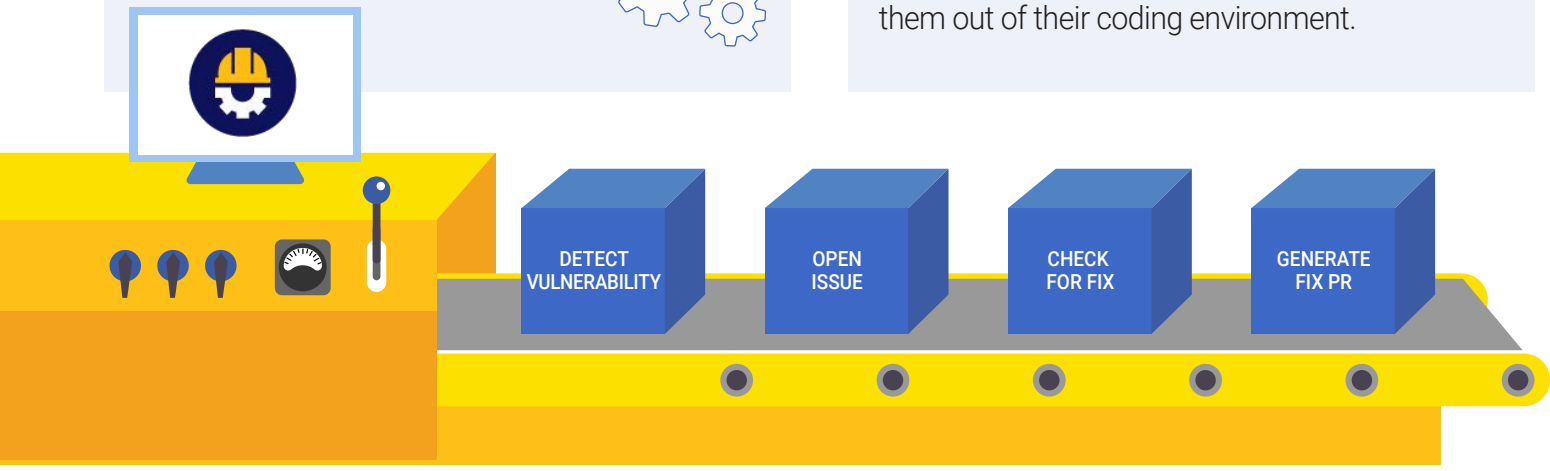
Open source security vulnerabilities need to be addressed quickly since the vulnerability and its exploitation information are publicly available to both users and hackers. This places organizations in a race against the hackers as soon as a known open source vulnerability has been published. But how can you remediate swiftly, considering the complex and time-consuming processes that are required in order to stay on top of known open source vulnerabilities?

THE SOLUTION

WhiteSource Remediate enables developers to fix vulnerable components with one click. It continuously tracks repositories to detect vulnerable open source libraries, and then automatically generates Pull Requests (PRs) with the latest version updates, including the relevant information to help users make educated decisions.

When a new security vulnerability is reported, WhiteSource Remediate provides a fixed version on the same day, to help reduce the attack window.

Automating the process of remediating vulnerable open source components helps developers meet tight deadlines, and reduce their risk of been exposed to known vulnerabilities, significantly improving their security posture without taking them out of their coding environment.



TOP BENEFITS

1 SPEED UP REMEDIATION WITH AUTOMATED WORKFLOWS

Enforce automated remediation policies to fix vulnerable open source components. Replace the time consuming manual tasks of detecting the known open source vulnerabilities in your projects, tracking newly disclosed vulnerabilities, and researching the right fix, all with automated workflows for quicker remediation.

2 ONE-CLICK FIX FOR MAXIMIZED PRODUCTIVITY

Pull Requests (PR) are generated automatically, in real-time, whenever a vulnerable open source component is detected so developers can simply click “merge” to update the vulnerable library. Each Pull Request is generated with release notes.

3 MINIMIZE THE ATTACK WINDOW

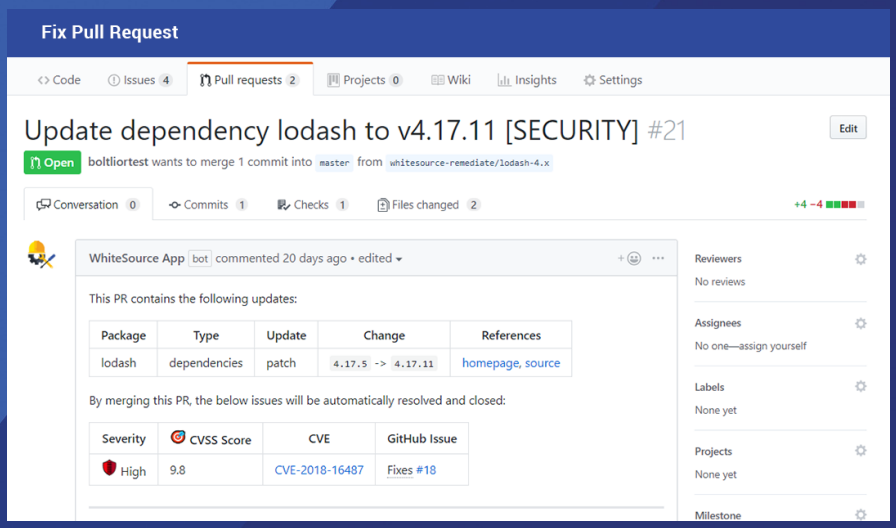
Once a known vulnerability is reported, all information about the vulnerability and its exploitation becomes public. Therefore, your product becomes exploitable until you update the vulnerable component. Minimize your exposure by automating the remediation process.

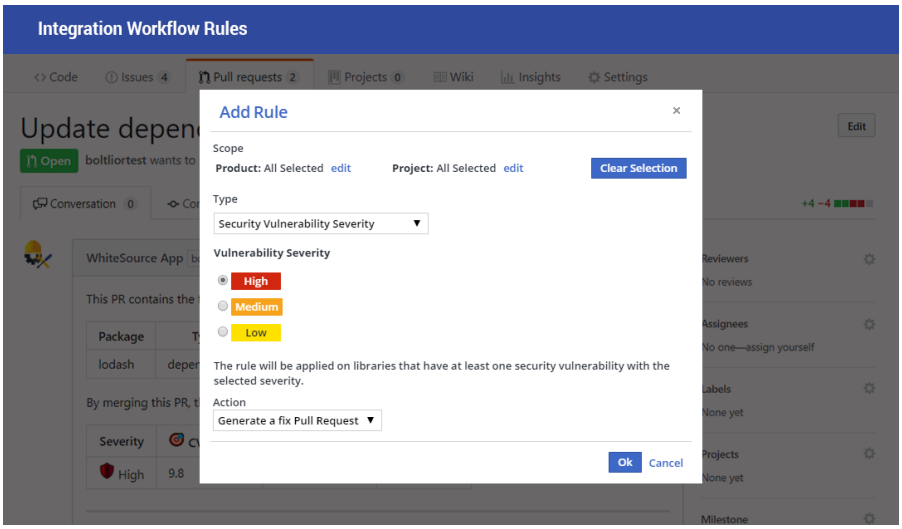
DATA SPECIFICATIONS

Languages	Java, JavaScript, PHP, Python, Golang, .NET
Package managers	Maven, NPM, Nuget, vgo (Go Modules), Composer, Pip, setuptools, Pipenv
Integration	Supports GitHub Enterprise and Bitbucket Server Integrations Bitbucket server: 5.16 and above GitHub Enterprise: 2.15.1 and above GitHub.com
API	Not supported

FIX PULL REQUEST

A pull request is generated with the latest version update. It is added to the repository along with release notes so that users can compare the versions and generate the fix with one click.





INTEGRATION WORKFLOW RULES

Users can set up automated policies which initiate remediation Workflows. Policies can be defined per vulnerability severity, CVSS score, and product hierarchy.

CHANGE LOG

Users can see the exact changes in the code that were part of the fix PR as part of the commit, for future reference.